paloalto TECHDOCS

# Guide de l'administrateur PAN-OS

Version 10.1

docs.paloaltonetworks.com

## Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

## About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

## Copyright



## Last Revised

September 13, 2021

# Table of Contents



# Démarrage

Les rubriques suivantes détaillent les étapes qui vous aideront à déployer un nouveau pare-feu de dernière génération Palo Alto Networks. Elles fournissent des détails sur l'intégration d'un nouveau pare-feu à votre pare-feu et sur la configuration d'une politique de sécurité de base. Pour obtenir des directives sur le déploiement des fonctions de la plate-forme de sécurité afin de répondre aux besoins en matière de sécurité de votre réseau, passez en revue les Recommandations pour la fin du déploiement du pare-feu.

# Intégration du pare-feu dans votre réseau de gestion

Tous les pare-feu Palo Alto Networks fournissent un port de gestion hors bande (MGT) que vous pouvez utiliser pour effectuer les fonctions d'administration de pare-feu. À l'aide du portMGT, vous pouvez séparer les fonctions de gestion du pare-feu des fonctions de traitement des données, afin de protéger l'accès au pare-feu et d'améliorer les performances. Lors de l'utilisation de l'interface Web, vous devez effectuer toutes les tâches de configuration initiales à partir du port MGT, même si vous envisagez d'utiliser un port de données intrabande pour la gestion future de votre pare-feu.

Certaines tâches de gestion, telles que la récupération des licences et la mise à jour des signatures de menaces et d'applications sur le pare-feu, nécessitent l'accès à Internet. Si vous ne souhaitez pas autoriser l'accès externe à votre port MGT, vous devez configurer un port de données intrabande permettant l'accès aux services externes requis (via des itinéraires de service) ou envisager de charger manuellement les mises à jour de manière régulière.

***N'activez pas l'accès à votre interface de gestion à partir d'Internet ou d'autres zones non approuvées dans les limites de sécurité de votre entreprise. Cela est vrai que vous utilisiez le port de gestion dédié (MGT) ou que vous configuriez un port de données en tant qu'interface de gestion. Lors de l'intégration de votre pare-feu à votre réseau de gestion, suivez les Meilleures pratiques pour sécuriser l'accès administratif afin de vous assurer que vous sécurisez l'accès administratif à vos pare-feu et aux autres appareils de sécurité d'une manière qui empêche les attaques réussies.***

Les rubriques suivantes décrivent les étapes de configuration initiales nécessaires pour intégrer un nouveau pare-feu dans le réseau de gestion et le déployer dans une configuration de sécurité de base.

- Détermination de votre stratégie de gestion
- Effectuer la configuration initiale
- Configuration de l'accès réseau pour les services externes

***Les rubriques suivantes décrivent les étapes d'intégration d'un pare-feu de dernière génération Palo Alto Networks dans votre réseau. Cependant, pour la redondance, envisagez de déployer une paire de pare-feu dans une configuration haute disponibilité.***

## Détermination de votre stratégie de gestion

Le pare-feu Palo Alto Networks peut être configuré et géré localement ou de manière centralisée à l'aide de Panorama, le système de gestion de sécurité centralisée de Palo Alto Networks. Si vous disposez de six pare-feu ou plus sur votre réseau, Panama vous permet de bénéficier des avantages suivants:

- Réduction de la complexité et des frais d'administration en matière de gestion de la configuration, des politiques, des logiciels et de mises à jour de contenu dynamiques. À l'aide des groupes et des modèles dans Panorama, vous pouvez gérer de manière efficace la configuration spécifique au pare-feu localement sur un pare-feu et appliquer des politiques partagées sur tous les pare-feu ou groupes de périphériques.

- Agrégation des données de tous les pare-feu gérés et gain de visibilité sur tout le trafic de votre réseau. Le Centre de commande de l'application (ACC) dans Panorama fournit une seule vitre pour la création de rapports unifiée sur tous les pare-feu, qui vous permet d'examiner, d'analyser et de signaler un trafic réseau, des incidents de sécurité et des modifications administratives.

Les procédures qui suivent décrivent la gestion du pare-feu à l'aide de l'interface Web locale. Si vous souhaitez utiliser Panorama pour la gestion centralisée, vous devez d'abord effectuer la configuration initiale et vérifié que le pare-feu peut établir une connexion à Panorama. À ce stade, vous pouvez utiliser Panorama pour configurer votre pare-feu de manière centralisée.

## Effectuer la configuration initiale

Par défaut, le pare-feu de la série PA a une adresse IP de 192.168.1.1 et un nom d'utilisateur/mot de passe d'admin/admin. Pour des raisons de sécurité, vous devez modifier ces paramètres avant de procéder à d'autres tâches de configuration du pare-feu. Vous devez effectuer ces tâches de configuration initiales à partir de l'interface MGT, même si vous n'envisagez pas d'utiliser cette interface pour la gestion de votre pare-feu, ou à l'aide d'une connexion de port série directe à un port de console du pare-feu.

**STEP 1 |** Installez votre pare-feu et branchez-y l'alimentation.

*Si votre modèle de pare-feu modèle dispose d'une double alimentation, branchez le second bloc d'alimentation pour la redondance. Reportez-vous au guide de référence du matériel de votre modèle pour plus de détails.*

**STEP 2 |** Contactez votre administrateur réseau pour obtenir les informations requises.

- Adresse IP du port MGT
- netmask
- Passerelle par défaut
- Adresse du serveur DNS

**STEP 3 |** Connectez votre ordinateur au pare-feu.

Vous pouvez vous connecter au pare-feu de l'une des manières suivantes :

- Connectez un câble série de votre ordinateur au port de console et connectez-vous au pare-feu à l'aide d'un logiciel d'émulation de terminal (9600-8-N-1). Attendez quelques minutes que la séquence de démarrage se termine ; lorsque le pare-feu est prêt, l'invite prend le nom du pare-feu, par exemple `Connexion à PA-220`
- Connectez un câbleEthernetRJ-45 de votre ordinateur au portMGT du pare-feu. Dans un navigateur, accédez à l'adresse **`https://192.168.1.1`**.

*Il se peut que vous deviez modifier l'adresse IP de votre ordinateur par une adresse dans le réseau 192.168.1.0/24, telle que 192.168.1.2, afin d'accéder à cette URL.*

**STEP 4 |** Lorsque vous y êtes invité, connectez-vous au pare-feu.

Vous devez vous connecter à l'aide du nom d'utilisateur et du mot de passe par défaut (admin/admin). Le pare-feu commence alors à s'initialiser.

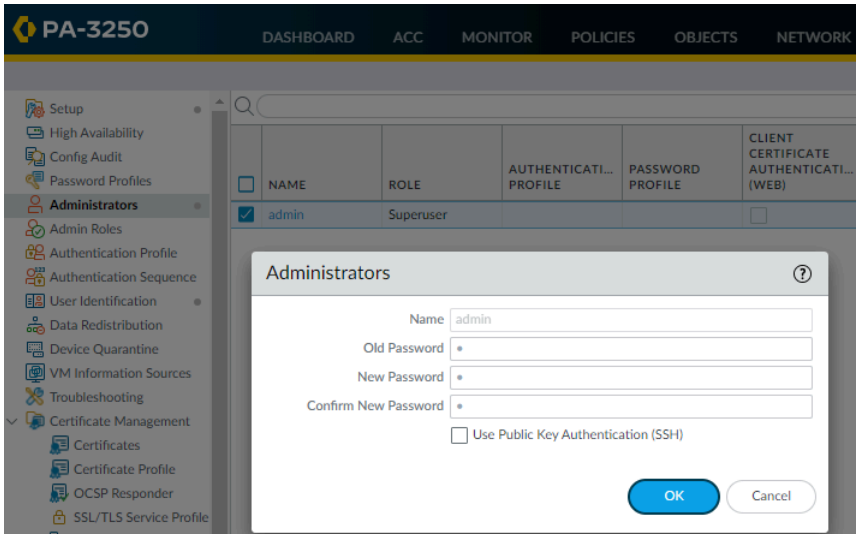
 

**STEP 5 |** Définissez un mot de passe sécurisé pour le compte d'administrateur.

*À partir de PAN-OS 9.0.4, le mot de passe de l'administrateur prédéfini par défaut (admin/admin) doit être modifié lors de la première connexion à l'appareil. Le nouveau mot de passe doit comporter au moins huit caractères et comprendre au moins une lettre minuscule et une lettre majuscule ainsi qu'un chiffre ou un caractère spécial.*

*Veillez à respecter les* bonnes pratiques en matière de robustesse des mots de passe *pour vous assurer de créer un mot de passe fort et de revoir les* paramètres de complexité des mots de passe.

1. Sélectionnez **Device (Périphérique)** > **Administrators (Administrateurs)**.
2. Sélectionnez le rôle **admin**.
3. Saisissez le mot de passe par défaut actuel et le nouveau mot de passe.




4. Cliquez sur **OK (OK)** pour sauvegarder vos paramètres.

**STEP 6 |** Configurez l'interface MGT.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Interfaces (Interfaces)** et modifiez les paramètres de l'interface de **Management (gestion)**.
2. Configurez les paramètres d'adresse pour l'interface MGT en utilisant l'une des méthodes suivantes :
   - Pour configurer les paramètres d'adresse IP statique pour l'interface MGT, définissez le **IP Type (Type d'IP)** à **Static (Statique)** et entrez **IP Address (l'Adresse IP)**, le **Netmask (Masque de réseau)**, et la **Default Gateway (Passerelle par défaut)**.
   - Pour configurer dynamiquement les paramètres d'adresse de l'interface MGT, définissez le **IP Type (Type d'adresse IP)** sur **DHCP Client (Client DHCP)**. Pour utiliser cette

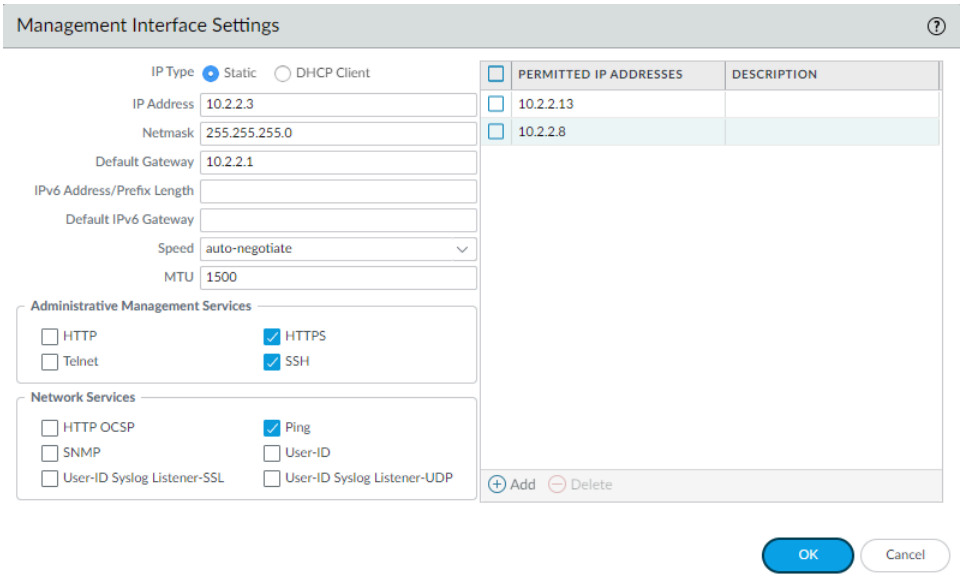
 

méthode, vous devez procéder à la Configuration de l'interface de gestion en tant que client DHCP.

*Pour empêcher tout accès non autorisé à l'interface de gestion, la meilleure pratique consiste à **Add (Ajouter)** les **Permitted IP Addresses (Adresses IP autorisées)** à partir desquelles un administrateur peut accéder à l'interface MGT.*

3. Définissez la **Speed (vitesse)** sur **auto-negotiate (Négocier automatiquement)**.
4. Sélectionnez les services de gestion à autoriser sur l'interface.

*Assurez-vous que **Telnet** et **HTTP** ne sont pas sélectionnés car ces services utilisent du texte en clair et ne sont pas aussi sécurisés que les autres services et peuvent compromettre les informations d'identification de l'administrateur.*




5. Cliquez sur **OK**.

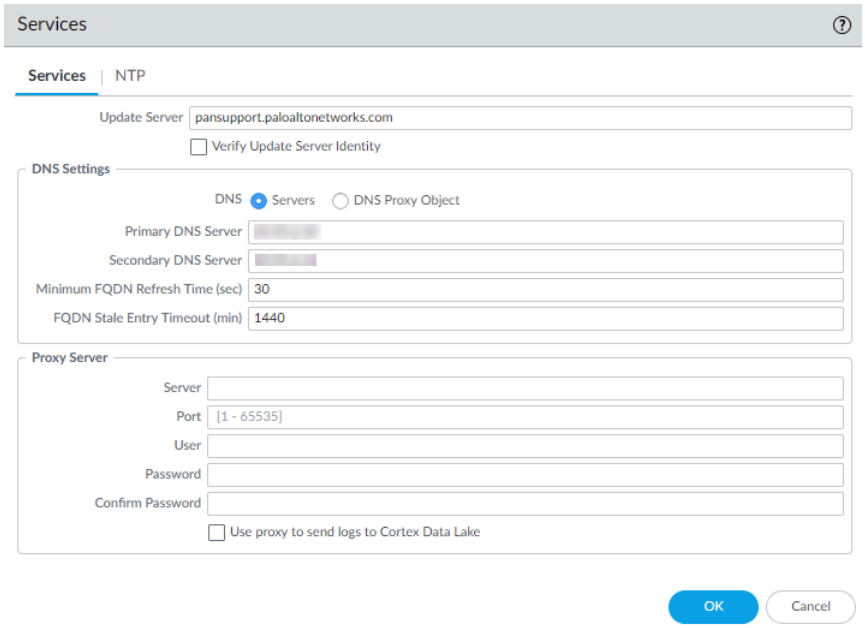
**STEP 7 |** Configurez DNS, mettez à jour le serveur et les paramètres du serveur proxy.

*Vous devez configurer manuellement au moins un serveur DNS sur le pare-feu, sinon il ne pourra pas résoudre les noms d'hôtes ; celui-ci n'utilisera aucun paramètre de serveur DNS d'une autre source, telle qu'un ISP.*

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Services**
   - Pour les plateformes de système multi-virtuelles, sélectionnez **Global (Global)** et modifiez la section Services.
   - Pour les plateformes de système virtuel unique, modifiez la section Services.
2. Sur l'onglet **Services (Services)**, pour **DNS**, sélectionnez l'un des éléments suivants :
   - **Servers (Serveurs)**: entrez l'adresse du **Primary DNS Server (serveur DNS principal)** et l'adresse du **Secondary DNS Server (serveur DNS secondaire)**.
   - **DNS proxy object (Objet proxy DNS)**: Depuis la liste déroulante, sélectionnez le **DNS Proxy (Proxy DNS)** que vous souhaitez utiliser pour configurer les services DNS

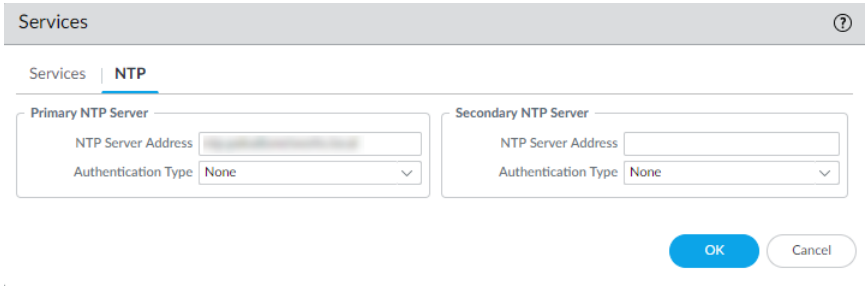
globaux, ou cliquez sur **DNS Proxy (Proxy DNS)** pour configurer un nouveau DNS proxy object (Objet proxy DNS).




3. Cliquez sur **OK**.

**STEP 8 |** Configurez les paramètres de date et d'heure (NTP).

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Services**
   - Pour les platesformes de système multi-virtuelles, sélectionnez **Global (Global)** et modifiez la section Services.
   - Pour les plateformes de système virtuel unique, modifiez la section Services.
2. Sur l'onglet **NTP**, pour utiliser le cluster virtuel des serveurs de temps sur Internet, entrez le nom d'hôte `pool.ntp.org` comme le **Primary NTP Server (Serveur NTP principal)** ou entrez l'adresse IP de votre serveur NTP principal.




3. (Facultatif) Saisissez une **Secondary NTP Server (adresse IP de serveur DNS Secondary (Secondaire))**.
4. (Facultatif Pour authentifier les mises à jour de temps à partir du (des) serveur (s) NTP, pour le **Authentication Type (Type d'authentification)**, sélectionnez l'un des éléments suivants pour chaque serveur :
   - **None (Aucun)**: (Par défaut) Désactive l'authentification NTP.
   - **Symmetric Key (Clé symétrique)**: Le pare-feu utilise l'échange de clés symétrique (secrets partagés) pour authentifier les mises à jour de temps.
     - **Key ID (ID de clé)** : saisissez l'ID de la clé (de 1 à 65 534).
     - **Algorithm (Algorithme)**– Sélectionnez l'algorithme à utiliser lors de l'authentification NTP (**MD5** ou **SHA1**).
   - **>Autokey**: Le pare-feu utilise autokey (cryptographie à clé publique) pour authentifier les mises à jour de temps.
5. Cliquez sur **OK**.

**STEP 9 |** (Facultatif) Configurez les paramètres généraux du pare-feu.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les paramètres généraux.
2. Saisissez un **nom d'hôte** pour le pare-feu, puis le nom de **domaine** de votre réseau. Le nom de domaine est un simple intitulé; il ne sera pas utilisé pour y accéder.
3. Entrez le texte de la **Login Banner (bannière de connexion)** qui informe les utilisateurs qui sont sur le point de se connecter qu'ils ont besoin d'une autorisation pour accéder aux fonctions de gestion du pare-feu.

   *Il est recommandé d'éviter d'utiliser du verbiage d'accueil. De plus, vous devriez demander à votre service juridique de revoir le message de la bannière. Il s'assurera que le message avertit convenablement les utilisateurs que tout accès non autorisé est interdit.*
4. Saisissez la **Latitude (latitude)** et la **Longitude (longitude)** pour permettre le placement précis du pare-feu sur la carte du monde.
5. Cliquez sur **OK**.

**STEP 10 |** Validez vos modifications.

*Une fois que les modifications de configuration sont enregistrées, vous perdez la connexion à l'interface Web car l'adresse IP a changé.*

Cliquez sur **Valider** dans le coin supérieur droit de l'interface Web. L'enregistrement de vos modifications par le pare-feu peut prendre jusqu'à 90 secondes.

**STEP 11 |** Connectez le pare-feu à votre réseau.

1. Déconnectez le pare-feu de votre ordinateur.
2. Connectez le port MGT à un port de commutateur sur votre réseau de gestion à l'aide d'un câble Ethernet RJ-45. Assurez-vous que le port de commutateur câblé au pare-feu est configuré pour la négociation automatique.

**STEP 12 |** Ouvrez une session de gestion SSH sur le pare-feu.

À l'aide d'un logiciel d'émulation de terminal, tel que PuTTY, lancez une session SSH sur le pare-feu à l'aide de la nouvelle adresse IP affectée à celui-ci.

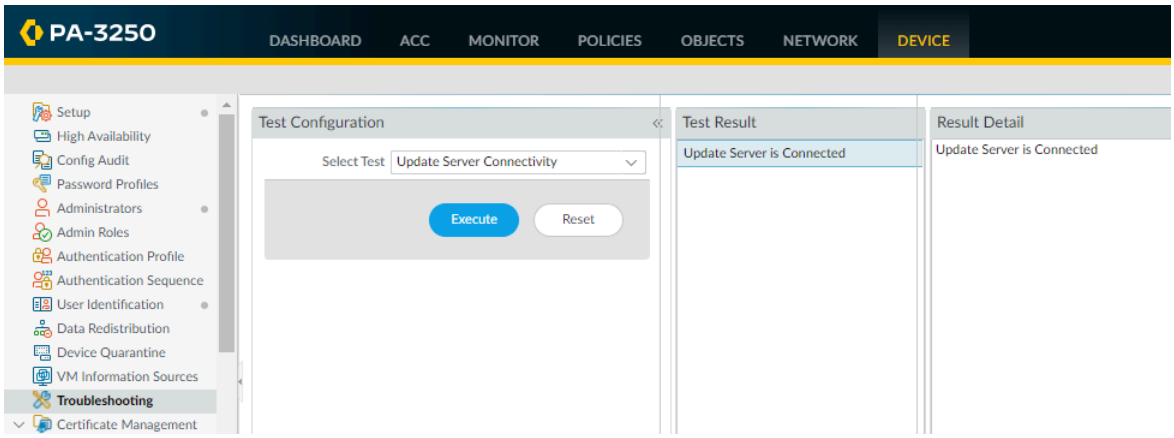
 

**STEP 13 |** Vérifiez l'accès réseau aux services externes nécessaire à la gestion de pare-feu, notamment au serveur de mise à jour Palo Alto Networks.

Vous pouvez le faire de l'une des façons suivantes :

- Si vous ne souhaitez pas autoriser l'accès réseau externe à l'interface MGT, vous devez configurer un port de données pour récupérer les mises à jour de service requises. Passez à la section Configuration de l'accès réseau pour les services externes.
- Si vous envisagez d'autoriser l'accès réseau externe à l'interface MGT, vérifiez que vous disposez de la connectivité, puis passez aux sections Enregistrer le pare-feu et Activation des licences d'abonnement.

1. Utilisez le test de connectivité au serveur de mises à jour pour vérifier la connectivité réseau au serveur Palo Alto Networks Update, comme illustré dans l'exemple suivant.
   1. Sélectionnez **Device (Périphérique)** > **Troubleshooting (Résolution des problèmes)**, puis sélectionnez **Update Server Connectivity (Connectivité au serveur de mises à jour)** dans la liste déroulante Select Test (Sélectionner le test).
   2. **Execute (Lancer)** le test de connectivité au serveur de mises à jour.




2. Utilisez la commande CLI suivante pour extraire des informations sur le droit de support pour le pare-feu à partir du serveur de mise à jour Palo Alto Network :

```
request support
check
```

Si vous disposez de la connectivité, le serveur de mise à jour répond avec l'état de support pour votre pare-feu. Si votre pare-feu n'est pas encore enregistré, le serveur de mise à jour renvoie le message suivant :

```
Contact Us

https://www.paloaltonetworks.com/company/contact-us.html

Support Home

https://www.paloaltonetworks.com/support/tabs/overview.html

Device not found on this update server
```

# Configuration de l'accès réseau pour les services externes

Par défaut, le pare-feu utilise l'interface MGT pour accéder aux services distants, tels que les serveurs DNS, les mises à jour de contenu et la récupération des licences. Si vous ne souhaitez pas autoriser l'accès réseau externe à votre réseau de gestion, vous devez configurer un port de données sur bande pour fournir l'accès aux services externes requis et configurer des itinéraires de service pour indiquer au pare-feu le port à utiliser pour accéder aux services externes.

***N'activez pas l'accès de gestion aux zones sécurisées de votre entreprise à partir d'Internet ou de toute autre zone non approuvée. Suivez les*** Meilleures pratiques pour sécuriser l'accès administratif ***afin de vous assurer que vous sécurisez correctement votre pare-feu.***

***Cette tâche nécessite la connaissance des interfaces, zones et politiques de pare-feu. Pour plus d'informations sur ces éléments, reportez-vous aux sections*** Configuration des interfaces et des zones ***et*** Configuration d'une politique de sécurité de base**.**

**STEP 1 |** Décidez quelle interface vous souhaitez utiliser pour accéder aux services externes et connectez-la à votre port de commutateur ou de routeur.

L'interface utilisée doit avoir une adresse IP statique.

**STEP 2 |** Connectez-vous à l'interface Web.

Dans votre navigateur Web, connectez-vous de manière sécurisée (https) à l'aide de la nouvelle adresse IP et du nouveau mot de passe affectés lors de la configuration initiale (https://<adresse IP>). Un avertissement de certificat s'affiche ; ne vous en préoccupez pas. Continuez vers la page Web.

**STEP 3 |** (Facultatif) Le pare-feu est préconfiguré avec une interface de câble virtuel par défaut entre les ports Ethernet 1/1 et Ethernet 1/2 (ainsi que des zones et une politique de sécurité par défaut correspondantes). Si vous n'envisagez pas d'utiliser cette configuration de câble virtuel, vous devez supprimer la configuration manuellement pour ne pas qu'elle interfère avec d'autres paramètres d'interface définis.

Vous devez supprimer la configuration dans l'ordre suivant:

1. Pour supprimer la politique de sécurité par défaut, sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis la règle et cliquez sur **Delete (Supprimer)**.
2. Pour supprimer le câble virtuel par défaut, sélectionnez **Network (Réseau)** > **Virtual Wires (Câbles virtuels)**, sélectionnez le câble virtuel et cliquez sur **Delete (Supprimer)**.
3. Pour supprimer les zones approuvées et non approuvées par défaut, sélectionnez **Network (Réseau)** > **Zones**, puis chaque zone et cliquez sur **Delete (Supprimer)**.
4. Pour supprimer les configurations d'interface, sélectionnez **Network (Réseau)** > **Interfaces**, puis sélectionnez chaque interface (ethernet 1/1 et ethernet 1/2) et cliquez sur **Delete (Supprimer)**.
5. **Commit (Validez)** les modifications.

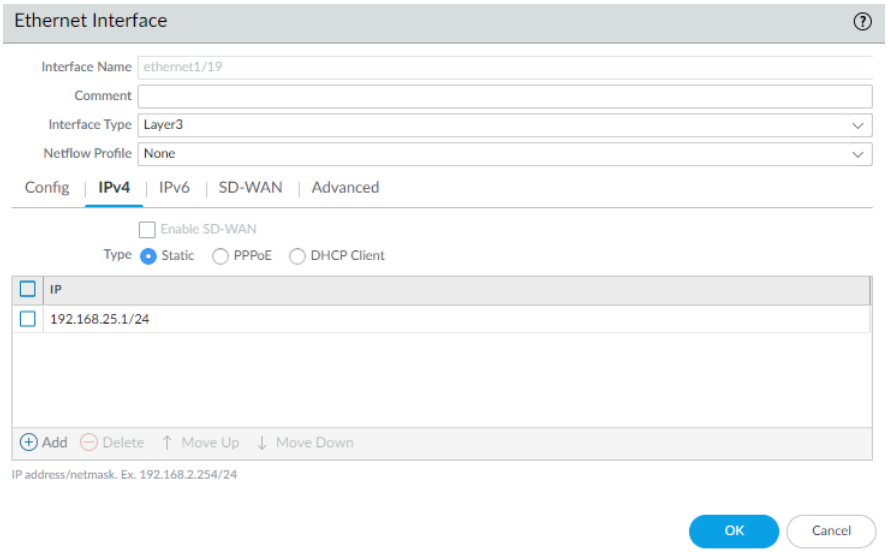
 

**STEP 4 |** Configurez l'interface que vous prévoyez d'utiliser pour l'accès externe aux services de gestion.

1. Sélectionnez **Network (Réseau)** > **Interfaces** et sélectionnez l'interface qui correspond à l'interface que vous avez câblée à l'étape 1.
2. Sélectionnez l'**Interface Type (Type d'interface)**. Bien que votre choix dépende ici de votre topologie réseau, cet exemple décrit les différentes étapes pour la **Layer 3 (Couche 3)**.
3. Dans l'onglet **Config (Configuration)**, développez la liste déroulante **Security Zone (Zone de sécurité)** et sélectionnez **New Zone (Nouvelle zone)**.
4. Dans la boîte de dialogue Zone, donnez un **Name (Nom)** à la nouvelle zone, par exemple, Gestion, puis cliquez sur **OK**.
5. Sélectionnez l'onglet **IPv4**, puis la case d'option **Static (Statique)**, cliquez sur **Add (Ajouter)** dans la section IP, puis saisissez l'adresse IP et le masque de réseau à affecter à l'interface,

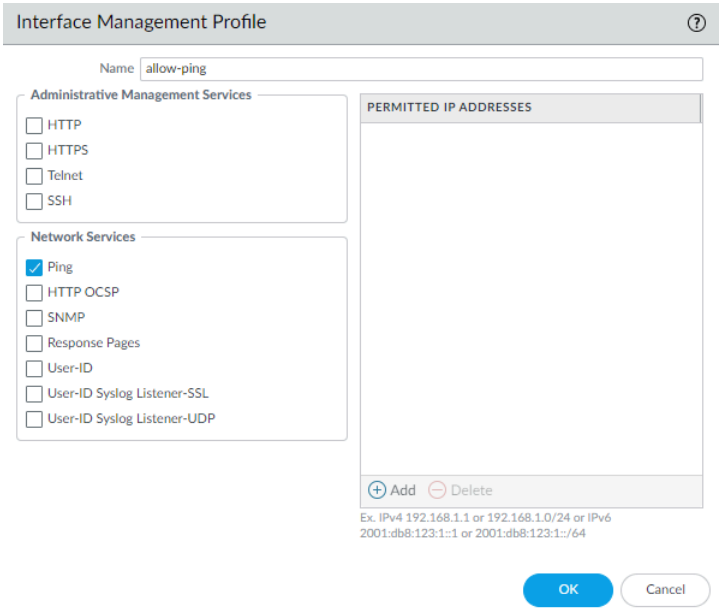
par exemple, 192.168.1.254/24. Vous devez utiliser une adresse IP statique sur cette interface.




6. Sélectionnez **Advanced (Avancé)** > **Other Info (Autres informations)**, développez la liste déroulante **Management Profile (Profil de gestion)**, puis sélectionnez **New Management Profile (Nouveau profil de gestion)**.
7. Saisissez un **Name (nom)** pour le profil, tel que allow_ping, puis sélectionnez les services que vous souhaitez autoriser sur l'interface. Afin d'autoriser l'accès aux services externes, activez uniquement **Ping**, puis cliquez sur **OK**.

*Ces services fournissent un accès de gestion au pare-feu ; par conséquent, sélectionnez uniquement les services qui correspondent aux activités de gestion que vous souhaitez autoriser sur cette interface. Par exemple, n'activez pas HTTP ou Telnet, car ces protocoles transmettent en texte simple et, par conséquent, ne sont pas sûrs. Ou, si vous envisagez d'utiliser l'interface MGT pour les tâches de configuration du pare-feu via l'interface Web ou la CLI, vous n'activez pas HTTP, HTTPS, SSH ou Telnet pour empêcher l'accès non autorisé via l'interface (si vous devez autoriser HTTPS ou SSH dans ce scénario, limitez l'accès à un ensemble donné de **Permitted IP Addresses [adresses IP autorisées]**). Pour plus d'informations, reportez-vous à la section* Utilisation des profils de gestion d'interface pour limiter l'accès.




8. Pour enregistrer la configuration de l'interface, cliquez sur **OK**.

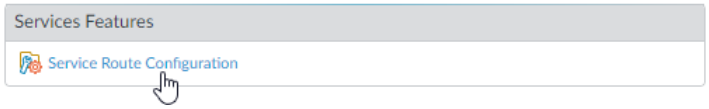
 

**STEP 5 |** Configuration des Itinéraires de service.

Le pare-feu utilise par défaut l'interface MGT pour accéder aux services externes requis. Pour changer l'interface que le pare-feu utilise pour envoyer des requêtes aux services externes, vous devez modifier les itinéraires de service.

*Cet exemple décrit comment configurer des itinéraires de service globaux. Pour obtenir des informations sur la configuration de l'accès réseau aux services externes sur la base d'un système virtuel plutôt que sur une base globale, reportez-vous au document* Itinéraires de service par système virtuel.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Services** > **Global** et cliquez sur **Service Route Configuration (Configuration de l'itinéraire de service)**.



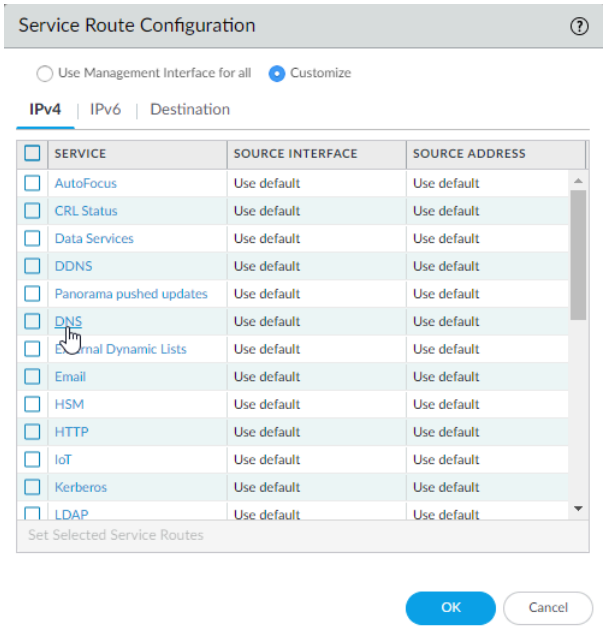

*Afin d'activer vos licences et d'obtenir le contenu et les mises à jour logicielles les plus récents, vous devez modifier l'itinéraire de service pour les services **DNS**, **Palo Alto Network Services (Services Palo Alto Network)**, **URL Updates (Mises à jour d'URL)**, et **AutoFocus**.*

2. Sélectionnez la case d'option **Customize (Personnaliser)**, puis l'une des options suivantes :
   - Pour un service prédéfini, sélectionnez **IPv4** ou **IPv6**, puis cliquez sur le lien correspondant au service. Pour restreindre la liste déroulante d'adresse source, sélectionnez **Source Interface (Interface source)**, puis sélectionnez l'interface que vous venez de configurer. Sélectionnez ensuite une adresse source (de cette interface) en tant qu'itinéraire de service.

     Si plusieurs adresses IP sont configurées pour l'interface sélectionnée, la liste déroulante **Source Address (Adresse source)** vous permet de sélectionner une adresse IP.
   - Pour créer un itinéraire de service pour une destination personnalisée, sélectionnez **Destination** et cliquez sur **Add (Ajouter)**. Saisissez l'adresse IP de **Destination**. Un paquet entrant dont l'adresse de destination correspond à cette adresse utilisera comme source l'adresse source que vous avez spécifié pour cette route de service. Pour restreindre la liste déroulante Source Address (Adresse source), sélectionnez une **Source Interface (Interface source)**. Si plusieurs adresses IP sont configurées pour l'interface

sélectionnée, la liste déroulante **Source Address (Adresse source)** vous permet de sélectionner une adresse IP.




3. Cliquez sur **OK** pour enregistrer les paramètres.
4. Répétez les étapes 5.2 à 5.3 ci-dessus pour chaque itinéraire de service que vous souhaitez modifier.
5. **Commit (Validez)** vos modifications.

**STEP 6 |** Configurez une interface externe et une zone associée, puis créez une règle de politique de sécurité pour permettre au pare-feu d'envoyer des demandes de service de la zone interne à la zone externe.

1. Sélectionnez **Network (Réseau)** > **Interfaces**, puis sélectionnez votre interface externe. Sélectionnez **Layer 3 (Couche3)** comme **Interface Type (Type d'interface)**, **Add (Ajoutez)** l'adresse **IP** (dans l'onglet **IPv4** ou **IPv6**), puis créez la **Security Zone (Zone de sécurité)** associée (dans l'onglet **Configuration**), telle que Internet. Cette interface doit disposer d'une adresse IP statique ; vous n'avez pas à configurer de services de gestion sur cette interface.

2. Pour configurer une règle de sécurité autorisant le trafic de votre réseau interne au serveur de mises à jour Palo Alto Networks, sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis cliquez sur **Add (Ajouter)**.

*Lors de la création de règles de politique de sécurité, il est recommandé d'utiliser des règles fondées sur une application plutôt que des règles fondées sur un port pour veiller à bien identifier l'application sous-jacente, peu importe le port, le protocole, la tactique d'évasion ou le chiffrement en cours d'utilisation. Assurez-vous que le **Service** est défini sur **application-default (par défaut de l'application)**. Dans ce cas, créez une règle de politique de sécurité qui autorise l'accès au serveur de mises à jour (et aux autres services Palo Alto Networks).*

| | NAME | Source ZONE | Destination ZONE | APPLICATION | SERVICE | ACTION |
|---|---|---|---|---|---|---|
| 1 | Palo Alto Networks Services | Management | Internet | paloalto-dns-security<br>paloalto-logging-service<br>paloalto-updates<br>paloalto-wildfire-cloud | application-... | Allow |

**STEP 7 |** Créez une règle de politique NAT.

1. Si vous utilisez une adresse IP privée sur l'interface interne, vous devez créer une règle NAT source pour traduire l'adresse en une adresse pouvant être acheminée publiquement. Sélectionnez **Policies (Politiques)** > **NAT**, puis cliquez sur **Add (Ajouter)**. Vous devez au moins définir un nom pour la règle (onglet **General (Général)**), indiquer une zone source et une zone de destination, Gestion à Internet dans ce cas (onglet **Original Packet (Paquet d'origine)**), définir les paramètres de traduction d'adresse source (onglet **Translated Packet (Paquet traduit)**), puis cliquer sur **OK**.
2. **Commit (Validez)** vos modifications.

| | NAME | Original Packet SOURCE ZONE | DESTINATION ZONE | SERVICE | Translated Packet SOURCE TRANSLATION | DESTINATION TRANSLATION |
|---|---|---|---|---|---|---|
| 1 | Source NAT | Management | Internet | any | dynamic-ip-and-port | none |

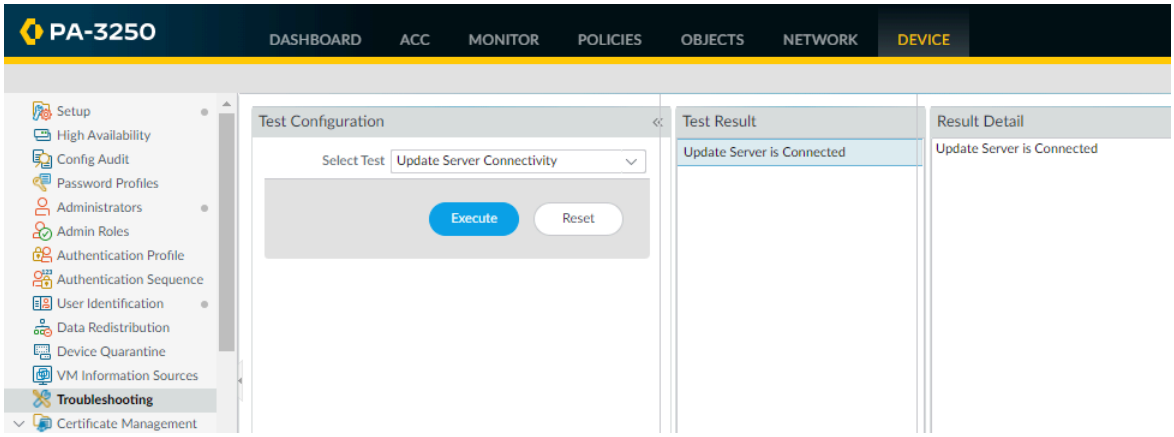
**STEP 8 |** Sélectionnez **Device (Périphérique)** > **Troubleshooting (Résolution des problèmes)** et vérifiez que vous disposez de la connectivité entre le port de données et les services externes, y compris la passerelle par défaut, en utilisant le test de connectivité **Ping**, et le serveur de mises à jour Palo Alto Networks à l'aide du test de **Update Server Connectivity (Connectivité au serveur de mises à jour)**. Dans cet exemple, la connectivité du pare-feu au serveur de mises à jour de Palo Alto Networks est testée.

Une fois que vous avez vérifié que vous disposez de la connexion réseau requise, passez aux sections Enregistrement du pare-feu et Activation des licences d'abonnement.

1. Sélectionnez **Update Server (Serveur de mises à jour)** dans la liste déroulante Select Test (Sélectionner le test).

2. **Execute (Exécutez)** le test de connectivité au serveur de mises à jour de Palo Alto Networks.




3. Accédez à la CLI du pare-feu, et utilisez la commande suivante pour extraire des informations sur le droit de support pour le pare-feu à partir du serveur de mise à jour Palo Alto Network :

```
request support
check
```

Si vous disposez de la connectivité, le serveur de mise à jour répond avec l'état de support pour votre pare-feu. Comme votre pare-feu n'est pas enregistré, le serveur de mise à jour renvoie le message suivant :

```
Contact Us
https://www.paloaltonetworks.com/company/contact-us.html
Support Home
https://www.paloaltonetworks.com/support/tabs/overview.html
Device not found on this update server
```

# Enregistrement du pare-feu

Avant de pouvoir activer le support et d'autres licences et abonnements, vous devez d'abord enregistrer le pare-feu. Avant de pouvoir enregistrer un pare-feu, vous devez d'abord disposer d'un compte de support actif. Effectuez l'une des tâches suivantes selon que vous possédez ou non un compte de support actif :

- Si vous n'avez pas de compte de support actif, alors Créer un nouveau compte de support et enregistrer un pare-feu.
- Si vous avez déjà un compte de support actif, alors vous êtes prêt à Enregistrement du pare-feu.
- (Facultatif) Procédez à la configuration du jour 1 sur un pare-feu enregistré
- Si votre pare-feu utilise des cartes de ligne telles qu'une NPC (Network Processing Card), alors Enregistrez les cartes de ligne de pare-feu.

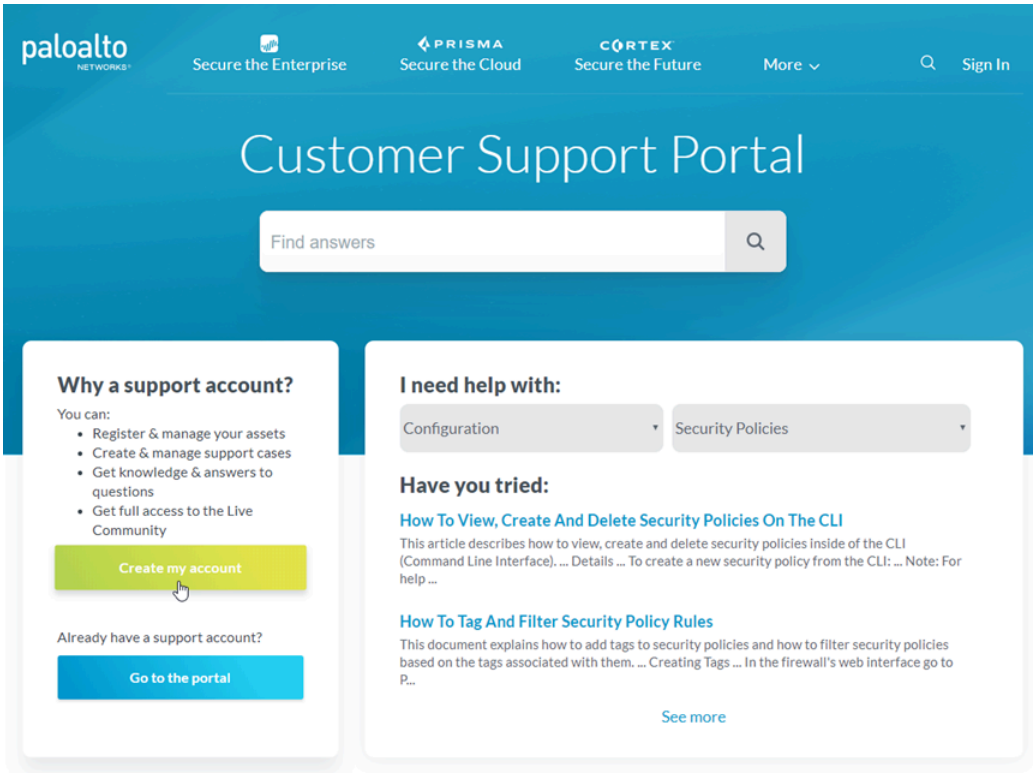
*Si vous* enregistrez un pare-feu VM-Series, *reportez-vous au* Guide de déploiement des pare-feu VM-Series.

## Créer un nouveau compte de support et enregistrer un pare-feu

Si vous ne possédez pas de compte de support Palo Alto Networks actif, vous devez alors enregistrer votre pare-feu lors de la création de votre nouveau compte de support.

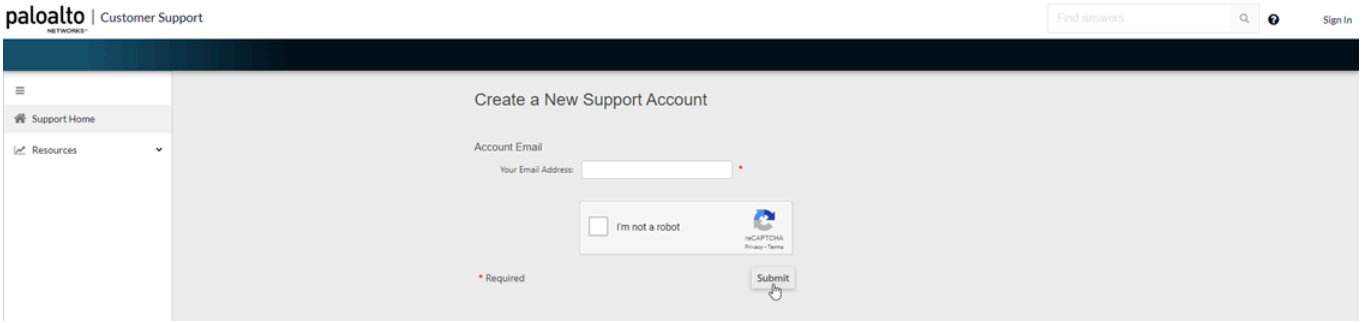
**STEP 1 |** Connectez-vous au portail de support client de Palo Alto Networks.

**STEP 2 |** Cliquez sur **Create my account (Créer mon compte)**.

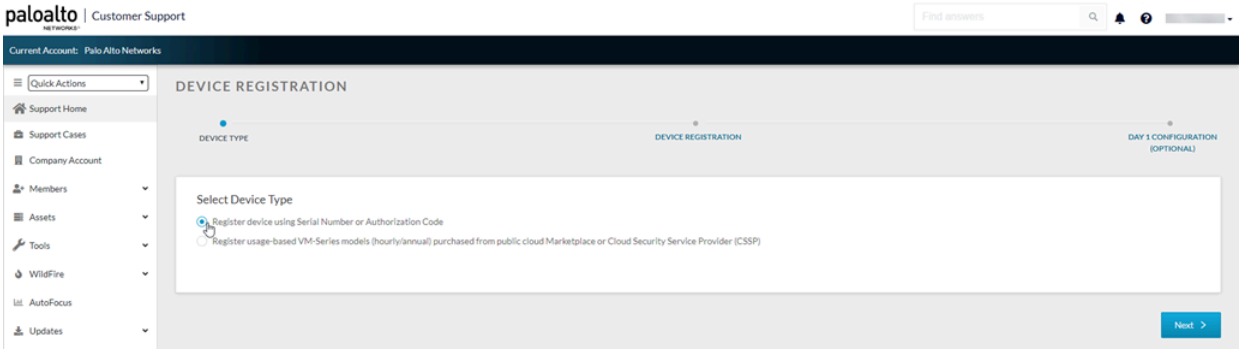


**STEP 3 |** Saisissez **Your Email Address (Votre adresse e-mail)**, cochez **I'm not a robot (Je ne suis pas un robot)**, puis cliquez sur **Submit (Soumettre)**.




**STEP 4 |** Sélectionnez **Register device using Serial Number or Authorization Code (Enregistrer un périphérique au moyen d'un numéro de série ou d'un code d'autorisation)** et cliquez sur **Submit (Soumettre)**.



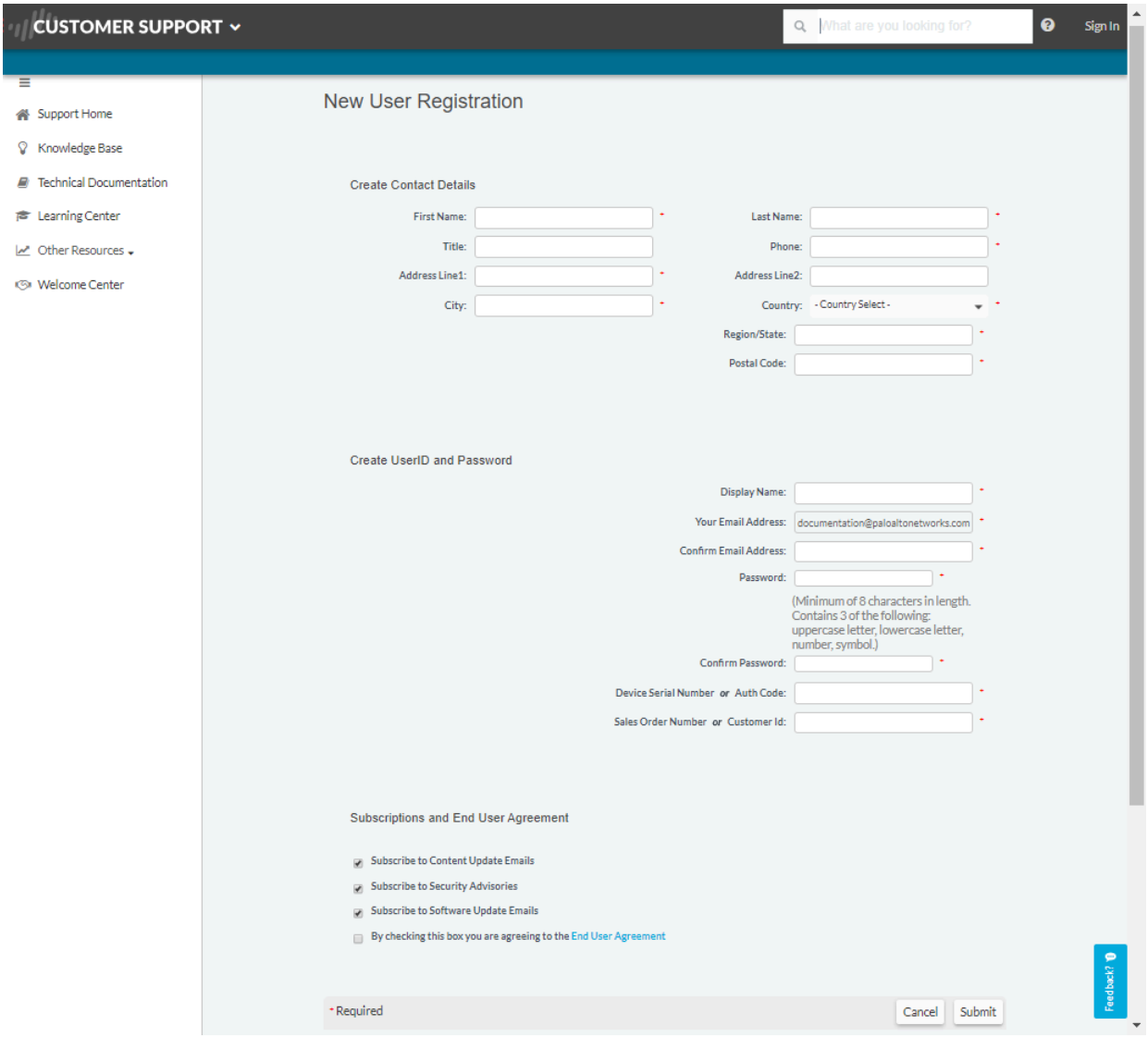

**STEP 5 |** Remplissez le formulaire d'enregistrement.

1. Entrez les coordonnées de la personne de votre organisation qui sera propriétaire de ce compte. Les champs obligatoires sont indiqués par des astérisques rouges.
2. Créez un nom d'utilisateur et un mot de passe pour le compte. Les champs obligatoires sont indiqués par des astérisques rouges.
3. Saisissez le **Device Serial Number** (Numéro de série du périphérique) ou **Auth Code** (Code d'autorisation) Panorama.
4. Saisissez votre **Sales Order Number (Numéro de commande)** ou **Customer ID (Identifiant client)**.
5. Pour vous assurer d'être toujours informé des dernières mises à jour et des avis de sécurité, **Subscribe to Content Update Emails (inscrivez-vous aux e-mails de mise à jour du contenu)**, **Subscribe to Security Advisories (inscrivez-vous aux avis de sécurité)** et

**Subscribe to Software Update Emails (abonnez-vous aux courriels de mise à jour des logiciels)**.

6. Cochez la case permettant d'accepter les conditions d'utilisation, puis cliquez sur **Submit (Soumettre)**.




# Enregistrement du pare-feu

Si vous avez déjà un compte de support client Palo Alto Networks actif, effectuez les tâches suivantes pour enregistrer votre pare-feu.

**STEP 1 |** Connectez-vous à l'interface Web du pare-feu.

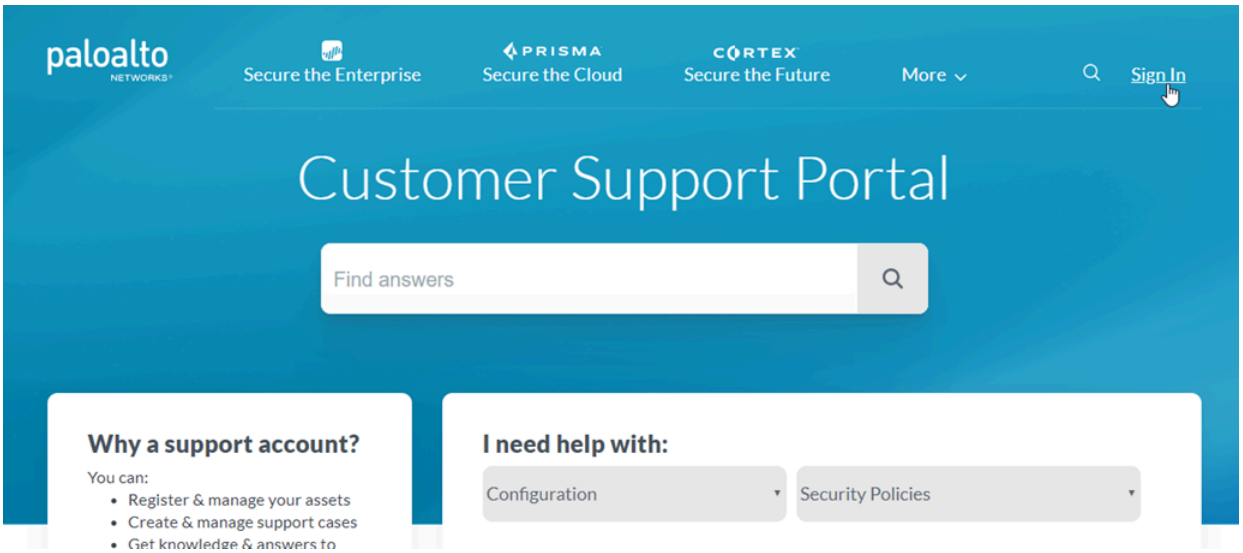
Dans votre navigateur Web, connectez-vous de manière sécurisée (HTTPS) à l'aide de la nouvelle adresse IP et du nouveau mot de passe affectés lors de la configuration initiale (https://<adresse IP>).

**STEP 2 |** Localisez votre numéro de série et copiez-le dans le Presse-papiers.

Sur le **Dashboard (tableau de bord)**, localisez votre **Serial Number (numéro de série)** dans la section Informations générales de l'écran.

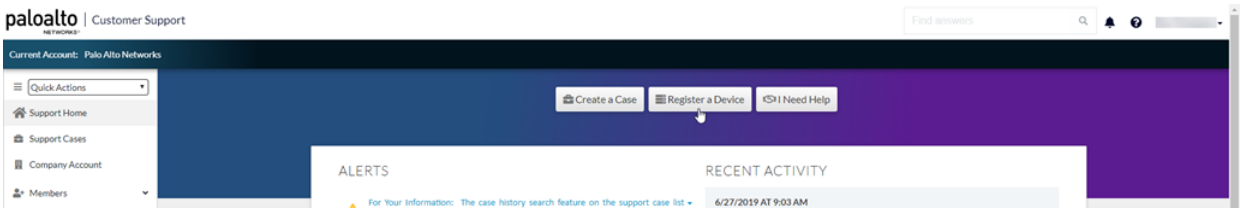
**STEP 3 |** Rendez-vous sur le portail de support client de Palo Alto Networks et, si vous n'êtes pas encore connecté, **Sign In (Ouvrez une session)** dès maintenant.



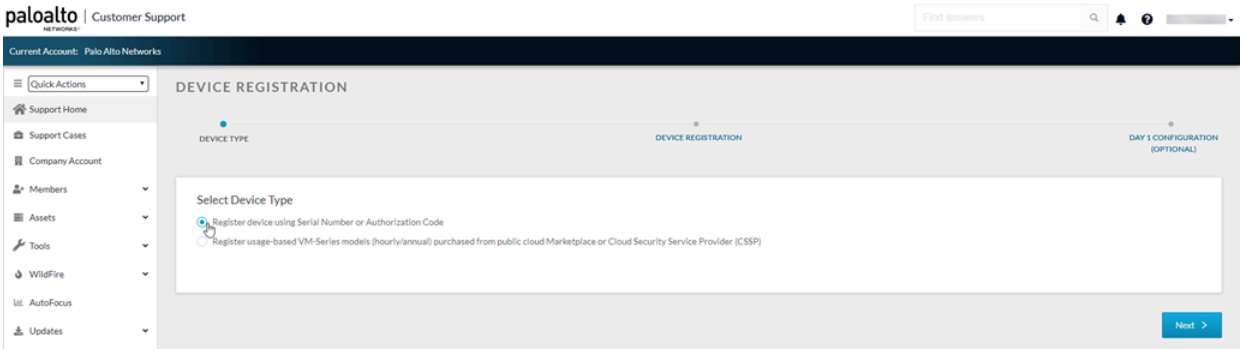

 

**STEP 4 |** Enregistrez le pare-feu.

1. Sur la page Support Home (Page d'accueil du support), cliquez sur **Register a Device (Enregistrer un périphérique)**.

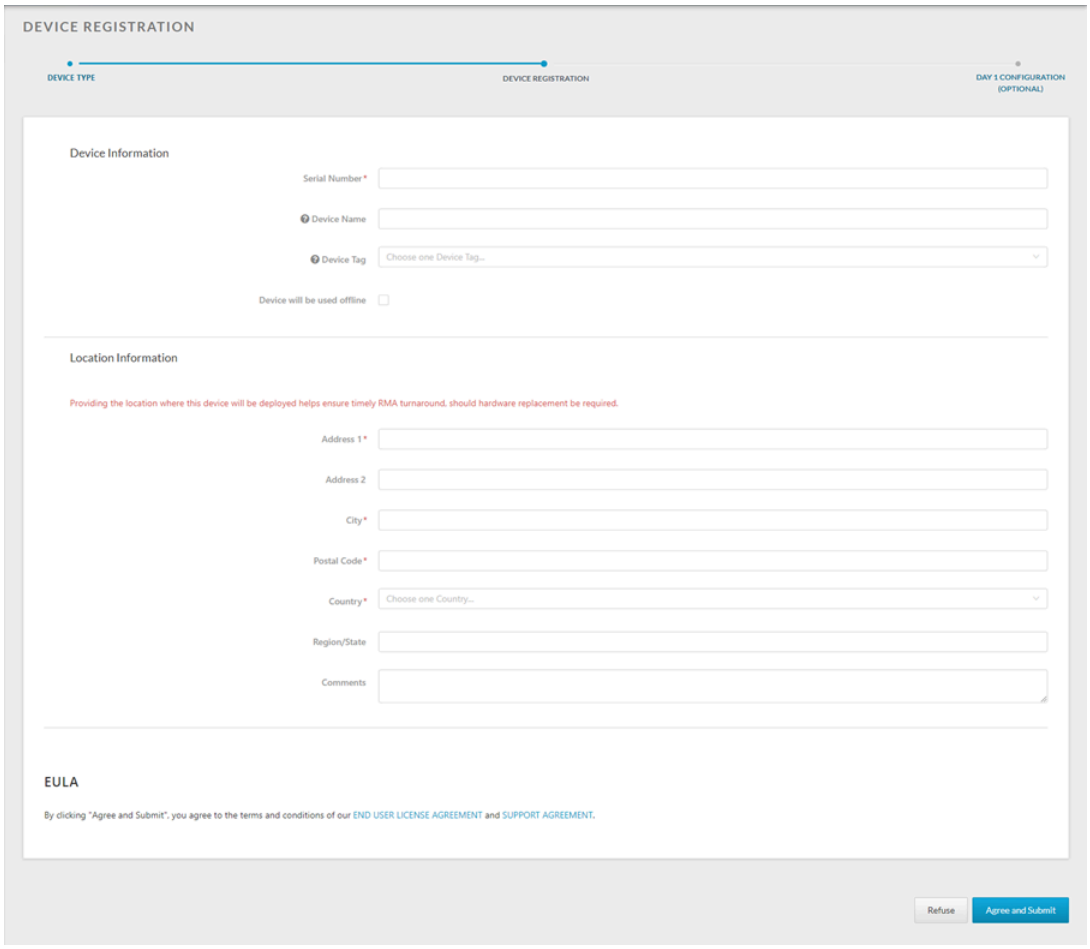



2. Sélectionnez **Register device using Serial Number or Authorization Code (Enregistrer un périphérique au moyen d'un numéro de série ou d'un code d'autorisation)** et cliquez sur **Next (Suivant)**.




3. Saisissez le **Serial Number (Numéro de série)** du pare-feu (vous pouvez le copier-coller à partir du tableau de bord du pare-feu).
4. (Facultatif) Saisissez un **Device Name (Nom du périphérique)** et une **Device Tag (Étiquette du périphérique)**.
5. (Facultatif) Si l'appareil n'est pas connecté à Internet, cochez la case **Device will be used Offline (L'appareil sera utilisé hors ligne)**, puis, dans le menu déroulant, sélectionnez la **OS Release (Version du système d'exploitation)** que vous prévoyez d'utiliser.
6. Donnez des informations sur l'endroit où vous prévoyez de déployer le pare-feu, notamment les informations **Address (Adresse)**, **City (Ville)**, **Postal Code (Code postal)** et **Country (Pays)**.
7. Lisez le contrat de licence d'utilisateur final (« CLUF ») et le contrat de soutien, puis **Agree and Submit (Accepter et soumettre)**.




Une entrée pour le pare-feu que vous venez d'enregistrer s'affiche sous **Devices (Périphériques)**.

**STEP 5 |** (Firewalls with line cards (Pare-feu avec cartes de ligne)) Pour vous assurer que vous bénéficiez de la prise en charge des cartes de ligne de votre pare-feu, assurez-vous de Enregistrez les cartes de ligne de pare-feu.

## (Facultatif) Procédez à la configuration du jour 1

Après avoir enregistré votre pare-feu, vous avez l'option d'exécuter la configuration du jour 1. L'outil de configuration du jour 1 fournit les modèles exemplaires recommandés par Palo Alto Networks que vous pouvez utiliser comme base à partir de laquelle bâtir le reste de votre configuration.

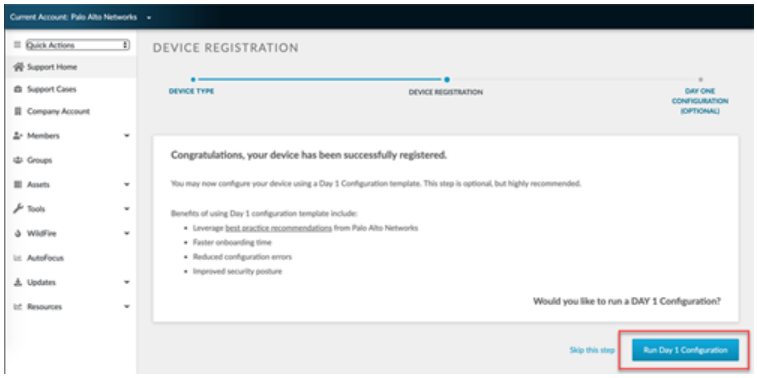
Les avantages des modèles de configuration du jour 1 comprennent :

- Des délais de mise en œuvre plus rapides
- Une réduction des erreurs de configuration
- Une amélioration de la position de sécurité

Effectuez la configuration du jour 1 en suivant les étapes indiquées ci-dessous.

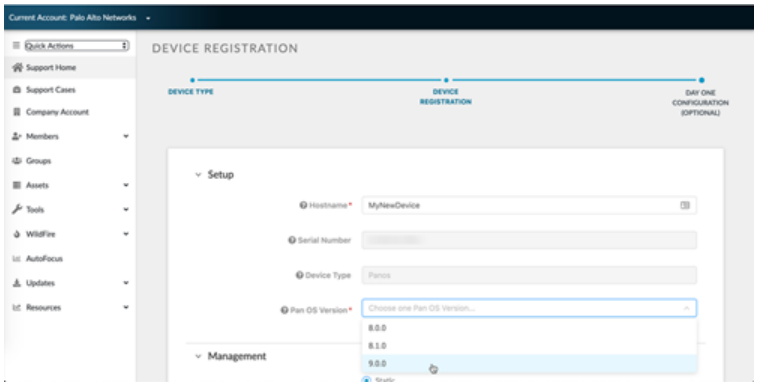
 

**STEP 1 |** À partir de la page qui s'affiche lorsque vous avez enregistré votre pare-feu, sélectionnez **Run Day 1 Configuration (Exécuter la configuration du jour 1)**.




*Si vous avez déjà enregistré votre pare-feu mais n'avez pas effectué la configuration du premier jour, vous pouvez aussi l'exécuter sur le Portail Support Client en sélectionnant* ***Tools (Outils) > Run Day 1 Configuration (Exécution la configuration du premier jour).***

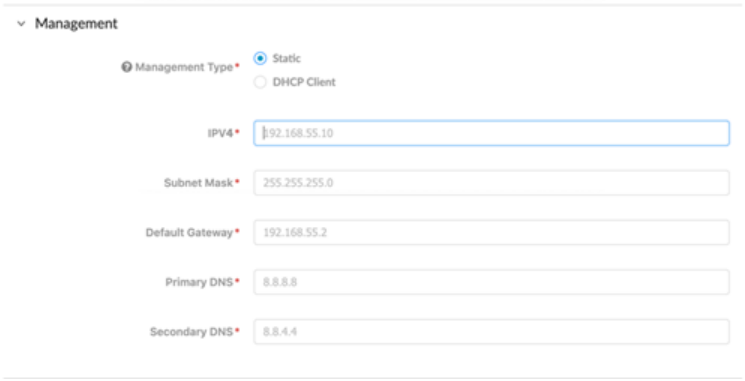
**STEP 2 |** Saisissez le **Hostname (Nom d'hôte)** et la **Pan OS Version (Version de PAN-OS)** de votre nouveau périphérique, et, éventuellement, le **Serial Number (Numéro de série)** et le **Device Type (Type de périphérique)**.



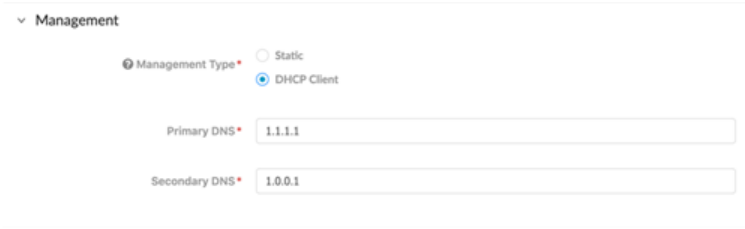

 

**STEP 3 |** Sous **Management (Gestion)**, sélectionnez **Static (Statique)** ou **DHCP Client (Client DHCP)** pour votre **Management Type (Type de gestion)**.

Si vous sélectionnez **Static (Statique)**, vous devrez remplir les champs **IPV4**,**Subnet Mask (Masque de sous-réseau)** et **Default Gateway (Passerelle par défaut)**.

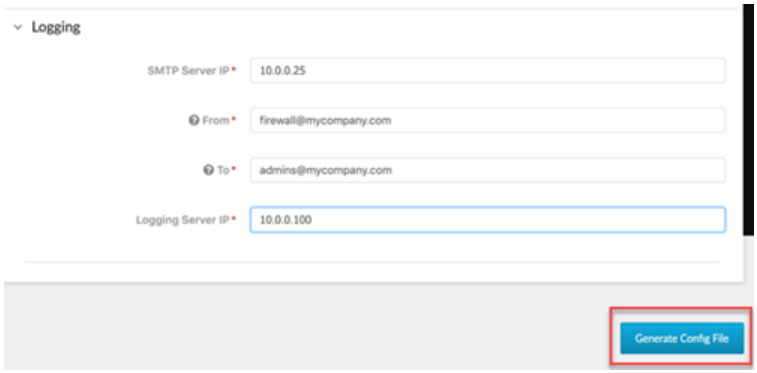



Si vous sélectionnez **DHCP Client (Client DHCP)**, vous devrez saisir le **Primary DNS (DNS principal)** et le **Secondary DNS (DNS secondaire)**. Un périphérique configuré en mode client DHCP permettra à l'interface de gestion de recevoir une adresse IP du serveur DHCP local ou il renseignera tous les paramètres s'ils sont connus.




**STEP 4 |** Remplissez tous les champs sous **Logging (Journalisation)**.

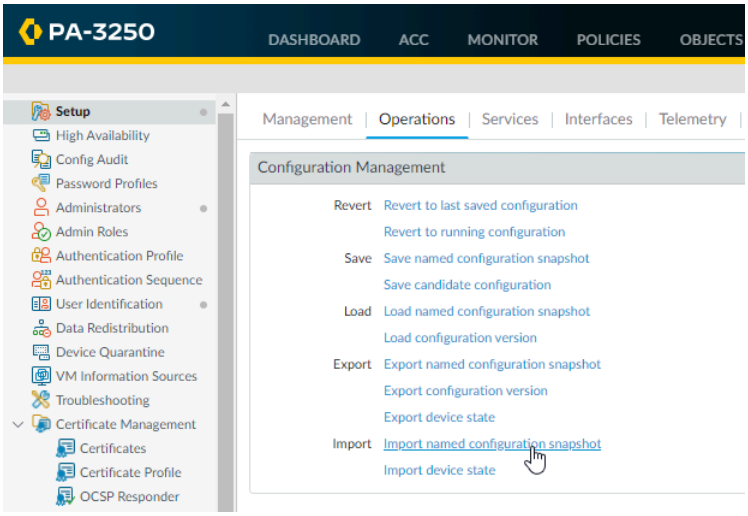
**STEP 5 |** Cliquez sur **Generate Config File (Générer le fichier de configuration)**.



**STEP 6 |** Pour importer et charger le fichier de configuration du jour 1 que vous venez de télécharger sur votre pare-feu :

1. Connectez-vous à l'interface Web de votre pare-feu.
2. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)**.
3. Cliquez sur **Import named configuration snapshot (Importer l'instantané de configuration)**.
4. Sélectionnez le fichier




# Enregistrez les cartes de ligne de pare-feu

Les pare-feux suivants utilisent des cartes de ligne qui doivent être enregistrées pour bénéficier d'une assistance en matière de dépannage et de retours :

- Pare-feu PA-7000 Series
- Pare-feu PA-5450

Si vous n'avez pas de compte d'assistance client Palo Alto Networks, créez-en un en suivant les étapes de Créer un nouveau compte de support et enregistrer un pare-feu. Revenez à ces instructions après avoir créé votre compte d'assistance client et enregistré votre pare-feu.

**STEP 1 |** Rendez-vous sur le portail de support client de Palo Alto Networks et, si vous n'êtes pas encore connecté, **Sign In (Ouvrez une session)** dès maintenant.

**STEP 2 |** Sélectionnez **Assets (Actifs)** > **Line Cards/Optics/FRUs (Cartes de ligne/optique/FRU)**.

**STEP 3 |** **Register Components (Enregistrez les composants)**.

**STEP 4 |** Entrez le numéro de commande de vente Palo Alto Networks des cartes de ligne dans le champ **Sales Order Number (Numéro de commande de vente)** pour afficher les cartes de ligne éligibles pour l'enregistrement.

**STEP 5 |** Enregistrez les cartes de ligne sur votre pare-feu en entrant son numéro de série de châssis dans le champ **Serial Number (Numéro de série)**. Les**Location information (informations de localisation)** ci-dessous se remplissent automatiquement en fonction des informations d'enregistrement de votre pare-feu.

**STEP 6 |** Cliquez sur **Agree and Submit (Accepter et soumettre)** pour accepter les conditions légales. Le système se met à jour pour afficher les cartes de ligne enregistrées sous **Assets (Actifs)** > **Line Cards/Optics/FRU (Cartes de ligne/Optique/FRU)**..

# Segmentation de votre réseau via les interfaces et les zones

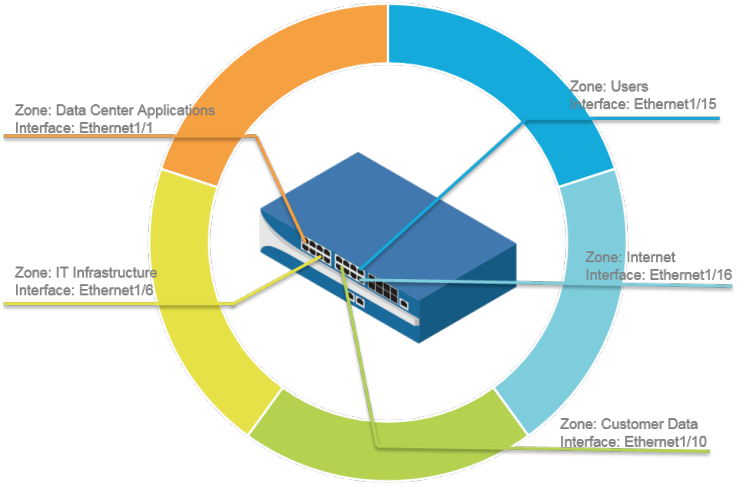
Le trafic doit traverser le pare-feu afin que ce dernier puisse le gérer et le contrôler. Le trafic entre et sort physiquement du pare-feu via les ***interfaces***. Le pare-feu détermine la manière dont il va agir sur un paquet selon qu'il corresponde ou non à une ***Règle de politique de sécurité***. À son niveau le plus basique, chaque règle de politique de sécurité doit identifier l'origine du trafic et sa destination. Sur un pare-feu Palo Alto Networks de dernière génération, les règles de politique de sécurité sont appliquées entre les zones. Une ***zone*** est un regroupement d'interfaces (physiques ou virtuelles) qui représente un segment de votre réseau qui est connecté et contrôlé par le pare-feu. Puisque le trafic ne peut circuler entre des zones que si une règle de politique de sécurité qui l'autorise a été définie, c'est votre première ligne de défense. Plus les zones que vous créez sont granulaires, meilleur sera le contrôle que vous aurez des applications et des données sensibles et plus grande sera la protection que vous aurez contre le déplacement latéral des logiciels malveillants dans votre réseau. Vous pouvez par exemple segmenter l'accès aux serveurs de base de données qui stockent les données sur les clients que vous détenez dans une zone intitulée Données clients. Vous pouvez ensuite définir des politiques de sécurité qui n'autorisent l'accès à la zone Données clients qu'à certains utilisateurs ou groupes d'utilisateurs, ce qui permet ainsi d'empêcher tout accès interne ou externe non autorisé aux données stockées dans ce segment

- Segmentation du réseau pour réduire la surface d'attaque
- Configuration des interfaces et des zones

## Segmentation du réseau pour réduire la surface d'attaque

Le diagramme suivant illustre un exemple de base de la Segmentation du réseau à l'aide de Zones. Plus vos zones (et les règles de politique de sécurité correspondantes qui autorisent la circulation du trafic entre les zones) sont granulaires, plus vous réduirez la surface d'attaque sur votre réseau. En effet, cela s'explique par le fait que le trafic peut circuler librement au sein d'une zone (trafic intra-zone), mais qu'il ne peut circuler d'une zone à l'autre (trafic inter-zone) si vous n'avez pas défini de règle de politique de sécurité qui l'autorise à le faire. De plus, une interface ne peut traiter le trafic si vous n'avez pas associé la circulation du trafic à une zone. Ainsi, en segmentant votre réseau en zones granulaires, vous avez un plus grand contrôle de l'accès aux applications et données de nature délicate et vous pouvez empêcher le trafic malveillant d'établir un canal de communication au sein de votre réseau, ce qui permet de réduire la probabilité qu'une attaque soit menée avec succès sur votre réseau.




# Configuration des interfaces et des zones

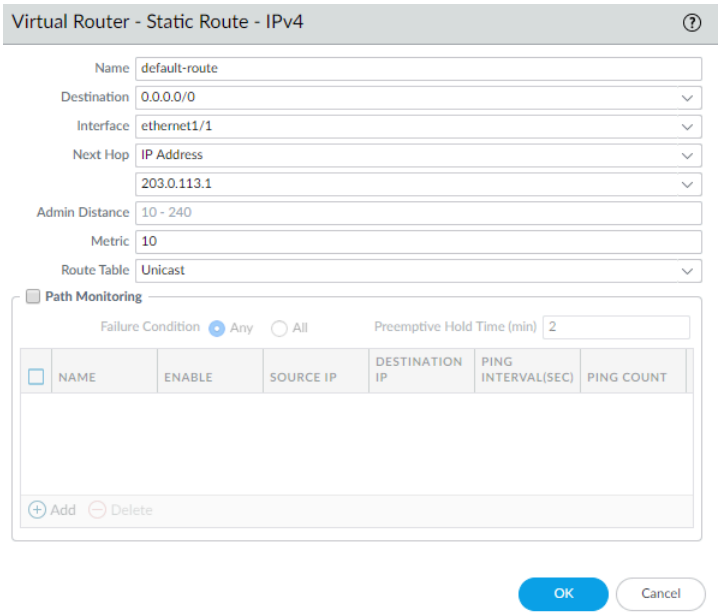
Une fois que vous avez déterminé la façon de segmenter votre réseau et les zones que vous avez besoin de créer pour y arriver (ainsi que les interfaces que vous devez mapper à chacune des zones), vous pouvez commencer à configurer les interfaces et zones de votre pare-feu. Procédez à la Configure interfaces (configuration des interfaces) du pare-feu pour qu'elles prennent en charge la topologie de chacune des sections du réseau auquel vous vous connectez. Le flux de travail suivant indique comment configurer des interfaces de Couche 3 et les associer à des zones. Pour obtenir de plus amples renseignements sur l'intégration du pare-feu à l'aide de divers types de déploiements d'interface (par exemple, des virtual wire interfaces (interfaces de câble virtuel) ou des Layer 2 interfaces (interfaces de Couche 2)), reportez-vous à la section Guide de l'administrateur de mise en réseau PAN-OS.

***Le pare-feu est préconfiguré avec une interface de câble virtuel par défaut entre les ports Ethernet 1/1 et Ethernet 1/2 (ainsi qu'une politique de sécurité et un routeur virtuel par défaut correspondants). Si vous ne prévoyez pas d'utiliser le câble virtuel par défaut, vous devez supprimer manuellement sa configuration et valider la modification avant de continuer, afin qu'elle n'interfère pas avec vos autres paramètres. Pour obtenir des instructions sur la suppression du câble virtuel par défaut, ainsi que de sa politique et de ses zones de sécurité associées, reportez-vous à l'étape 3 de la section*** Configuration d'un accès réseau pour les services externes.

**STEP 1 |** Configurez un itinéraire par défaut vers votre routeur Internet.

1. Sélectionnez **Network (Réseau)** > **Virtual Router (Routeur virtuel)**, puis cliquez sur le lien **default (par défaut)** pour ouvrir la boîte de dialogue Routeur virtuel.
2. Cliquez sur l'onglet **Static Routes (Itinéraires statiques)**, puis sur **Add (Ajouter)**. Donnez un **Name (Nom)** à l'itinéraire et saisissez l'itinéraire dans le champ **Destination (Destination)** (par exemple : 0.0.0.0/0).
3. Cliquez sur le bouton radio **IP Address (Adresse IP)** dans le champ **Next Hop (Saut suivant)**, puis saisissez l'adresse IP et le masque de réseau de votre passerelle Internet (par exemple : 203.0.113.1).




4. Cliquez deux fois sur **OK (OK)** pour enregistrer la configuration du routeur virtuel.

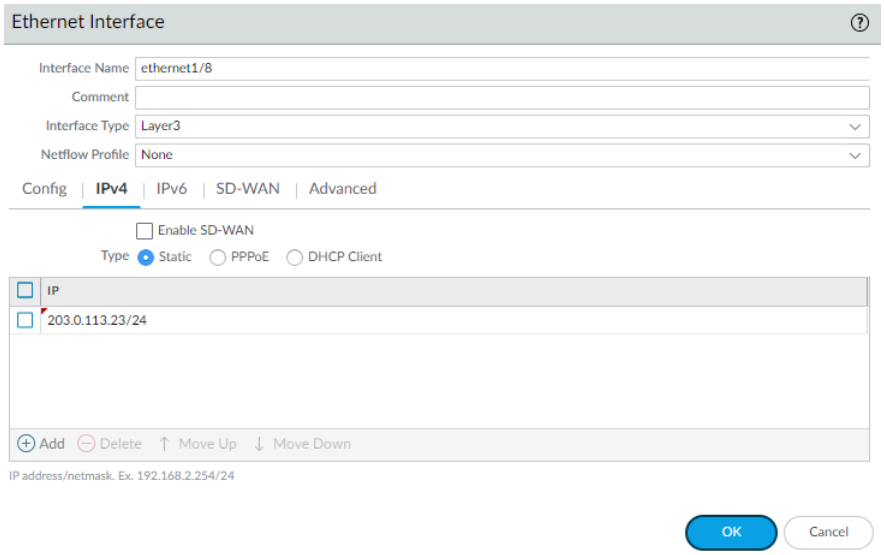
**STEP 2 |** Configurez l'interface externe (l'interface qui se connecte à Internet).

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)**, puis choisissez l'interface que vous voulez configurer. Dans cet exemple, nous configurons Ethernet1/8 en tant qu'interface externe.
2. Sélectionnez l'**Interface Type (Type d'interface)**. Bien que votre choix dépende ici de la topologie de l'interface, cet exemple décrit les différentes étapes pour la **Layer3 (Couche 3)**.
3. Dans l'onglet **Config (Configuration)**, sélectionnez **New Zone (Nouvelle zone)** dans la liste déroulante **Security Zone (Zone de sécurité)**. Dans la boîte de dialogue Zone (Zone),

donnez un **Name (Nom)** à la nouvelle zone, par exemple : Internet, puis cliquez sur **OK (OK)**.

4. Dans la liste déroulante **Virtual Router (Routeur virtuel)**, sélectionnez **default (Par défaut)**.
5. Pour assigner une adresse IP à l'interface, cliquez sur l'onglet **IPv4**, puis sur **Add (Ajouter)** dans la section IP et saisissez l'adresse IP, ainsi que le masque réseau à assigner à l'interface, par exemple : 203.0.113.23/24.




6. Pour envoyer des requêtes ping à l'interface, sélectionnez **Advanced (Avancé)** > **Other Info (Autres informations)**, développez la liste déroulante **Management Profile (Profil de gestion)** et sélectionnez **New Management Profile (Nouveau profil de gestion)**. Donnez un **Name (Nom)** au profil, sélectionnez **Ping (Ping)** puis cliquez sur **OK (OK)**.
7. Pour enregistrer la configuration de l'interface, cliquez sur **OK**.

**STEP 3 |** Configurez l'interface qui se connecte à votre réseau interne.

*Dans cet exemple, l'interface se connecte à un segment de réseau qui utilise des adresses IP privées. Étant donné que les adresses IP privées ne peuvent pas être acheminées en externe, vous devez configurer* NAT.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** et choisissez l'interface que vous voulez configurer. Dans cet exemple, nous configurons Ethernet1/15 en tant qu'interface interne à laquelle nos utilisateurs se connectent.
2. Sélectionnez **Layer3 (Couche 3)** comme **Interface Type (Type de liaison)**.
3. Dans l'onglet **Config (Configuration)**, développez la liste déroulante **Security Zone (Zone de sécurité)** et sélectionnez **New Zone (Nouvelle zone)**. Dans la boîte de dialogue Zone

(Zone), donnez un **Name (Nom)** à la nouvelle zone, par exemple : Utilisateurs, puis cliquez sur **OK (OK)**.

4. Sélectionnez le même routeur virtuel que celui que vous avez utilisé précédemment, par défaut dans cet exemple.
5. Pour assigner une adresse IP à l'interface, cliquez sur l'onglet **IPv4**, puis sur **Add (Ajouter)** dans la section IP et saisissez l'adresse IP, ainsi que le masque réseau à assigner à l'interface, par exemple : 192.168.1.4/24.
6. Pour envoyer des requêtes ping à l'interface, sélectionnez le profil de gestion que vous venez de créer.
7. Pour enregistrer la configuration de l'interface, cliquez sur **OK**.

**STEP 4 |** Configurez l'interface qui se connecte à vos applications de centres de données.

***Veillez à définir des** zones granulaires **pour empêcher tout accès non autorisé à des applications ou des données sensibles et éliminer la possibilité que des logiciels malveillants se déplacent latéralement dans votre centre de données.***

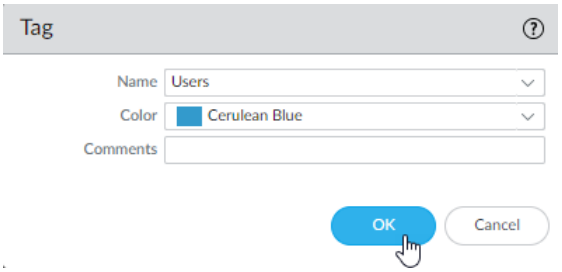
1. Sélectionnez l'interface que vous voulez configurer.
2. Sélectionnez **Layer3 (Couche 3)** dans la liste déroulante **Interface Type (Type d'interface)**. Dans cet exemple, nous configurons Ethernet1/1 en tant qu'interface qui fournit un accès aux applications de centres de données.
3. Dans l'onglet **Config (Configuration)**, développez la liste déroulante **Security Zone (Zone de sécurité)** et sélectionnez **New Zone (Nouvelle zone)**. Dans la boîte de dialogue Zone (Zone), donnez un **Name (Nom)** à la nouvelle zone, par exemple : Applications de centres de données, puis cliquez sur **OK (OK)**.
4. Sélectionnez le même routeur virtuel que celui que vous avez utilisé précédemment, par défaut dans cet exemple.
5. Pour affecter une adresse IP à l'interface, cliquez sur l'onglet **IPv4**, puis sur **Add (Ajouter)** dans la section IP et saisissez l'adresse IP, ainsi que le masque réseau à affecter à l'interface, par exemple : 10.1.1.1/24.
6. Pour envoyer des requêtes ping à l'interface, sélectionnez le profil de gestion que vous avez créé.
7. Pour enregistrer la configuration de l'interface, cliquez sur **OK**.

**STEP 5 |** (Facultatif) Créez des étiquettes pour chaque zone.

Les étiquettes vous permettent d'analyser les règles de politique visuellement.

1. Sélectionnez **Objects (Objets)** > **Tags (Étiquettes)**, puis **Add (Ajouter)**.
2. Sélectionnez un **Name (Nom)** de zone.
3. Sélectionnez une **Color (Couleur)** d'étiquette, puis cliquez sur **OK (OK)**.




**STEP 6 |** Enregistrez la configuration de l'interface.

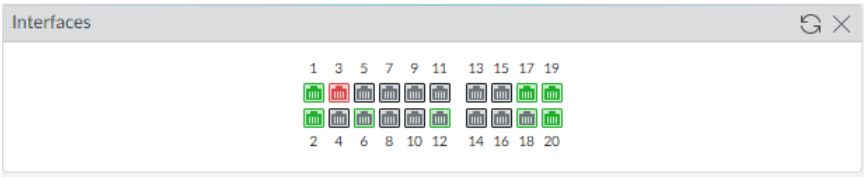
Cliquez sur **Commit (Valider)**.

**STEP 7 |** Câblez le pare-feu.

Connectez les câbles directs des interfaces que vous avez configurées au commutateur ou au routeur correspondant sur chaque segment de réseau.

**STEP 8 |** Vérifiez que les interfaces sont actives.

Sélectionnez **Dashboard (Tableau de bord)** et vérifiez que les interfaces que vous avez configurées s'affichent en vert dans le widget Interfaces.



# Configuration d'une politique de sécurité de base

Maintenant que vous avez défini des zones et que vous les avez associées aux interfaces, vous être prêt à commencer à créer votre Politique de sécurité. Le pare-feu n'autorisera pas la circulation du trafic d'une zone à l'autre si aucune règle de politique de sécurité l'autorisant n'est définie. Lorsqu'un paquet entre dans l'interface d'un pare-feu, le pare-feu met les attributs du paquet en correspondance avec les règles de politique de sécurité afin de déterminer si la session doit être bloquée ou autorisée en fonction des attributs comme la zone de sécurité source et de destination, l'adresse IP source et de destination, l'application, l'utilisateur et le service. Le pare-feu évalue le trafic entrant en le comparant à la base de règles de politique de sécurité de gauche à droite et de haut en bas ; il entreprend ensuite l'action précisée dans la première règle de sécurité correspondante (par exemple, autoriser, refuser ou abandonner le paquet). Vous devez ainsi placer les règles au sein de votre base de règles de politique de sécurité de sorte que les règles plus spécifiques se trouvent au début de la base de règle et que les règles plus générales se trouvent au bas. Vous vous assurerez ainsi que le pare-feu applique la politique comme prévu.

Même si une règle de politique de sécurité autorise un paquet, cela ne signifie pas que le trafic est exempt de menaces. Pour permettre au pare-feu d'analyser tout le trafic autorisé basé sur une règle de politique de sécurité, vous devez associer des Profils de Sécurité - incluant le filtrage des URL, l'antivirus, l'antispyware, le blocage de fichier, ainsi que l'analyse WildFire - à chaque règle (les profils que vous pouvez utiliser dépendent des Abonnements auxquels vous avez souscrit). Lorsque vous créez votre politique de sécurité de base, utilisez les profils de sécurité prédéfinis pour vous assurer que le trafic que vous autorisez à l'intérieur de votre réseau est analysé pour détecter les menaces. Vous pouvez personnaliser ces profils plus tard selon les besoins de votre environnement.

Utilisez le processus de travail suivant pour configurer une politique de sécurité de base qui autorise un accès à l'infrastructure du réseau, aux applications du centre de données, et à internet. Cela vous permet d'avoir un pare-feu opérationnel afin de pouvoir confirmer que vous l'avez configuré avec succès. Cependant, cette politique initiale n'est pas assez complète pour protéger votre réseau. Après avoir confirmé que votre pare-feu est configuré avec succès et intégré à votre réseau, poursuivez en créant une Politique de sécurité des passerelles Internet exemplaire qui permet un accès sécurisé aux applications tout en protégeant votre réseau des attaques.

**STEP 1 |** (Facultatif) Supprimez la règle de politique de sécurité par défaut.

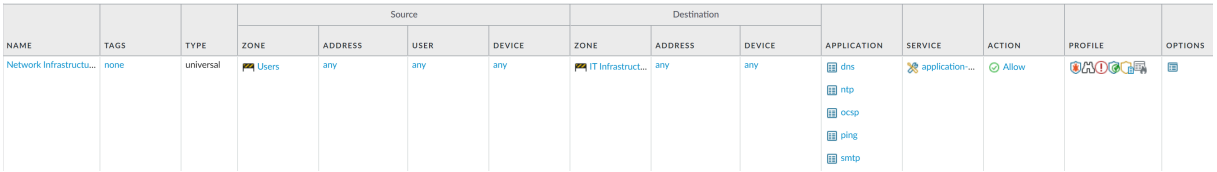
Par défaut, le pare-feu inclut une règle de politique de sécurité nommée ***règle1*** qui autorise tout trafic issu d'une zone de confiance vers une zone non approuvée. Vous pouvez supprimer cette règle ou la modifier afin qu'elle reflète votre convention de dénomination de zone.

**STEP 2 |** Autorisez l'accès aux ressources de votre infrastructure de réseau.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et cliquez sur **Add (Ajouter)**.
2. Dans l'onglet **General (Général)**, donnez un **Name (Nom)** descriptif à la règle.
3. Dans l'onglet **Source**, réglez la **Source Zone (Zone Source)** sur **Users (Utilisateurs)**.
4. Dans l'onglet **Destination**, réglez la **Destination Zone (Zone de destination)** sur **IT Infrastructure (Infrastructure Informatique)**.

   *Il est recommandé d'utiliser des objets d'adresse dans le champ **Destination Address (Adresse de destination)** pour autoriser l'accès uniquement à des serveurs ou des groupes de serveurs donnés, particulièrement pour des services tels que DNS et SMTP, qui sont fréquemment exploités. En restreignant les utilisateurs à des adresses de serveurs de destination, vous pouvez prévenir l'exfiltration de données et empêcher le trafic de commande et de contrôle d'établir une communication grâce à des techniques comme la tunnellisation DNS.*
5. Dans l'onglet **Applications**, **Add (Ajoutez)** les applications qui correspondent aux services réseau que vous voulez autoriser en toute sécurité. Par exemple, sélectionnez **dns**, **ntp**, **ocsp**, **ping** et **smtp**.
6. Dans l'onglet **Service/ URL Category (Catégorie de service/d'URL)**, définissez le **Service** sur **application-default (par défaut de l'application)**.
7. Dans l'onglet **Actions**, définissez **Action Setting (Paramètre d'action)** sur **Allow (Autoriser)**.
8. Sélectionnez **Profiles (Profils)** comme **Profile Type (Type de Profil)** et sélectionnez les profils de sécurité suivants à associer à la règle de politique :
   - Pour **Antivirus**, sélectionnez **default (par défaut)**.
   - Pour **Vulnerability Protection (Protection contre les vulnérabilités)**, sélectionnez **strict**.
   - Pour **Anti-Spyware (Antispyware)**, sélectionnez **strict**.
   - Pour **URL Filtering (Filtrage des URL)**, sélectionnez **default (par défaut)**.
   - Pour **File Blocking (Blocage de fichiers)**, sélectionnez **basic file blocking (blocage de fichiers de base)**.
   - Pour l'**WildFire Analysis (Analyse Wildfire)**, sélectionnez **default (par défaut)**.
9. Vérifiez que **Log at Session End (Journalisation en fin de session)** est activé. Seul le trafic qui correspond à une règle de politique de sécurité sera consigné.
10. Cliquez sur **OK**.

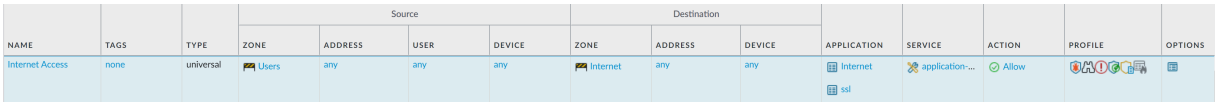


**STEP 3 |** Activez l'accès aux applications Internet générales.

*Il s'agit d'une règle temporaire qui vous permet de recueillir des informations sur le trafic sur votre réseau. Lorsque vous aurez une idée plus précise des applications auxquelles vos utilisateurs doivent avoir accès, vous pourrez prendre des décisions éclairées sur les applications qui doivent être autorisées et créer des règles plus granulaires fondées sur les applications pour chaque groupe d'utilisateurs.*

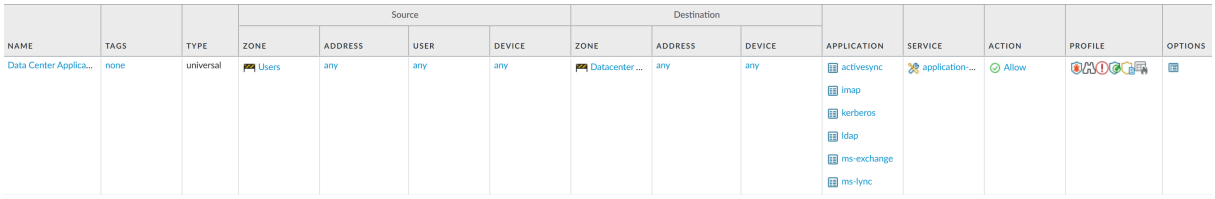
1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis **Add (Ajoutez)** une règle.
2. Dans l'onglet **General (Général)**, donnez un **Name (Nom)** descriptif à la règle.
3. Dans l'onglet **Source**, réglez la **Source Zone (Zone Source)** sur **Users (Utilisateurs)**.
4. Dans l'onglet **Destination**, réglez la **Destination Zone (Zone de destination)** sur **Internet**.
5. Dans l'onglet **Applications**, **Add (Ajoutez)** un **Application Filter (Filtre d'application)** et saisissez un **Name (Nom)**. Pour autoriser l'accès en toute sécurité aux applications Web légitimes, dans le filtre d'applications, définissez la **Category (Catégorie)** sur **general-internet (Internet grand public)**, puis cliquez sur **OK**. Pour autoriser l'accès aux sites chiffrés, **Add (Ajoutez)** l'application **ssl**.
6. Dans l'onglet **Service/ URL Category (Catégorie de service/d'URL)**, définissez le **Service** sur **application-default (par défaut de l'application)**.
7. Dans l'onglet **Actions**, définissez **Action Setting (Paramètre d'action)** sur **Allow (Autoriser)**.
8. Sélectionnez **Profiles (Profils)** comme **Profile Type (Type de Profil)** et sélectionnez les profils de sécurité suivants à associer à la règle de politique :
   - Pour **Antivirus**, sélectionnez **default (par défaut)**.
   - Pour **Vulnerability Protection (Protection contre les vulnérabilités)**, sélectionnez **strict**.
   - Pour **Anti-Spyware (Antispyware)**, sélectionnez **strict**.
   - Pour **URL Filtering (Filtrage des URL)**, sélectionnez **default (par défaut)**.
   - Pour **File Blocking (Blocage de fichiers)**, sélectionnez **strict file blocking (blocage de fichiers strict)**.
   - Pour l'**WildFire Analysis (Analyse Wildfire)**, sélectionnez **default (par défaut)**.
9. Vérifiez que **Log at Session End (Journalisation en fin de session)** est activé. Seul le trafic qui correspond à une règle de sécurité sera consigné.
10. Cliquez sur **OK**.



**STEP 4 |** Activez l'accès aux applications du centre de données.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis **Add (Ajoutez)** une règle.
2. Dans l'onglet **General (Général)**, donnez un **Name (Nom)** descriptif à la règle.
3. Dans l'onglet **Source**, réglez la **Source Zone (Zone Source)** sur **Users (Utilisateurs)**.
4. Dans l'onglet **Destination**, réglez la **Destination Zone (Zone de destination)** sur **Data Center Applications (Applications du centre de données)**.
5. Dans l'onglet **Applications**, **Add (Ajoutez)** les applications qui correspondent aux services réseau que vous voulez autoriser en toute sécurité. Par exemple, sélectionnez **activesync**, **imap**, **kerberos**, **ldap**, **ms-exchange**, et **ms-lync**.
6. Dans l'onglet **Service/ URL Category (Catégorie de service/d'URL)**, définissez le **Service** sur **application-default (par défaut de l'application)**.
7. Dans l'onglet **Actions**, définissez **Action Setting (Paramètre d'action)** sur **Allow (Autoriser)**.
8. Sélectionnez **Profiles (Profils)** comme **Profile Type (Type de Profil)** et sélectionnez les profils de sécurité suivants à associer à la règle de politique :
   - Pour **Antivirus**, sélectionnez **default (par défaut)**.
   - Pour **Vulnerability Protection (Protection contre les vulnérabilités)**, sélectionnez **strict**
   - Pour **Anti-Spyware (Antispyware)**, sélectionnez **strict**
   - Pour **URL Filtering (Filtrage des URL)**, sélectionnez **default (par défaut)**
   - Pour **File Blocking (Blocage de fichiers)**, sélectionnez **basic file blocking (blocage de fichiers de base)**
   - Pour l'**WildFire Analysis (Analyse Wildfire)**, sélectionnez **default (par défaut)**
9. Vérifiez que **Log at Session End (Journalisation en fin de session)** est activé. Seul le trafic qui correspond à une règle de sécurité sera consigné.
10. Cliquez sur **OK**.




**STEP 5 |** Enregistrez vos règles de politique dans la configuration active sur le pare-feu.

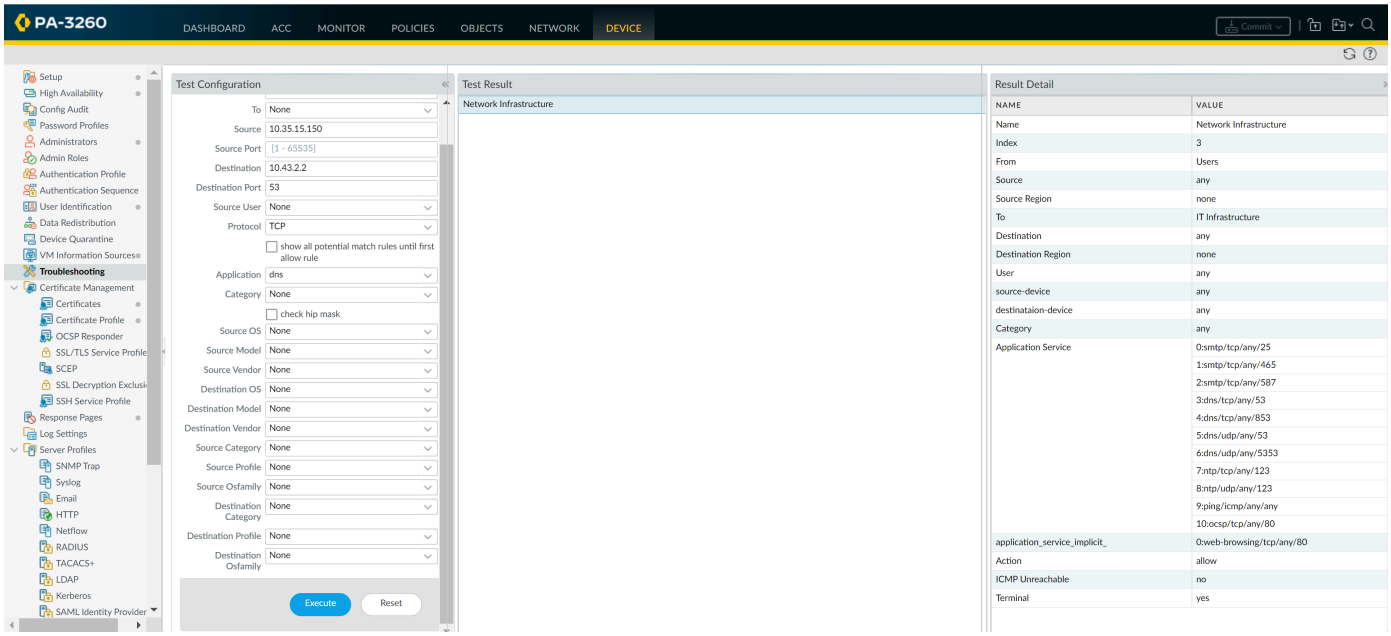
Cliquez sur **Commit (Valider)**.

**STEP 6 |** Pour vérifier que vous avez correctement paramétré vos politiques de base, testez si vos règles de politique de sécurité sont en cours d'évaluation et déterminez la règle de politique de sécurité qui s'applique à un flux de trafic.

Par exemple, pour vérifier la règle de politique qui sera appliquée à un serveur dans la zone utilisateur avec l'adresse IP 10.35.14.150 lorsqu'il enverra une requête DNS au serveur DNS dans le centre de données :

1. Sélectionnez **Device (Périphérique)** > **Troubleshooting (Résolution des problèmes)**, puis sélectionnez **Security Policy Match (Correspondance de la politique de sécurité)** (**Select Test [Sélectionner le test]**).
2. Saisissez les adresses IP **Source** et de **Destination**.
3. Saisissez le **Protocol (Protocole)**.
4. Sélectionnez **dns** (**Application**).
5. **Execute (Exécutez)** le test de correspondance de la politique de sécurité.



# Évaluation du trafic réseau

Maintenant que vous disposez d'une politique de sécurité de base, vous pouvez passer en revue les statistiques et les données figurant dans le Application Command Center (Centre de commande de l'application ; ACC), les journaux de trafic et les journaux de menaces afin d'observer les tendances sur votre réseau. Servez-vous de cette information pour identifier les emplacements où vous devez créer des règles de politique de sécurité plus granulaires.

- Utilisation du centre de commande de l'application et Utilisation du moteur de corrélation automatique.

  Dans ACC, passez en revue les applications les plus utilisées et les applications présentant des risques élevés dans votre réseau. L'ACC récapitule sous forme graphique les informations du journal afin de mettre en évidence les applications traversant le réseau, la personne qui les utilise (avec User-ID activé) et l'éventuel impact sur la sécurité du contenu afin de vous aider à identifier ce qui se passe sur le réseau en temps réel. Vous pouvez ensuite utiliser ces informations pour créer des règles de politique de sécurité adéquates qui bloquent des applications indésirables, tout en autorisant et en activant des applications de manière sécurisée.

  Le widget Hôtes compromis, dans **ACC (ACC)** > **Threat Activity (Activité des menaces)**, affiche les hôtes susceptibles d'être compromis sur votre réseau et dans les journaux présente les preuves qui corroborent les événements.

- Déterminez les mises à jour/modifications qui sont requises pour les règles de politique de sécurité de votre réseau et implémentez ces modifications.

  Par exemple :

  - Évaluez si le contenu Web doit être autorisé en fonction du planning, des utilisateurs ou des groupes.
  - Autorisez ou contrôlez certaines applications ou fonctions au sein d'une application.
  - Décryptez ou inspectez le contenu.
  - Autorisez, mais analysez les menaces et les exploitations.

  Pour obtenir de plus amples renseignements sur la façon de préciser vos politiques de sécurité et l'association de profils de sécurité personnalisés, consultez les sections qui portent sur la Création d'une règle de politique de sécurité et sur les Profils de sécurité.

- Affichage des journaux.

  Plus particulièrement, affichez le trafic et les journaux de menaces (**Monitor (Surveillance)** > **Logs (Journaux)**).

  *Les journaux de trafic dépendent de la manière dont vos politiques de sécurité sont définies et paramétrées pour consigner le trafic. Toutefois, le widget Application Usage (Utilisation de l'application) de l'onglet **ACC (ACC)** enregistre les applications et les statistiques qu'elle que soit la configuration des politiques ; il affiche l'ensemble du trafic autorisé sur votre réseau. Il inclut donc le trafic inter-zone autorisé par la politique et le même trafic de zone qui est autorisé implicitement.*

- Configuration de quotas de stockage et de périodes d'expiration des journaux.

  Passez en revue le récapitulatif des données de renseignements d'AutoFocus des artefacts présents dans vos journaux. Un ***artefact*** est un élément, un bien, une activité ou un comportement associé aux événements de connexion qui se sont produits sur le pare-feu. Le récapitulatif révèle le nombre de sessions et les échantillons dans lesquels WildFire a détecté l'artefact. Servez-vous des verdicts de WildFire (bénin, indésirable, malveillant) et des étiquettes de correspondance AutoFocus pour trouver les risques éventuels qui sont présents sur votre réseau.

  ***Les étiquettes AutoFocus qui ont été crées par l'Unité 42, l' équipe de renseignements sur les menaces de Palo Alto Networks, attirent l'attention sur les menaces et les campagnes d'attaque ciblées et sophistiquées sur votre réseau.***

  À partir du récapitulatif des données de renseignements d'AutoFocus, vous pouvez lancer une recherche d'artefacts dans AutoFocus et évaluer leur omniprésence au sein de votre réseau ou du secteur, ou à plus grande échelle.

- Surveillance de l'activité Web des utilisateurs du réseau.

  Passez en revue les journaux de filtrage des URL à analyser par le biais d'alertes et de catégories/URL refusées. Des journaux d'URL sont générés lorsqu'un trafic correspond à une règle de sécurité à laquelle un profil de filtrage des URL avec une action d'alerte, de maintien, de forçage ou de blocage est associé.

# Activation du transfert WildFire gratuit

WildFire un environnement d'exécution virtuel basé sur le cloud qui analyse et exécute des échantillons inconnus (fichiers et liens contenus dans les courriers électroniques) et détermine si les échantillons sont malveillants, indésirables ou bénins ou s'il s'agit d'hameçonnage. Lorsque WildFire est activé, un pare-feu Palo Alto Networks peut transmettre des échantillons inconnus à WildFire à des fins d'analyse. Pour les logiciels malveillants récemment découverts, WildFire génère une signature pour détecter le logiciel malveillant, qui est mise à disposition pour être récupérée en temps réel pour tous les pare-feux ayant un abonnement WildFire actif. Tous les pare-feu Palo Alto Networks de nouvelle génération peuvent ainsi détecter et bloquer les logiciels malveillants détectés par un seul pare-feu. Les signatures antivirus correspondent souvent à plusieurs variantes de la même famille de logiciels malveillants et, par le fait même, bloquent de nouvelles variantes de logiciels malveillants que le pare-feu n'a jamais vues. L'équipe spécialisée dans la recherche des menaces de Palo Alto Networks se sert des renseignements sur les menaces recueillis des variantes des logiciels malveillants pour bloquer des adresses IP, des domaines et des URL malveillants.

Un service WildFire de base est inclus dans le pare-feu nouvelle génération de Palo Alto Networks et ne nécessite aucun abonnement WildFire. Avec de service de base, vous pouvez activer le pare-feu pour qu'il transfère les fichiers PE (Portable Executable/exécutable portable). De plus, si vous ne disposez d'aucun abonnement WildFire, mais que vous avez un abonnement de prévention des menaces, vous pouvez recevoir les signatures pour les logiciels malveillants que WildFire identifie aux 24 à 48 heures (dans le cadre des mises à jour antivirus).

Au-delà du service WildFire de base, un abonnement WildFire est nécessaire pour que le pare-feu :

- Obtenez les dernières signatures WildFire en temps réel.
- Empêchez les exécutables portables, les scripts PowerShell malveillants et les fichiers ELF d'entrer sur votre réseau en temps réel en utilisant WildFire Inline ML.
- Transfère les types de fichiers avancés et les liens d'e-mail pour analyse.
- Utilise l'API WildFire.
- Utilise un appareil WildFire pour héberger un cloud WildFire privé ou un cloud WildFire hybride.

Si vous avez un abonnement WildFire, n'attendez plus et commencez à utiliser WildFire pour tirer le meilleur profit de votre abonnement. Autrement, suivez les étapes suivantes pour activer le transfert WildFire de base :

**STEP 1 |** Confirmez que votre pare-feu est enregistré et que vous disposez d'un compte de support valide, ainsi que de tout abonnement requis.

1. Connectez-vous au portail de support client de Palo Alto Networks et, dans le panneau de navigation de gauche, sélectionnez **Assets (Ressources)** > **Devices (Périphériques)**.
2. Vérifiez que le pare-feu est disponible. S'il n'est pas indiqué, sélectionnez **Register New Device (Enregistrer un nouveau périphérique)** et passez à l'enregistrement du pare-feu.
3. (Facultatif) Si vous avez un abonnement Prévention des menaces, assurez-vous de procéder à l'Activation des licences d'abonnement.

**STEP 2 |** Connectez-vous au pare-feu et configurez les paramètres de transfert WildFire.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **WildFire (WildFire)** et modifiez les General Settings (Paramètres généraux).
2. Configurez le champ **WildFire Public Cloud (Cloud WildFire public)** pour qu'il transfère des fichiers vers le cloud global de WildFire (U.S.) à l'adresse : **`wildfire.paloaltonetworks.com`**.

   *Vous pouvez également transférer les fichiers vers un cloud régional Wildfire ou un cloud privé selon votre emplacement et les exigences de votre organisation.*
3. Passez en revue les **File Size Limits (Limites de taille de fichier)** des fichiers PE que le pare-feu transfère à WildFire à des fins d'analyse. Définissez la **Size Limit (Limite de taille)** des fichiers PE que le pare-feu peut transférer à la limite maximale disponible, fixée à 10 Mo.

   *Parmi les recommandations WildFire, définissez la **Size Limit (Limite de taille)** des fichiers PE à la limite maximale disponible, soit 10 Mo.*
4. Cliquez sur **OK** pour enregistrer vos modifications.

**STEP 3 |** Permettez au pare-feu de transférer les fichiers PE aux fins d'analyse.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **WildFire Analysis (Analyse WildFire)** et **Add (Ajoutez)** une nouvelle règle de profil.
2. Donnez un **Name (Nom)** à la nouvelle règle de profil.
3. **Add (Ajoutez)** une règle de transfert et donnez-lui un **Name (Nom)**.
4. Dans la colonne **File Types (Types de fichier)**, ajoutez les fichiers **pe (pe)** à la règle de transfert.
5. Dans la colonne **Analysis (Analyse)**, sélectionnez **public-cloud (cloud public)** pour transférer les fichiers PE au cloud WildFire public.
6. Cliquez sur **OK**.

**STEP 4 |** Appliquez le nouveau profil d'analyse WildFire au trafic que le pare-feu autorise.

1. Sélectionnez **Policies (Policies)** > **Security (Sécurité)**, puis choisissez une politique existante ou créez une nouvelle politique, comme décrit dans la section Configuration d'une politique de sécurité de base.
2. Sélectionnez **Actions (Actions)** et, dans la section Profile Settings (Paramètre de profil), définissez le **Profile Type (Type de profil** sur **Profiles (Profils)**.
3. Sélectionnez le profil d'**WildFire Analysis (Analyse WildFire)** que vous venez de créer pour appliquer cette règle de profil à tout le trafic autorisé par cette politique.
4. Cliquez sur **OK**.

**STEP 5 |** Activez le pare-feu pour qu'il transfère le trafic décrypté pour analyse par WildFire.

**STEP 6 |** Passez en revue les recommandations WildFire et appliquez-les pour vous assurer de tirer le maximum de la détection WildFire et de ses fonctionnalités de prévention.

**STEP 7 |** **Commit (Validez)** les mises à jour apportées à la configuration.

**STEP 8 |** Vérifiez que le pare-feu transfère bien les fichiers PE vers le cloud WildFire public.

Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **WildFire Submissions (Envois WildFire)** pour afficher les entrées de journal correspondant aux fichiers PE que le pare-feu a envoyés pour analyse WildFire. La colonne Verdict indique si WildFire a déterminé que le fichier PE était malveillant, indésirable ou bénin. (WildFire n'affecte le verdict d'hameçonnage qu'aux liens contenus dans des messages électroniques). La colonne Action (Action) indique si le pare-feu a autorisé ou bloqué l'échantillon. La colonne Gravité indique quelle est l'ampleur de la menace qu'un échantillon présente pour une organisation au moyen des valeurs suivantes : critique, élevée, moyenne, faible, informations.

**STEP 9 |** (Abonnement de prévention des menaces uniquement) Si vous avez un abonnement de prévention des menaces, mais n'avez pas d'abonnement WildFire, vous pouvez tout de même recevoir les mises à jour de signatures WildFire aux 24 à 48 heures.

1. Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**.
2. Vérifiez que le pare-feu est configuré pour télécharger et installer les mises à jour antivirus.

# Recommandations pour la fin du déploiement du pare-feu

Maintenant que vous avez intégré le pare-feu dans votre réseau et activé les fonctions de sécurité de base, vous pouvez passer à la configuration de fonctions plus avancées. Voici quelques informations à prendre en compte :

- Suivez les meilleures pratiques pour sécuriser l'accès administrateur pour vous assurer que vous sécurisez correctement les interfaces de gestion.
- Configurez une base de règles de politique de sécurité exemplaire pour autoriser, en toute sécurité, les applications et protéger votre réseau contre les attaques. Accédez à la page Meilleures pratiques et sélectionnez les meilleures pratiques de sécurité pour votre déploiement de pare-feu.
- Paramétrez la haute disponibilité : la high Availability (haute disponibilité ; HA) est une configuration dans laquelle deux pare-feu sont placés dans un groupe et où leur configuration et leurs tables de session sont synchronisées afin d'éviter tout point de défaillance unique sur votre réseau. Une connexion de pulsation entre les pare-feu homologues garantit un basculement transparent en cas d'arrêt d'un homologue. Le paramétrage d'un cluster composé de deux pare-feu fournit une redondance et vous permet d'assurer la continuité de l'activité.
- Activation de l'identification utilisateur (User-ID) : User-ID est une fonction des pare-feu de dernière génération Palo Alto Networks qui vous permet de créer des politiques et de générer des rapports en fonction des utilisateurs et des groupes d'utilisateurs, au lieu des adresses IP.
- Activation du décryptage : les pare-feu Palo Alto Networks offrent la possibilité de décrypter et d'inspecter le trafic à des fins de visibilité, de contrôle et de sécurité granulaire. Utilisez le décryptage sur un pare-feu afin d'empêcher du contenu malveillant d'accéder à votre réseau ou du contenu sensible de sortir de votre réseau sous forme de trafic crypté ou tunnellisé.
- Suivez les Meilleures pratiques pour sécuriser votre réseau contre les fuites au niveau des couches 4 et 7.
- Partage des renseignement sur les menaces avec Palo Alto Networks : permet au pare-feu de recueillir périodiquement des renseignements sur les applications, sur les menaces et sur la santé des périphériques et de les transmettre à Palo Alto Networks. La télémétrie comprend des options permettant d'activer la surveillance DNS passive et d'autoriser l'exécution des signatures de tests expérimentaux en arrière-plan sans qu'il n'y ait aucun effet sur vos règles de politique de sécurité, sur les journaux du pare-feu ou sur la performance du pare-feu. Tous les clients de Palo Alto Networks peuvent profiter des renseignements recueillis grâce à la télémétrie, que Palo Alto Networks utilise pour améliorer les fonctions de prévention des menaces du pare-feu.

# Meilleures pratiques pour sécuriser l'accès administratif

La protection de votre réseau contre les cyberattaques commence par un déploiement sécurisé du pare-feu. Si le réseau que vous utilisez pour gérer vos périphériques informatiques sensibles, y compris les pare-feu de nouvelle génération Palo Alto Networks et Panorama, n'est pas sécurisé correctement, vous ne pourrez pas détecter les vulnérabilités et vous défendre de celles-ci, ce qui pourrait entraîner une infiltration et/ou la perte de données à caractère sensible. Ultimement, la sécurisation de l'accès au pare-feu vise à garantir que, même si un attaquant accède à des informations d'identification privilégiées, vous pouvez toujours contrecarrer sa capacité à pénétrer sur le réseau et à y faire des dégâts. Suivez ces meilleures pratiques pour sécuriser l'accès administratif afin de vous assurer que vous sécurisez l'accès administratif à vos pare-feu et aux autres appareils de sécurité d'une manière qui empêche les attaques réussies.

- Isolez le réseau de gestion
- Utilisez les itinéraires de service pour accéder aux services externes
- Limitez l'accès à l'interface de gestion
- Gérez l'accès des administrateurs
- Créez des mots de passe administrateurs forts
- Analysez tout le trafic destiné à l'interface de gestion
- Remplacement du certificat du trafic de gestion entrant
- Gardez les mises à jour de contenu et logicielles à jour

## Isolez le réseau de gestion

Tous les pare-feu Palo Alto Networks fournissent un port de gestion hors bande (MGT) que vous pouvez utiliser pour effectuer les fonctions d'administration de pare-feu. Vous pouvez également choisir d'utiliser le port de gestion pour la configuration initiale, puis de configurer un port de données pour l'accès de gestion au pare-feu. Dans les deux cas, l'interface de gestion vous permet d'accéder à votre configuration de sécurité, vous devez prendre les précautions suivantes pour protéger l'accès à cette interface :

***N'activez pas l'accès à votre interface de gestion à partir d'Internet ou d'autres zones non approuvées dans les limites de sécurité de votre entreprise. Cela est vrai que vous utilisiez le port de gestion dédié (MGT) ou que vous configuriez un port de données en tant qu'interface de gestion.***

- Isolez l'interface de gestion sur un VLAN de gestion dédié.
- Limitez les adresses IP source autorisées dans le réseau de gestion à celles de vos périphériques de gestion dédiés, tels qu'un serveur de saut ou un hôte de bastion.
- Utilisez un serveur de saut ou un hôte bastion (avec enregistrement d'écran) pour fournir un accès sécurisé depuis votre réseau d'entreprise à votre réseau de gestion dédié et exiger que les utilisateurs s'authentifient et soient autorisés à accéder à votre réseau de gestion.
- Si vous ne possédez pas d'hôte bastion, utilisez la politique d'authentification avec l'authentification multifacteur (MFA) pour demander aux administrateurs de s'authentifier correctement avant d'être autorisés à passer à la page de connexion de l'interface Web ou à

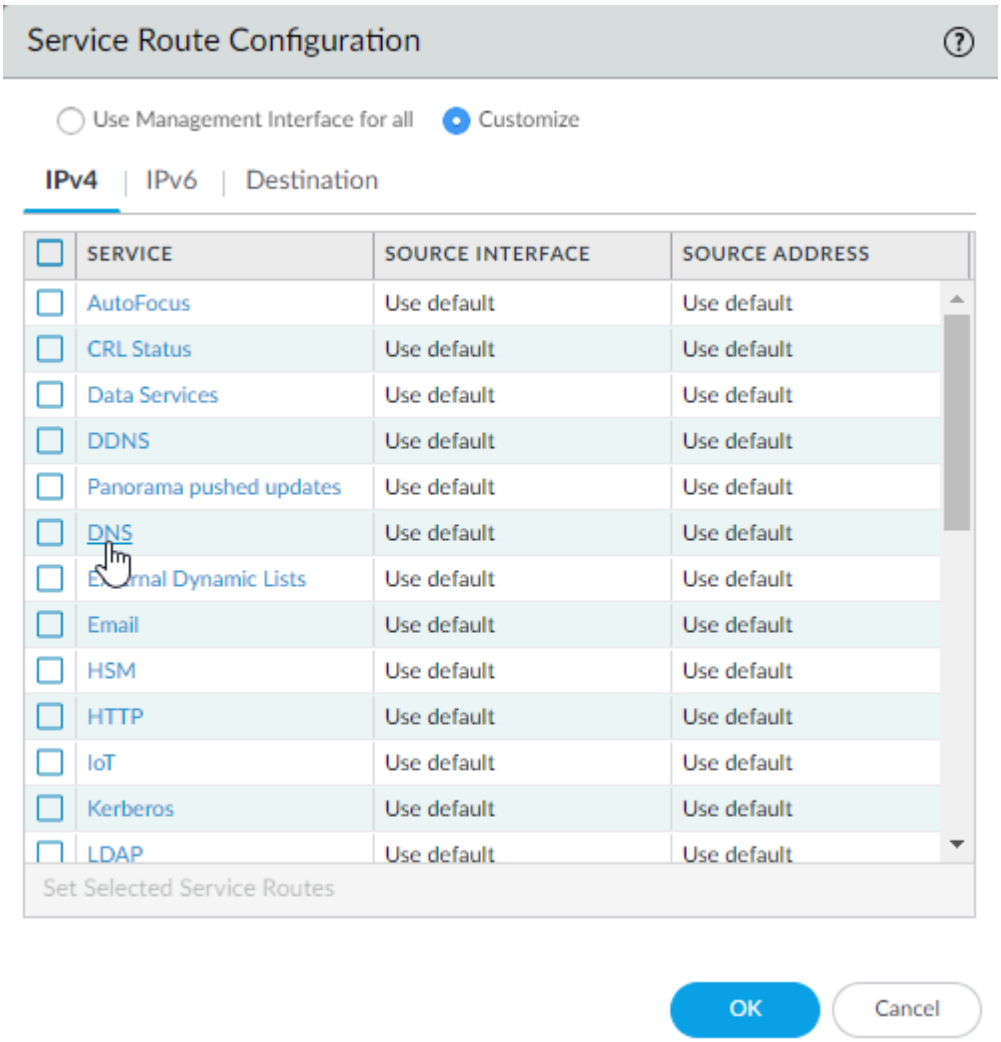
l'invite de connexion de la CLI. Cette méthode empêche l'accès à l'interface de gestion à l'aide d'informations d'identification volées ou d'exploits de vulnérabilité.

- Limitez l'accès aux groupes d'utilisateurs administrateurs TI, administrateurs de réseau ou administrateurs de la sécurité, selon ce qui convient à votre organisation.
- Si vous devez activer l'accès à distance au réseau de gestion, vous devez obtenir un accès via un tunnel VPN en utilisant GlobalProtect. Une fois que les administrateurs ont réussi à établir un tunnel VPN dans votre zone VPN, ils doivent toujours s'authentifier dans le réseau de gestion via votre hôte bastion.
- N'utilisez pas de profil de gestion d'interface qui autorise HTTP, HTTPS, Telnet ou SSH sur l'interface où vous avez configuré un portail ou une passerelle GlobalProtect car cette configuration expose l'accès à l'interface de gestion via Internet. N'utilisez pas HTTP ou Telnet à l'interne, car ces protocoles transmettent en texte clair.
- Si vous utilisez un modèle pour déployer un pare-feu VM-Series incluant un champ pour restreindre l'accès de gestion à une adresse IP spécifique, veillez à fournir un bloc CIDR correspondant à vos adresses IP ou à votre réseau dédié de gestion. Si nécessaire, modifiez le groupe de sécurité correspondant pour ajouter des hôtes ou des réseaux supplémentaires après le lancement du modèle. Ne définissez pas une plage de réseau source autorisée plus grande que nécessaire et ne configurez jamais la source autorisée comme 0.0.0.0/0.

## Utilisez les itinéraires de service pour accéder aux services externes

Par défaut, le pare-feu utilise le port de gestion (MGT) pour accéder aux services qui sont à l'extérieur du réseau de gestion sur les réseaux potentiellement non fiables, comme les serveurs DNS, les serveurs NTP et les serveurs d'authentification, notamment les services nécessitant un accès Internet, tels que les services de Palo Alto Networks et AutoFocus. Étant donné que votre interface de gestion, qu'il s'agisse du port MGT ou d'un port de données, doit être isolée sur le réseau de gestion, vous devez utiliser des itinéraires de service (**Device (Périphérique)** > **Setup (Configuration)** > **Services** > **Service Route Configuration (Configuration des itinéraires de service)**) pour permettre l'accès à ces services. Lorsque vous configurez un itinéraire de service, le pare-feu utilise plutôt l'interface source et l'adresse spécifiées pour accéder aux services dont vous avez besoin. Indiquez l'adresse IP / l'interface source de votre itinéraire de service sur une interface dont l'accès de gestion (HTTPS ou SSH) n'est pas activé.



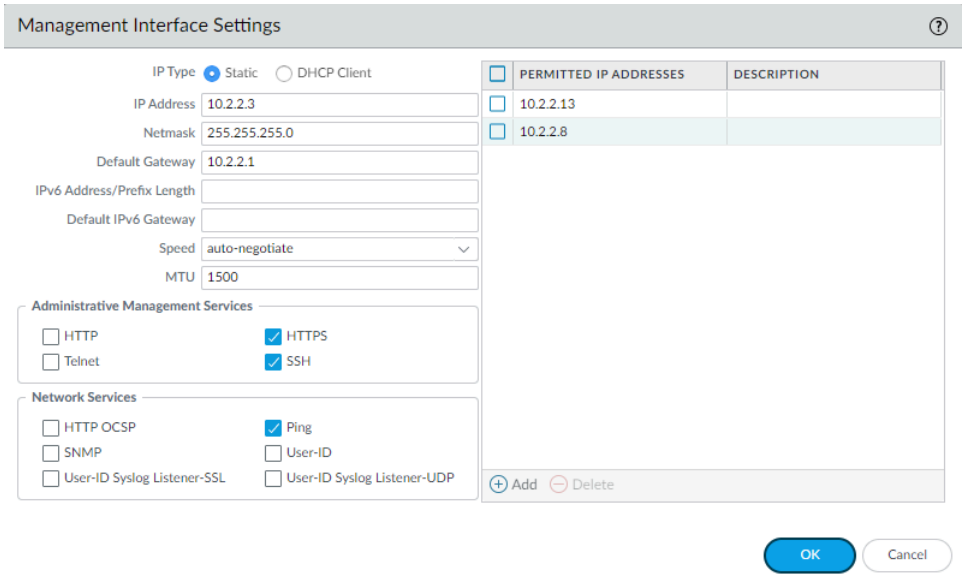

## Limitez l'accès à l'interface de gestion

- Vous devez restreindre les adresses IP autorisées à accéder à l'interface de gestion.

  Même si votre pare-feu est sur un réseau de gestion dédié qui est accessible uniquement par un périphérique sur le même VLAN ou par l'intermédiaire d'un hôte bastion ou d'un tunnel VPN, vous pouvez sécuriser davantage les pare-feu en limitant les adresses IP source qui peuvent accéder à l'interface de gestion à celles de vos administrateurs. La limitation de l'accès à l'interface de gestion réduit la surface d'attaque en empêchant l'accès à partir d'adresses IP ou de sous-réseaux inattendus et empêche l'accès au moyen d'informations d'identification volées.
- Vous devez restreindre les services disponibles sur l'interface de gestion.
  - N'autorisez pas l'accès via Telnet et HTTP, car ces services utilisent du texte en clair et ne sont pas aussi sécurisés que les autres services et peuvent compromettre les informations d'identification de l'administrateur. Demandez plutôt aux administrateurs d'accéder aux interfaces de pare-feu via SSH ou HTTPS.
  - Activez le ping si vous voulez pouvoir tester la connectivité à l'interface, mais n'activez aucun autre service sur l'interface de gestion.

- La façon dont vous configurez ces paramètres varie selon que vous utilisez le port de gestion ou un port de données pour accéder aux interfaces de gestion du pare-feu :
  - Si vous utilisez le port MGT comme interface de gestion, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Interfaces** et sélectionnez l'interface de **Management (Gestion)** pour configurer les paramètres afin de restreindre l'accès à l'interface de gestion et les services autorisés par l'interface.

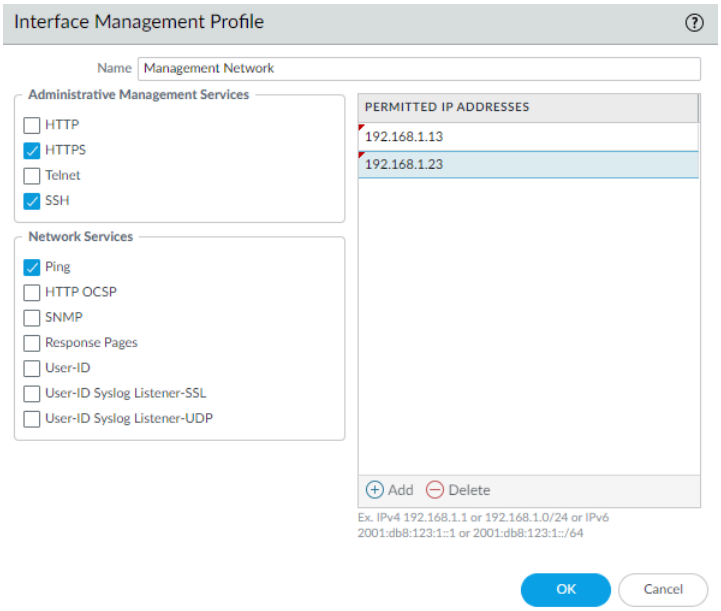



  - Si vous utilisez un port de données comme interface de gestion, après avoir configure the interface (configuré l'interface), sélectionnez **Network(Réseau )** > **Network Profiles (Profils réseau)** > **Interface Mgmt (Gestion de l'interface)** et **Add (Ajoutez)** un interface management

profile (profil de gestion d'interface) pour restreindre l'accès à l'interface de gestion et les services autorisés par l'interface.

***N'affectez pas un profil de gestion de l'interface qui autorise Telnet, SSH, HTTP ou HTTPS à une interface sur laquelle vous avez configuré un portail ou une passerelle GlobalProtect, car ce faisant vous exposeriez l'interface de gestion à l'Internet. N'utilisez pas HTTP ou Telnet pour un profil d'interface de gestion, car ces protocoles transmettent en texte clair.***




## Gérez l'accès des administrateurs

- Le pare-feu est préconfiguré avec un compte administrateur par défaut (admin) qui fournit un accès en lecture-écriture complet (également appelé accès super-utilisateur) au pare-feu. Vous devez modifier le mot de passe du compte d'administrateur par défaut (**Device (Périphérique)** > **Administrators (Administrateurs)** > **admin**) immédiatement lors de la configuration initiale.

  Si les exigences de conformité, d'audit ou de sécurité stipulent que le compte administratif par défaut doit être supprimé de vos périphériques, vous pouvez le supprimer après avoir créé au moins un compter administratif de superutilisateur. Vous ne pouvez supprimer le compte administratif par défaut avant d'avoir configuré au moins un autre compte administratif de superutilisateur sur le périphérique.
- Configurez un compte de pare-feu administrateur pour chaque personne qui a besoin d'accéder aux fonctions d'administration ou de génération de rapports du pare-feu. Cela vous permet de mieux protéger le pare-feu contre la configuration (ou modification) non autorisée et d'activer la journalisation des actions de chaque administrateur.
- Affectez chaque compte d'administrateur à un profil de rôle d'administrateur qui limite les privilèges de gestion aux seules fonctions dont l'administrateur individuel a besoin.
- Pour les administrateurs ayant des privilèges de modification, exigez l'authentification multifacteurs (MFA) à l'aide d'une authentification externe et l'autorisation à l'aide de RADIUS ou

de SAML. Voir Configurez l'authentification locale ou externe pour les administrateurs de pare-feu pour plus de détails sur la configuration de l'authentification externe avec MFA.

***Si vous disposez d'une infrastructure d'authentification forte utilisant des cartes à puce, vous pouvez procédez à la*** configuration de l'authentification administrateur basée sur les certificats pour l'interface Web ***et à la*** configuration de l'authentification administrateur basée sur les clés SSH pour la CLI**.**

***Si elles sont disponibles, utilisez des solutions Privileged Account Management (de gestion des comptes privilégiés ; PAM) et / ou de Privileged Identity Management (gestion des identités privilégiées ; PIM) pour sécuriser les informations d'identification de l'administrateur en externe.***

- Surveillez les journaux système pour identifier l'activité anormale du compte sur l'un de vos comptes administrateur. Par exemple, si les journaux affichent des tentatives de connexion excessives ou des connexions répétées à certains moments de la journée, ce que le compte administratif pourrait avoir été compromis. En outre, informez tous les administrateurs de l'Utilisation des indicateurs d'activité de connexion de l'administrateur pour détecter toute utilisation frauduleuse du compte.

## Créez des mots de passe administrateurs forts

Configurez une stratégie de mot de passe stricte, y compris en exigeant des changements de mot de passe fréquents (**Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **Minimum Password Complexity (Complexité minimale du mot de passe)**).

Vous êtes responsable de l'évaluation des exigences relativement aux mots de passe qui conviennent pour votre organisation ; cependant, il est recommandé d'utiliser les caractéristiques suivantes pour la création de mots de passe forts. Les mots de passe :

- doivent comporter au moins huit caractères ;
- ne doivent pas se fonder sur un mot du dictionnaire ;
- ne doivent pas contenir des mots contextuels (par exemple, le nom d'un site Web) ;
- ne doivent pas comprendre un nom d'utilisateur ou un dérivé d'un nom d'utilisateur (par exemple, @dmin, Johnny) ;
- ne doivent pas contenir des caractères répétitifs ou séquentiels (par exemple, aaaaaa, 1234abcd) ;
- doivent comprendre des majuscules et des minuscules, des chiffres et des caractères spéciaux (y compris des espaces).

Une façon de créer un mot de passe fort consiste à créer une longue phrase secrète plutôt qu'un mot de passe complexe. Selon les normes du secteur, il est recommandé de créer des phrase secrètes longues et unique dont vous vous souviendrez facilement (à l'aide des caractères de votre choix, y compris des mots de dictionnaire) plutôt que de créer des mots de passes complexes qui sont faciles à oublier. On estime que les mots de passe plus longs qui comportent au moins 15 caractères remplacent les mots de dictionnaires. Essayez de créer une phrase secrète en vous basant sur des expressions longues et familières que vous êtes seul à connaître ou rassemblez au moins quatre mots.

Pour obtenir de plus amples renseignements sur la détermination des exigences en matière de mots de passe qui conviennent à votre organisation, nous vous recommandons les ressources suivantes :

- NIST SP 800-63B, Digital Identity Guidelines
- NIST, Easy Ways to Build a Better P@$5w0rd

## Analysez tout le trafic destiné à l'interface de gestion

***Étant donné que la politique de sécurité et la politique de déchiffrement n'évaluent pas le trafic du plan de gestion, vous ne pouvez pas analyser directement le port de gestion afin d'y repérer des menaces. Si vous utilisez le port de gestion comme interface de gestion, envisagez d'acheminer le trafic destiné au port de gestion via un port de données ou via un autre pare-feu afin de pouvoir appliquer ces contrôles de sécurité importants à votre trafic de gestion.***

- Créez des règles de politique de sécurité pour autoriser l'accès aux interfaces de gestion du pare-feu et de Panorama (interface Web ou CLI). La façon dont vous définissez la politique dépend de l'utilisation ou non d'un hôte bastion pour activer l'accès au réseau de gestion.
  - Si vous n'utilisez pas d'hôte bastion pour isoler votre réseau de gestion, créez une règle de politique de sécurité pour autoriser l'accès de la zone Utilisateurs à la zone Infrastructure informatique. Cette règle de politique de sécurité doit être très précise et spécifier la zone source, l'adresse IP source (si disponible) et le groupe d'utilisateurs source de l'utilisateur qui tente d'accéder à l'interface de gestion, ainsi que la zone de destination (pare-feu ou Panorama) et l'ID d'application pour identifier l'application de gestion spécifique (interface Web ou CLI) s'exécutant sur le port par défaut de l'application. Par exemple, vous utiliserez l'interface d'application Web panos-web App-ID pour autoriser l'accès à l'interface Web et l'ID d'application ssh pour autoriser l'accès à l'interface CLI. Vous devez également associer un profil de protection contre les vulnérabilités à la règle, comme décrit dans la section suivante.

    L'exemple de règle suivant permet d'accéder directement à la zone Infrastructure informatique depuis la zone Utilisateurs et restreint l'accès aux utilisateurs du groupe IT-admins qui tentent d'accéder à l'adresse IP de l'interface de gestion pour accéder à l'application interface panos-web sur le port par défaut de l'application uniquement :

| | Source | | Destination | | | | |
|---|---|---|---|---|---|---|---|
| NAME | ZONE | USER | ZONE | APPLICATION | SERVICE | ACTION | PROFILE |
| FW-mgt | Users | IT-admins | IT-infrastruc... | panos-web-interface<br>ssh | application-default | Allow | |

  - Si vous utilisez un hôte bastion pour activer l'accès à votre réseau de gestion, vous avez besoin de deux règles de politique de sécurité : une règle pour autoriser l'accès de la zone utilisateur à la zone hôte du bastion et une deuxième règle pour autoriser l'accès de la zone hôte du bastion à la zone d'infrastructure informatique. Encore une fois, ces deux règles de sécurité doivent être aussi précises que possible et inclure la zone source, l'adresse (si disponible), l'utilisateur et la zone et l'adresse de destination, ainsi que l'identifiant de l'application. Gardez à l'esprit que, si vous utilisez un hôte bastion, l'adresse IP de l'utilisateur correspond généralement à l'adresse IP de l'hôte bastion, vous ne pouvez donc pas identifier le User-ID de l'administrateur à moins que vous utilisiez l'agent Terminal Server sur l'hôte bastion pour identifier des utilisateurs individuels. Dans ce cas, vous devez également associer un profil de protection contre les vulnérabilités aux deux règles, comme décrit dans la section suivante.

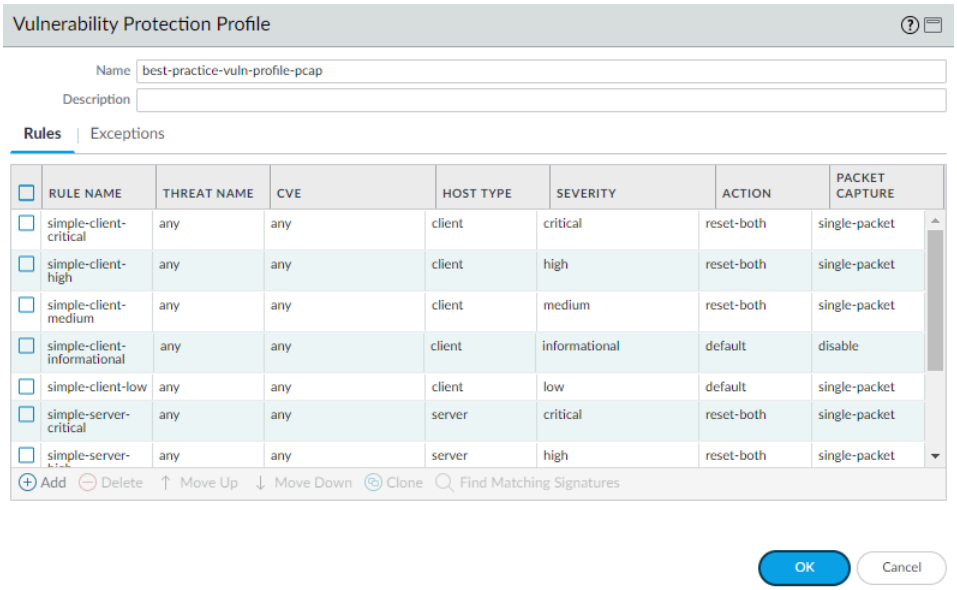
    Dans les exemples de règles qui suivent, la première règle autorise l'accès de la zone Utilisateurs à la zone hôte Bastion pour les utilisateurs du groupe IT-admins qui tentent

d'accéder à l'adresse IP du serveur bastion spécifiée via SSH et / ou RDP. La seconde règle permet aux utilisateurs d'accéder à la zone Bastion-host à la zone IT-infrastructure qui tente d'accéder à l'application panos-web-interface sur le port par défaut du pare-feu avec l'adresse de destination spécifiée.

| | Source | | Destination | | | | |
|---|---|---|---|---|---|---|---|
| NAME | ZONE | USER | ZONE | APPLICATION | SERVICE | ACTION | PROFILE |
| Bastion-host-access | Users | IT-admins | Bastion-host | ms-rdp<br>ssh | application-default | Allow | |
| FW-mgt | Bastion-host | IT-admins | IT-infrastruc... | panos-web-interface<br>ssh | application-default | Allow | |

- Associez un Profil de protection contre les vulnérabilités exemplaire aux règles de sécurité qui autorisent l'accès à votre réseau de gestion pour le protéger contre les dépassements de la capacité de la mémoire tampon, l'exécution non autorisée de code et d'autres tentatives d'exploitation des vulnérabilités côté client et côté serveur. Pour créer un profil dans le but de protéger votre interface de gestion, clonez le profil strict, puis activez la capture de paquets étendue pour vous aider à repérer la source de toute attaque éventuelle.




- Procédez à la Configuration de l'inspection SSL entrante ou à la Configuration du proxy de transfert SSL pour le trafic depuis ou vers l'interface de gestion pour vous assurer que vous pouvez déchiffrer et analyser le trafic afin d'y déceler des menaces. Associez un Profil de déchiffrement exemplaire à la règle de décryptage pour vous assurer que vous bloquez les versions SSL / TLS vulnérables telles que TLS 1.0 et SSLv3 et que vous rejetez les sessions à l'aide d'algorithmes de chiffrement faibles tels que RC4 et 3DES et d'algorithmes d'authentification faibles tels que MD5 et SHA1.

## Remplacement du certificat du trafic de gestion entrant

Par défaut, le pare-feu est fourni avec un certificat par défaut qui autorise l'accès HTTPS à l'interface Web sur l'interface de gestion (MGT) et sur toute interface qui prend en charge le trafic de gestion HTTPS. Pour renforcer la sécurité du trafic de gestion sortant, remplacez le certificat défini par défaut par un nouveau certificat délivré spécialement pour votre organisation. Utilisez des certificats signés par votre autorité de certification d'entreprise afin que les utilisateurs n'apprennent pas à

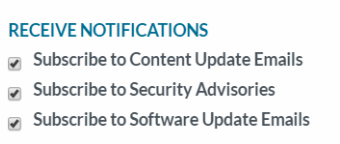
 

ignorer les avertissements de certificat. De plus, dans le profil SSL/TLS profile, définissez la **Min version (Version minimale)** sur **TLSv1.2** pour pouvoir utiliser le protocole le plus rigoureux et définissez la **Max version (Version maximale)** sur **Max** pour que vous puissiez continuer à utiliser le protocole le plus fort au fur et à mesure que des versions plus fortes deviennent disponibles.

## Gardez les mises à jour de contenu et logicielles à jour

Les mises à jour logicielles et du contenu font en sorte que vous êtes toujours protégé par les derniers correctifs de sécurité et les plus récentes mises à jour de menaces.

- Pour être toujours informé des dernières mises à jour et des derniers avis de sécurité, accédez au portail de support Palo Alto Networks, sélectionnez **Edit Profile (Modifier le profil)** et **Subscribe to Content Update Emails (S'abonner aux e-mails de mise à jour du contenu)**, **Subscribe to Security Advisories (S'abonner aux avis de sécurité)** et **Subscribe to Software Update Emails (S'abonner aux e-mails)**. Assurez-vous de **Save Edits (Enregistrer les modifications)**.




- Suivez les Best Practices for Applications and Threats Content Updates (Meilleures pratiques pour les mises à jour du contenu de menace et des applications) lors de la mise à jour vers la dernière version de contenu.
- Avant de Passer à PAN-OS, lisez les plus récentes notes de version.

# Abonnements

Découvrez tous les abonnements et services qui fonctionnent avec le pare-feu, et commencez à les utiliser en activant vos licences d'abonnement :



*Certains services cloud, comme Cortex XDR™ – Analytics, ne s'intègrent pas directement avec le pare-feu, mais dépendent des données du service de journalisation pour obtenir une visibilité des activités du réseau. La fonctionnalité de journalisation avancée d'applications est une fonctionnalité qui vient avec la souscription Cortex Data Lake -- Elle permet au pare-feu de collecter les données spécifiquement à Cortex XDR qui les utilisent pour détecter des activités anormales réseaux Activer la journalisation avancée d'applications est une meilleure pratique de Cortex XDR.*

# Abonnements à utiliser avec le pare-feu

Les abonnement de Palo Alto Networks suivants déverrouillent certaines fonctionnalités du pare-feu ou permettent au pare-feu d'exploiter le service cloud de Palo Alto Networks (ou les deux). Ici, vous pouvez en lire davantage sur chaque service ou fonctionnalité qui exige un abonnement pour fonctionner avec le pare-feu. Pour activer un abonnement, vous devez d'abord Activation des licences d'abonnement ; une fois actifs, la plupart des services d'abonnement peuvent utiliser les Dynamic Content Updates (Mises à jour de contenu dynamiques) pour procurer au pare-feu une fonctionnalité nouvelle et mise à jour.

| Abonnements à utiliser avec le pare-feu | |
|---|---|
| **IoT Security** | La solution IoT Security fonctionne avec les pare-feu de nouvelle génération pour découvrir et maintenir dynamiquement un inventaire en temps réel des périphériques IdO sur votre réseau. Grâce à l'IA et aux algorithmes d'apprentissage machine, la solution IoT Security atteint un niveau de précision élevé, allant même jusqu'à classifier les types de périphériques IdO rencontrés pour la première fois. Et parce qu'il est dynamique, votre inventaire de périphériques IdO est toujours à jour. IoT Security permet également la génération automatique de recommandations de politiques pour contrôler le trafic des périphériques IdO, ainsi que la création automatique d'attributs de périphériques IdO à utiliser dans les politiques de pare-feu.<br>• Premiers pas avec IoT Security |
| **SD-WAN** | Fournit une sélection intelligente et dynamique des chemins en plus de la sécurité de pointe que le logiciel PAN-OS offre déjà. Gérée par Panorama, l'implémentation de SD-WAN comprend ce qui suit :<br>• Gestion centralisée de la configuration<br>• Création automatique de la topologie VPN<br>• Distribution du trafic<br>• Surveillance et dépannage<br>• Premiers pas avec SD-WAN |
| **Prévention contre les menaces** | La prévention des menaces fournit :<br>• Une protection antivirus, anti-spyware (commande-et-contrôle) et contre les vulnérabilités.<br>• Des listes dynamiques externes intégrées que vous pouvez utiliser pour sécuriser votre réseau contre les hôtes malveillants.<br>• Une capacité à identifier des hôtes infectés qui tentent de se connecter à des domaines malveillants. |

| Abonnements à utiliser avec le pare-feu | |
|---|---|
| | • Premiers pas avec la prévention contre les menaces |
| **Sécurité DNS** | Améliore les capacités de mise en entonnoir DNS en interrogeant la sécurité DNS, un service basé sur le cloud extensible capable de générer des signatures DNS à l'aide de l'analyse prédictive avancée et de l'apprentissage machine. Ce service offre un accès complet aux renseignements sur les menaces DNS produit par Palo Alto Networks, lesquels ne cessent de croître.<br><br>Pour paramétrer la sécurité DNS, vous devez d'abord acheter et installer une licence de prévention contre les menaces.<br><br>• Premiers pas avec la sécurité DNS |
| **Filtrage des URL** | Fournit la capacité de contrôler non seulement l'accès web, mais également la manière dont les utilisateurs interagissent avec le contenu en ligne en fonction de catégories d'URL dynamiques. Vous pouvez également empêcher le vol d'informations d'identification en contrôlant les sites auxquels les utilisateurs peuvent soumettre leurs informations d'identification d'entreprise.<br><br>Pour paramétrer le filtrage des URL, vous devez acheter et installer un abonnement pour la base de données de filtrage des URL prises en charge : PAN-DB. Avec PAN-DB, vous pouvez configurer l'accès au cloud PAN-DB public ou au cloud PAN-DB privé.<br><br>*Le filtrage d'URL n'est plus disponible en tant qu'abonnement autonome. Toutes les fonctionnalités contenues dans le filtrage d'URL sont incluses dans l'abonnement au filtrage d'URL avancé.*<br><br>• Premiers pas avec le filtrage des URL |
| **Filtrage d'URL avancé** | Le filtrage avancé des URL utilise un moteur de sécurité Web basé sur le ML pour effectuer une inspection du trafic Web basée sur le ML en temps réel. Cela réduit la dépendance aux bases de données d'URL et à l'exploration Web hors bande pour détecter et prévenir les attaques Web avancées et sans fichier, y compris le phishing ciblé, les logiciels malveillants et les exploits sur le Web, la commande et le contrôle, l'ingénierie sociale et d'autres types d'attaques Web.<br><br>• Get Started with Advanced URL Filtering (Prise en main du filtrage avancé des URL) |

| Abonnements à utiliser avec le pare-feu | |
|---|---|
| **WildFire** | Bien que le support WildFire® de base soit inclus dans la licence Prévention des menaces, le service d'abonnement WildFire offre des services avancés pour les entreprises qui ont besoin d'une protection immédiate contre les menaces, de mises à jour de signatures WildFire fréquentes, du transfert de types de fichiers avancés (APK, PDF, Microsoft Office et Applet Java) et du chargement de fichiers à l'aide de l'API WildFire. Un abonnement WildFire est également requis si vos pare-feu transfèrent des fichiers vers un appareil WF-500 sur site.<br>• Premiers pas avec WildFire |
| **AutoFocus** | Donne une analyse graphique des journaux du trafic sur le pare-feu et détermine les risques éventuels qui menacent votre réseau au moyen des renseignements sur les menaces tirés du portail AutoFocus. Si vous possédez une licence active, vous pouvez également lancer une recherche AutoFocus basée sur les journaux consignés sur le pare-feu.<br>• Premiers pas avec AutoFocus |
| **Lac de données Cortex** | Fournit un stockage et une agrégation de journaux centralisés basés sur le cloud. Le lac de données Cortex est requis ou hautement recommandé pour la prise en charge de plusieurs autres services fournis dans le nuage, notamment Cortex XDR, IoT Security et Prisma Access, ainsi que le service de gestion des interruptions.<br>• Premiers pas avec le lac de données Cortex |
| **GlobalProtect** | Offre des solutions de mobilité et/ou des fonctionnalités de réseau privé virtuel à grande échelle. Par défaut, vous pouvez déployer des portails et des passerelles GlobalProtect (sans aucune vérification HIP) sans aucune licence. Si vous voulez utiliser les fonctionnalités avancées GlobalProtect (archivages HIP et mises à jour de contenu connexes, application mobile GlobalProtect, connexions IPv6 ou VPN sans client GlobalProtect) vous devrez détenir une licence GlobalProtect (abonnement) pour chaque passerelle.<br>• Premiers pas avec GlobalProtect |
| **Systèmes virtuels** | Il s'agit d'une licence perpétuelle, et elle est nécessaire pour permettre la prise en charge de plusieurs systèmes virtuels sur les pare-feu de la série PA-3200. En outre, vous devez acheter une licence Systèmes virtuels si vous souhaitez augmenter le nombre de systèmes virtuels au-delà du nombre de base fourni par défaut sur les pare-feux PA-5200 et PA-7000 Series (le nombre de base varie en fonction de la plate-forme). Les pare- |

| Abonnements à utiliser avec le pare-feu | |
|---|---|
| | feu PA-800 Series, PA-220 et VM-Series ne prennent pas en charge les systèmes virtuels.<br>• Premiers pas avec les systèmes virtuels |
| **Prévention des pertes de données d'entreprise (DLP)** | Offre une protection dans le nuage contre l'accès non autorisé, l'utilisation abusive, l'extraction et le partage d'informations sensibles. DLP entreprise fournit un moteur unique pour une détection précise et une application cohérente des politiques pour les données sensibles au repos et en mouvement en utilisant une classification des données basée sur l'apprentissage machine, des centaines de modèles de données utilisant des expressions régulières ou des mots clés, et des profils de données utilisant une logique booléenne pour rechercher des types de données collectives.<br>• Premiers pas avec la prévention des pertes de données d'entreprise |
| **SaaS Security Inline (Sécurité SaaS en ligne)** | La solution de sécurité SaaS fonctionne avec Cortex Data Lake pour découvrir toutes les applications SaaS utilisées sur votre réseau. SaaS Security Inline peut découvrir des milliers d'applications Shadow IT et leurs utilisateurs et détails d'utilisation. SaaS Security Inline applique également les recommandations de règles de stratégie SaaS de manière transparente sur vos pare-feu Palo Alto Networks existants. App-ID Cloud Engine (ACE) nécessite également SaaS Security Inline.<br>• Get Started with Prisma SaaS (Premiers pas avec Prisma SaaS) |

# Activation des licences d'abonnement

Suivez ces étapes pour activer une nouvelle licence sur le pare-feu.

La fonctionnalité Decryption Mirroring (Mise en miroir du décryptage) nécessite que vous activiez une licence gratuite pour déverrouiller la fonctionnalité de la fonctionnalité. Pour ces fonctionnalités, vous devez plutôt suivre les étapes de Activation des licences gratuites pour le déchiffrement.

**STEP 1 |** Localisez les codes d'activation pour les licences que vous avez achetées.

Lorsque vous avez acheté vos abonnements, vous avez dû recevoir un e-mail du service client de Palo Alto Networks indiquant le code d'activation associé à chaque abonnement. Si vous ne parvenez pas à trouver ce e-mail, contactez le Support client pour obtenir vos codes d'activation avant de continuer.

**STEP 2 |** Activer votre licence d'assistance.

Vous ne pourrez pas mettre votre logiciel PAN-OS à jour si vous ne détenez pas de licence de support valide.

1. Connectez-vous à l'interface Web, puis sélectionnez **Device (Périphérique)** > **Support (Support)**.
2. Cliquez sur **Activate support using authorization code (Activer la prise en charge à l'aide du code d'autorisation)**.
3. Saisissez votre **Authorization Code (Code d'autorisation)**, puis cliquez sur **OK (OK)**.

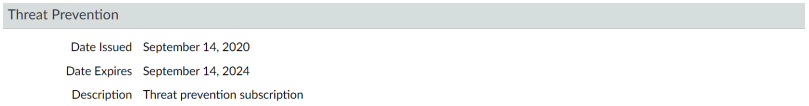
**STEP 3 |** Activez chaque licence achetée.

Sélectionnez **Device (Périphérique)** > **Licenses (Licences)**, puis activez vos licences et vos abonnements de l'une des manières suivantes :

- **Retrieve license keys from license server (Récupérer les clés de licence auprès du serveur de licences)** : utilisez cette option si vous avez activé votre licence sur le portail du Support client.
- **Activate feature using authorization code (Activer la fonction à l'aide du code d'autorisation)** : utilisez cette option pour activer des abonnements souscrits à l'aide d'un code d'autorisation pour les licences qui n'ont pas été précédemment activées sur le portail de support. Lorsque vous y êtes invité, saisissez le **Authorization Code (Code d'autorisation)**, puis cliquez sur **OK (OK)**.
- **Manually upload license key (Charger manuellement la clé de licence)** : utilisez cette option si votre pare-feu ne dispose d'aucune connectivité au portail de support aux clients de Palo Alto Networks. Dans ce cas, vous devez télécharger un fichier de clé de licence à partir du site de support sur un ordinateur connecté à Internet, puis le charger sur le pare-feu.

**STEP 4 |** Vérifiez que la licence a été activée avec succès.

Sur la page **Device (Périphérique)** > **Licenses (Licences)**, vérifiez que la licence a été activée avec succès. Par exemple, une fois que vous avez activé la licence WildFire, vous pouvez voir la validité de la licence :




**STEP 5 |** (Abonnements WildFire uniquement) Effectuez une action de validation pour terminer l'activation de l'abonnement WildFire.

Une fois l'abonnement WildFire activé, une validation est requise pour que le pare-feu puisse commencer à transférer des types de fichiers avancés . Vous devriez :

- Valider les modifications en attente.
- Vérifier que les règles de profil d'analyse WildFire comprennent les types de fichiers avancés qui sont désormais pris en charge grâce à l'abonnement WildFire. Si aucune règle n'a à être modifiée, modifiez légèrement une description de règle et validez.

# Que se passe-t-il à l'expiration des licences ?

Grâce aux abonnements Palo Alto Networks, le pare-feu bénéficie de fonctionnalités accrues et/ou d'un accès à un service infonuagique de Palo Alto Networks. Lorsqu'une licence est dans les 30 jours suivant son expiration, un message d'avertissement s'affiche quotidiennement dans le journal système jusqu'à ce que l'abonnement soit renouvelé ou expire. Lorsque la licence arrive à expiration, certains abonnements continuent de fonctionner de façon limitée, et d'autres cessent complètement de fonctionner. Vous découvrirez ici ce qui se produit lors de l'expiration de chaque abonnement.

*Le moment précis de l'expiration de la licence est au début du jour suivant à 00h00 (GMT). Par exemple, si votre licence doit se terminer le 1/20, vous aurez des fonctionnalités pour le reste de la journée. Au début de la nouvelle journée le 21/01 à 00h00 (GMT), la licence expirera. Toutes les fonctions liées aux licences fonctionnent à l'heure GMT (Greenwich Mean Time), quel que soit le fuseau horaire configuré sur le pare-feu.*

| Abonnement | Comportement à l'expiration |
|---|---|
| Prévention contre les menaces | Des alertes indiquant que la licence est expirée apparaissent dans le journal système.<br>**Vous pouvez tout de même :**<br>• Utilisez les signatures qui ont été installées au moment où la licence a expiré, sauf si vous installez une nouvelle mise à jour du contenu des applications uniquement, soit manuellement, soit dans le cadre d'un programme automatique. Si vous le faites, la mise à jour supprimera vos signatures de menace existantes et vous ne serez plus protégé contre celles-ci.<br>• Utiliser et modifier les App-ID™ et les signatures de menaces personnalisés.<br>**Vous ne pouvez plus :**<br>• Installer de nouvelles signatures.<br>• Retourner à des versions antérieures des signatures. |
| Sécurité DNS | **Vous pouvez tout de même :**<br>• Utiliser les signatures DNS locales et vous détenez une licence de prévention des menaces.<br>**Vous ne pouvez plus :**<br>• Obtenir de nouvelles signatures DNS. |
| Filtrage d'URL avancé / Filtrage d'URL | **Vous pouvez tout de même :**<br>• Appliquer la politique au moyen des catégories d'URL personnalisées. |

| Abonnement | Comportement à l'expiration |
|---|---|
| | • Appliquer la politique au moyen des catégories PAN-DB qui se trouvaient dans votre mémoire tampon local lors de l'expiration de la licence.<br>**Vous ne pouvez plus :**<br>• Obtenir les mises à jour des catégories PAN-DB mises en mémoire tampon.<br>• Connectez-vous à la base de données de filtrage d'URL PAN-DB.<br>• Obtenir les catégories PAN-DB des URL qui ne sont pas en mémoire tampon.<br>• Analysez les demandes d'URL en temps réel à l'aide du filtrage d'URL avancé. |
| WildFire | **Vous pouvez tout de même :**<br>• Transmettre des PE à des fins d'analyse.<br>• Obtenir les mises à jour des signatures aux 24 à 48 heures, si vous détenez un abonnement Prévention des menaces actif.<br>**Vous ne pouvez plus :**<br>• Obtenez des mises à jour aux cinq minutes grâce aux clouds WildFire publics et privés.<br>• Transférez des types de fichiers avancés, comme les fichiers APK, Flash, PDF, Microsoft Office, applets Java, fichiers Java (.jar et .class), ainsi que les liens d'e-mail HTTP/HTTPS contenus dans les messages électroniques SMTP et POP3.<br>• Utilise l'API WildFire.<br>• Utilisez l'appareil WildFire pour héberger un cloud WildFire privé ou un cloud WildFire hybride. |
| AutoFocus | **Vous pouvez tout de même :**<br>• Utiliser une liste dynamique externe avec des données AutoFocus pour une période de grâce de trois mois.<br>**Vous ne pouvez plus :**<br>• Accéder au portail AutoFocus.<br>• Consulter le récapitulatif des données de renseignements d'AutoFocus du journal de surveillance ou des artefacts ACC. |
| Lac de données Cortex | **Vous pouvez tout de même :**<br>• Stocker les données des journaux pour une période de grâce de 30 jours, après quoi ils sont supprimés. |

| Abonnement | Comportement à l'expiration |
|---|---|
| | • Transférer les journaux au lac de données Cortex jusqu'à la fin de la période de grâce de 30 jours. |
| GlobalProtect | **Vous pouvez tout de même :**<br>• Utiliser l'application pour les terminaux exécutant Windows et macOS.<br>• Configurer des passerelles internes uniques ou multiples.<br>**Vous ne pouvez plus :**<br>• Accéder à l'application Linux OS et à l'application mobile pour iOS, Android, Chrome OS et les applications UWP de Windows 10.<br>• Utiliser IPv6 pour les passerelles externes.<br>• Exécuter des vérifications HIP.<br>• Utiliser le VPN sans client.<br>• Appliquez la segmentation des tunnels en fonction du domaine de destination, du processus client ou de l'application de diffusion vidéo en continu. |
| VM-Series | **Vous pouvez tout de même :**<br>• Configurer et utiliser les pare-feu qui étaient déployés lors de l'expiration de la licence. |
| Assistance | **Vous ne pouvez plus :**<br>• Recevoir les mises à jour logicielles.<br>• Télécharger les images de VM.<br>• Recevoir l'aide du soutien technique. |

# Journaux des applications améliorés pour les services cloud Palo Alto Networks

Le pare-feu peut collecter des données qui permettent d'accroître la visibilité des activités réseau pour les applications et services Palo Alto Networks, comme Cortex XDR. Ces journaux d'application améliorés sont conçus uniquement pour consommer et traiter les applications et services de Palo Alto Networks ; vous ne pouvez pas afficher les journaux d'applications améliorés sur le pare-feu ou sur Panorama. Seuls les pare-feu qui envoient des journaux au lac de données Cortex peut générer des journaux d'applications améliorés.

Parmi les exemples de types de données collectées par les journaux d'applications améliorées, notons les enregistrements de requêtes DNS, le champ d'en-tête HTTP de l'agent utilisateur spécifiant le navigateur Web ou l'outil utilisé pour accéder à une URL et l'affectation automatique d'adresses IP par DHCP. Avec les informations DHCP, par exemple, Cortex XDR™ peut signaler une activité inhabituelle en fonction du nom d'hôte plutôt que de l'adresse IP. Cela permet à l'analyste de sécurité utilisant Cortex XDR d'évaluer de manière significative si l'activité de l'utilisateur relève de son rôle et, dans le cas contraire, de rapidement prendre des mesures pour arrêter l'activité.

Pour bénéficier de l'ensemble le plus complet de journaux d'applications améliorés, vous devez activer User-ID ; les déploiements de l'agent User-ID Windows et l'agent User-ID intégré à PAN-OS collectent certaines données dont les journaux User-ID du pare-feu ne tiennent pas compte, mais qui s'avèrent utiles pour associer l'activité réseau à des utilisateurs spécifiques.

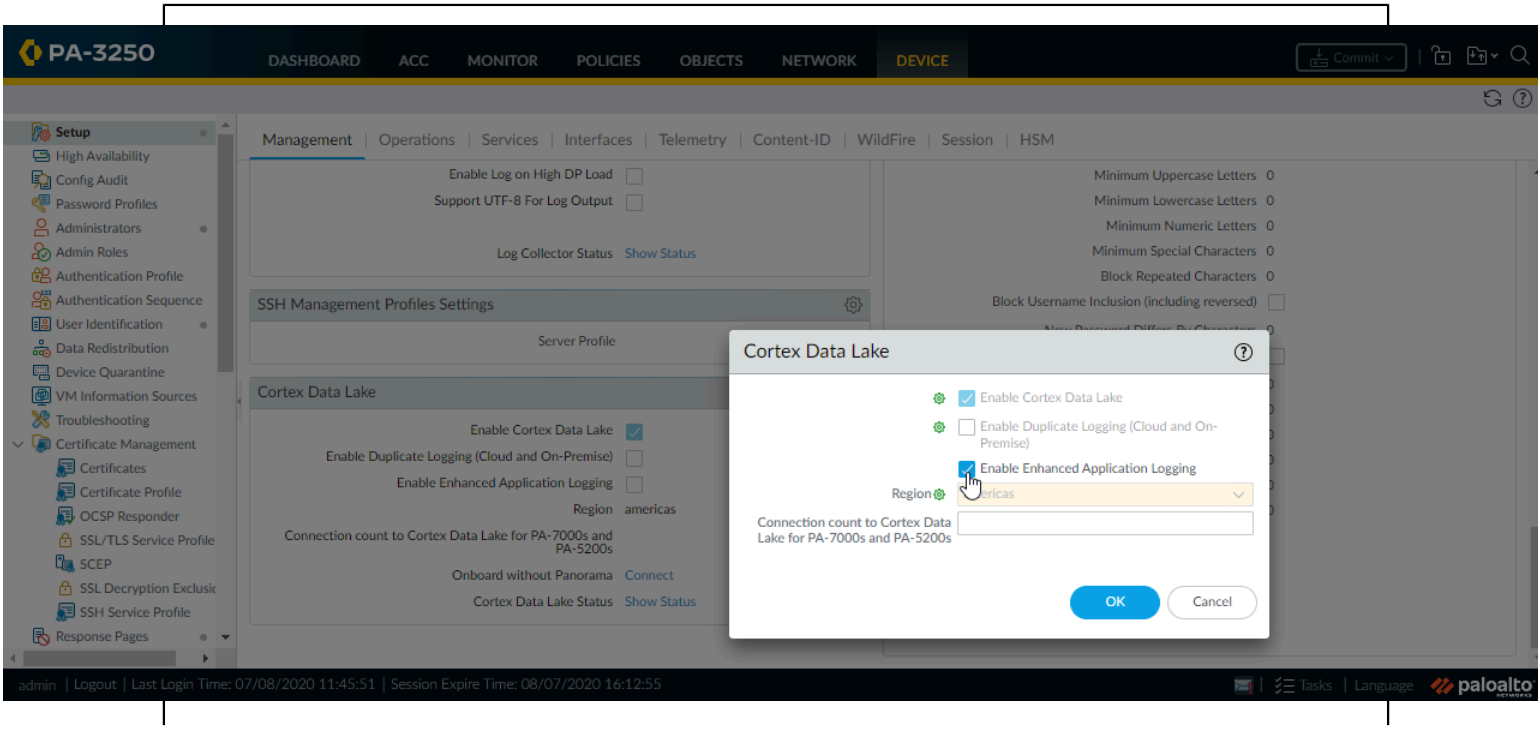
Pour commencer à transférer les journaux d'applications améliorés vers le lac de données Cortez, activez la journalisation améliorée des applications globalement, puis activez-la sur une base de règle de sécurité (à l'aide d'un profil de transfert de journal). Le paramètre global est requis et capture les données concernant le trafic qui ne sont pas basées sur la session (requêtes ARP, par exemple). Le paramètre de règle de stratégie est fortement recommandé ; la majorité des journaux d'applications améliorés sont collectés à partir du trafic basé sur la session que vos règles de stratégie de sécurité appliquent.

**STEP 1 |** La journalisation d'applications améliorée exige un abonnement à un lac de données Cortex ; User-ID est également recommandé. Voici les étapes à suivre pour commencer à utiliser le lac de données Cortex et activer User-ID.

**STEP 2 |** Pour **Enable Enhanced Application Logging (Activer la journalisation des applications améliorée)** sur le pare-feu, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** >

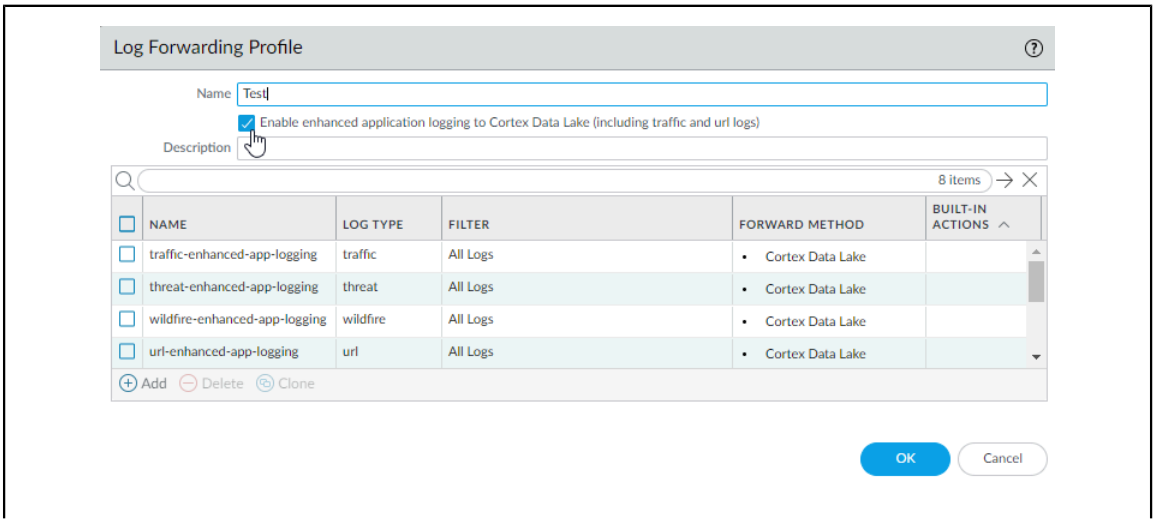
 

**Management (Gestion)** > **Cortex Data Lake (Lac de données Cortex)**, puis modifiez les paramètres du lac de données Cortex.




**STEP 3 |** Continuez à activer la journalisation des applications améliorée pour les règles de politique de sécurité qui contrôlent le trafic pour lequel vous souhaitez obtenir une visibilité étendue.

1. Sélectionnez **Objects (Objets)** > **Log Forwarding (Transfert des journaux)**, puis **Add (Ajoutez)** ou modifiez un profil de transfert de journal.
2. Mettez à jour le profil sur **Enable enhanced application logging to Cortex Data Lake (Permettre la journalisation améliorée des applications au lac de données Cortex) (y compris les journaux de trafic et les journaux URL)**.




Remarquez que, lorsque vous activez la journalisation améliorée des applications dans un profil de transfert de journal, les listes de correspondance qui spécifient les types de

journaux requis pour la journalisation des applications améliorées sont automatiquement ajoutées au profil.

3. Cliquez sur **OK** pour enregistrer le profil et continuez à mettre à jour autant de profils que nécessaire.
4. Assurez-vous que le profil de transfert de journal que vous avez mis à jour est associé à une règle de politique de sécurité, afin de déclencher la génération et la transmission du journal du trafic correspondant à la règle.
   1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** pour afficher les profils associés à chaque règle de politique de sécurité.
   2. Pour mettre à jour le profil de transfert de journal associé à une règle, **Add (Ajoutez)** ou modifiez la règle et sélectionnez **Policies (Politiques)** > **Security (Sécurité)** > **Actions** > **Log Forwarding (Transfert des journaux)**, puis sélectionnez le profil de transfert de journal activé faisant l'objet de la journalisation des applications améliorée.

# Administration des pare-feu

Les administrateurs peuvent configurer, gérer et surveiller des pare-feu Palo Alto Networks à l'aide de l'interface Web, de la CLI et de l'interface de gestion de l'API. Vous pouvez personnaliser l'accès administrateur basé sur les rôles aux interfaces de gestion afin de déléguer des tâches administratives spécifiques ou des autorisations à certains administrateurs.

# Interfaces de gestion

Vous pouvez utiliser les interfaces utilisateur suivantes pour gérer le pare-feu de Palo Alto Networks :

***N'activez pas l'accès de gestion aux zones sécurisées de votre entreprise à partir d'Internet ou de toute autre zone non approuvée. Suivez les*** Meilleures pratiques pour sécuriser l'accès administratif ***afin de vous assurer que vous sécurisez correctement votre pare-feu.***

- Utilisez l'Interface Web pour effectuer des tâches de configuration et de surveillance relativement facilement. Cette interface graphique vous permet d'accéder au pare-feu à l'aide de HTTPS (recommandé) ou HTTP et c'est le meilleur moyen d'effectuer des tâches administratives.
- Utilisez l'interface de ligne de commande (CLI) pour effectuer une série de tâches en entrant des commandes rapidement sur SSH (recommandé), Telnet ou le port de la console. L'interface de ligne de commande est une interface simple qui prend en charge deux modes de commande, opérationnel et configure, chacun avec une hiérarchie distincte de commandes et d'instructions. Lorsque vous êtes familiarisé avec la structure d'imbrication et la syntaxe des commandes, l'interface de ligne de commande fournit des temps de réponse rapides et une efficacité administrative.
- Utilisez l'API XML pour simplifier vos opérations et d'intégrer avec des applications existantes et des référentiels développés en interne. L'API XML est un service Web implémenté à l'aide de requêtes et de réponses HTTP / HTTPS.
- Utilisez Panorama pour effectuer la gestion Web, la création de rapports et la collecte de journaux pour plusieurs pare-feu. L'interface Web Panorama ressemble à l'interface Web du pare-feu, mais avec des fonctions supplémentaires pour la gestion centralisée.

# Utilisation de l'interface Web

Les rubriques suivantes expliquent comment utiliser l'interface Web du pare-feu. Pour plus d'informations sur les onglets et les champs spécifiques dans l'interface Web, reportez-vous au Guide de référence de l'interface Web.

- Lancement de l'interface Web
- Configuration des bannières, du message du jour et des logos
- Utilisation des indicateurs d'activité de connexion de l'administrateur pour détecter toute utilisation frauduleuse du compte
- Gestion et surveillance des tâches administratives
- Validation et Prévisualisation des modifications de configuration de pare-feu
- Exportation des données du tableau de configuration
- Utilisation de la recherche globale pour effectuer une recherche sur le serveur de gestion du pare-feu ou de Panorama
- Gérez les Verrous pour Restreindre les Modifications de Configuration

## Lancement de l'interface Web

Les navigateurs Web suivants sont pris en charge pour accéder à l'interface Web :

- Internet Explorer 11+
- Firefox 3.6+
- Safari 5+
- Chrome 11+

Effectuer les tâches suivantes pour lancer l'interface Web.

**STEP 1 |** Lancer un navigateur Internet et entrer l'adresse IP du pare-feu dans le champ URL (https://<IP address>).

*Par défaut, l'interface de gestion (MGT) autorise uniquement l'accès HTTPS à l'interface Web. Pour activer les autres protocoles, sélectionnez* ***Device (Périphérique)*** *>* ***Setup (Configuration)*** *>* ***Interfaces (Interfaces)*** *et modifiez les paramètres de l'interface de* ***Management (gestion)****.*

**STEP 2 |** Connectez-vous au pare-feu en fonction du type d'authentification utilisé pour votre compte. Si vous vous connectez au pare-feu pour la première fois, utilisez la valeur par défaut **admin** pour votre nom d'utilisateur et votre mot de passe.

- **SAML** : cliquez sur **Use Single Sign-On (Utiliser l'ouverture de session unique)**. Si le pare-feu exécute l'autorisation (attribution de rôle) pour les administrateurs, entrez votre **Username (Nom d'utilisateur)** et **Continue (Continuez)**. Si le fournisseur d'identité (IdP) SAML effectue l'autorisation, **Continue (Continuez)** sans entrer de **Username (Nom d'utilisateur)**. Dans les deux cas, le pare-feu vous redirige vers l'IdP, qui vous invite à entrer un nom d'utilisateur et un mot de passe. Après vous être authentifié auprès de l'IdP, l'interface Web du pare-feu s'affiche.

- **Tout autre type d'authentification** : entrez votre **Name (Nom)** d'utilisateur et votre **Password (Mot de passe)**. Lisez la bannière de connexion et sélectionnez **I Accept and Acknowledge the Statement Below (J'accepte et accuse réception de l'énoncé ci-dessous)** si la page de connexion dispose de la bannière et de la case à cocher. Cliquez ensuite sur **Login (Connexion)**.

**STEP 3 |** Lisez et **Close (fermer)** tous les messages de la journée.

## Configuration des bannières, du message du jour et des logos

Une ***bannière de connexion*** est un texte facultatif que vous pouvez ajouter à la page de connexion pour que les administrateurs prennent connaissance de renseignements qu'ils doivent connaître avant d'ouvrir une session. Par exemple, vous pourriez ajouter un message pour aviser les utilisateurs des restrictions quant à l'utilisation non autorisée du pare-feu.

Vous pouvez ajouter des bannières colorées qui mettent en valeur du texte superposé au haut (***bannière d'en-tête***) et au bas (***bannière de bas de page***) de l'interface Web afin de vous assurer que les administrateurs voient certaines informations cruciales, comme le niveau de classification pour l'administration du pare-feu.

Une boîte de dialogue présentant le ***message du jour*** s'affiche automatiquement après l'ouverture de session. Celle-ci présente les messages que Palo Alto Networks intègre pour mettre en évidence des renseignements importants associés à un logiciel ou à une version de contenu. Vous pouvez également ajouter un message personnalisé pour garantir que les administrateurs voient certains renseignements, comme le redémarrage imminent du système, qui pourraient avoir une incidence sur leurs tâches.

Vous pouvez remplacer les logos qui s'affichent par défaut sur la page de connexion et dans l'en-tête de l'interface Web par les logos de votre organisation.

**STEP 1 |** Configurez la bannière de connexion.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les paramètres généraux.
2. Saisissez la **Login Banner (Bannière de connexion)** (3 200 caractères maximum).
3. (Facultatif) Sélectionnez **Force Admins to Acknowledge Login Banner (Obliger les administrateurs à prendre acte de la bannière de connexion)** pour obliger les administrateurs à cocher une case **I Accept and Acknowledge the Statement Below (J'accepte et prends acte de l'énoncé ci-dessous)** située au-dessus du texte de la bannière pour activer le bouton de **Login (Connexion)**.
4. Cliquez sur **OK**.

**STEP 2 |** Définissez le message du jour.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les paramètres Banners and Messages (des bannières et des messages).
2. Activez le **Message of the Day (Message du jour)**.
3. Saisissez le **Message of the Day (Message du jour)** (3 200 caractères maximum).

   *Une fois que vous avez entré le message et cliqué sur **OK (OK)**, les administrateurs qui se connectent ensuite ainsi que les administrateurs actifs qui actualisent leur navigateur voient immédiatement le nouveau message ou le message mis à jour ; une validation n'est pas requise. Cela vous permet d'informer les autres administrateurs de l'imminence d'une validation qui pourrait avoir des incidences sur les changements qu'ils souhaitent apporter à leur configuration. Selon le moment de la validation précisé dans votre message, les administrateurs peuvent alors décider d'effectuer, d'enregistrer ou d'annuler leurs modifications.*
4. (Facultatif) Sélectionnez **Allow Do Not Display Again (Autoriser à ne plus afficher)** (option désactivée par défaut) pour donner aux administrateurs l'option de supprimer un message du jour lors de leur première ouverture de session. Chaque administrateur peut supprimer les messages de leurs propres ouvertures de session. Dans la boîte de dialogue présentant le message du jour, chaque message sera assorti de sa propre option de suppression.
5. (Facultatif) Saisissez un **Title (Titre)** d'en-tête pour le Message du jour (par défaut `Message of the Day`).

**STEP 3 |** Configurez l'en-tête et le pied-de-page des bannières.

*En utilisant une couleur vive pour l'arrière-plan d'une bannière et une couleur contrastante pour son texte, vous augmentez la probabilité que les administrateurs la remarquent et la lisent. Vous pouvez également utiliser des couleurs qui correspondent à des niveaux de classification au sein de votre organisation.*

1. Saisissez la **Header Banner (Bannière d'en-tête)** (3 200 caractères maximum).
2. (Facultatif) Décochez l'option **Same Banner Header and Footer (Bannières d'en-tête et de pied-de-page identiques)** (activée par défaut) pour utiliser des bannières d'en-tête et de pied-de-page différentes.
3. Saisissez la **Footer Banner (Bannière de pied-de-page)** (3 200 caractères maximum), si les bannières d'en-tête et de pied-de-page sont différentes.
4. Cliquez sur **OK**.

**STEP 4 |** Remplacez les logos qui apparaissent sur la page de connexion et dans l'en-tête.

*La taille maximale d'image d'un logo est de 128 Ko. Les types de fichiers pris en charge sont png et jpg. Le pare-feu ne prend pas en charge les fichiers d'image qui sont entrelacés ou qui contiennent des canaux alpha, car ces fichiers interfèrent avec la génération de rapports PDF.*

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)**, puis cliquez sur **Custom Logos (Logos personnalisés)** dans la section Miscellaneous (Divers).
2. Effectuez les étapes suivantes pour remplacer le logo du **Login Screen (Écran de connexion)** et celui de la **Main UI (Interface principale)** (en-tête) :
   1. Cliquez sur Télécharger.
   2. Sélectionnez une image d'un logo et cliquez sur **Open (Ouvrir)**.

      *Vous pouvez prévisualiser l'image pour voir comment elle sera rognée par PAN-OS pour qu'elle puisse tenir dans l'espace en cliquant sur l'icône de la loupe.*
   3. Cliquez sur **Close (Fermer)**.
3. **Commit (Validez)** vos modifications.

**STEP 5 |** Vérifiez que les bannières, le message du jour et les logos s'affichent comme il se doit.

1. Déconnectez-vous pour revenir à la page de connexion, où s'afficheront les nouveaux logos que vous avez sélectionnés.
2. Saisissez vos informations d'identification de connexion, passez en revue la bannière, sélectionnez **I Accept and Acknowledge the Statement Below (J'accepte et prends acte de l'énoncé ci-dessous)** pour activer le bouton de **Login (Connexion)**, puis **Login (Ouvrez une session)**.

   Une boîte de dialogue affiche le message du jour. Les messages que Palo Alto Networks intègre s'affichent sur des pages distinctes de la même boîte de dialogue. Pour naviguer parmi les pages, cliquez sur les flèches droite ou gauche situées sur les côtés de la boîte de dialogue ou cliquez sur un sélecteur de page ●○○○ dans la partie inférieure de la boîte de dialogue.
3. (Facultatif) Vous pouvez sélectionnez **Do not show again (Ne plus afficher)** pour le message que vous avez configuré et pour tout autre message que Palo Alto Networks a intégré.
4. **Close (Fermez)** la boîte de dialogue présentant le message du jour pour accéder à l'interface Web.

   Les bannières d'en-tête et de pied-de-page s'affichent sur toutes les pages de l'interface Web et présentent le texte et les couleurs que vous avez configurés. Le nouveau logo que vous avez sélectionné pour l'interface Web s'affiche sous la bannière d'en-tête.

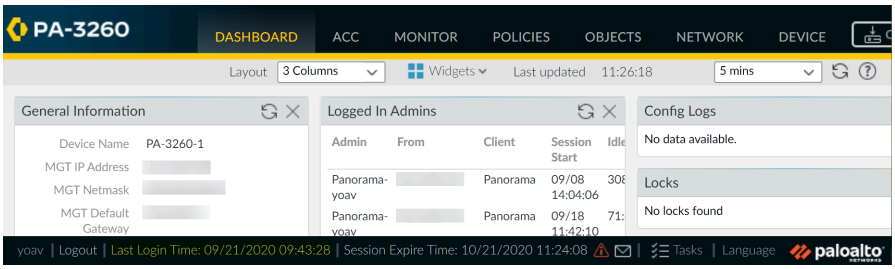
 

# Utilisation des indicateurs d'activité de connexion de l'administrateur pour détecter toute utilisation frauduleuse du compte

Les indicateurs de dernière connexion et de tentatives de connexion ayant échoué proposent un moyen visuel de détecter l'utilisation abusive de votre compte d'administrateur sur un pare-feu Palo Alto Networks ou serveur d'administration Panorama. Utilisez les informations de dernière connexion pour déterminer si quelqu'un d'autre s'est connecté avec vos informations d'identification et utilisez l'indicateur de tentatives de connexion ayant échoué pour déterminer si votre compte est visé par une attaque par force brute.

**STEP 1 |** Affichez les indicateurs d'activité de connexion pour surveiller les activités récentes sur votre compte.

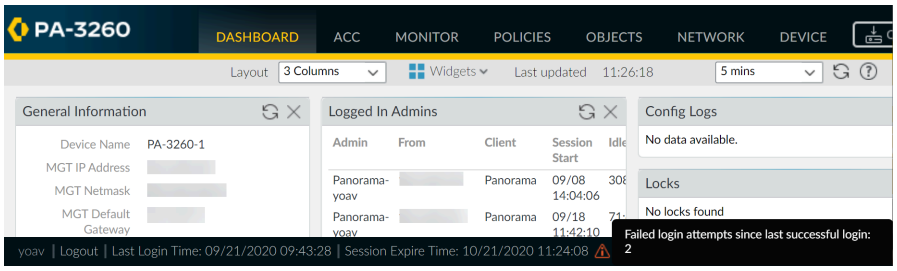
1. Connectez-vous à l'interface Web sur votre pare-feu ou le serveur de gestion de Panorama.
2. Affichez les détails de la dernière connexion situés en bas à gauche de la fenêtre et vérifiez que l'horodatage correspond à votre dernière connexion.




3. Recherchez un symbole d'avertissement sur la droite des informations d'heure de dernière connexion pour les tentatives de connexion infructueuses.

   L'indicateur de connexion infructueuse s'affiche si une ou plusieurs tentatives ayant échoué surviennent avec votre compte depuis la dernière connexion réussie.

   1. Si vous voyez le symbole d'avertissement, survolez-le pour afficher le nombre de tentatives de connexion ayant échoué.



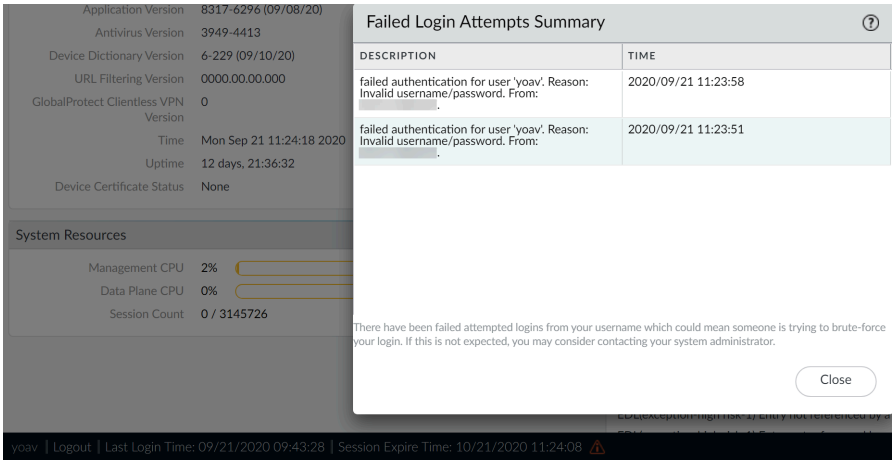

   2. Cliquez sur le symbole d'avertissement pour afficher le résumé des tentatives de connexion ayant échoué. Les détails comprennent le nom du compte administrateur, la raison de l'échec de connexion, l'adresse IP source et la date et l'heure.

> *Après avoir réussi à vous connecter et à vous déconnecter, le compteur de connexions ayant échoué se réinitialise à zéro. Lors de votre prochaine connexion, vous verrez donc les détails des nouvelles tentatives de connexion ayant échoué, le cas échéant.*

**STEP 2 |** Localisez les hôtes qui tentent continuellement de se connecter à votre pare-feu ou à votre serveur d'administration Panorama.

1. Cliquez sur le symbole d'avertissement de tentative de connexion ayant échoué pour afficher le résumé des tentatives de connexion ayant échoué.
2. Localisez et enregistrez l'adresse IP source de l'hôte ayant tenté de se connecter. Par exemple, l'illustration suivante montre plusieurs tentatives de connexion ayant échoué.




3. Travaillez avec votre administrateur réseau pour localiser l'utilisateur et l'hôte qui utilisent l'adresse IP que vous avez identifiée.

   Si vous ne parvenez pas à localiser le système qui effectue l'attaque en force brute, envisagez de renommer le compte pour empêcher de futures attaques.

**STEP 3 |** Prenez les mesures suivantes si vous détectez un compte compromis.

1. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Configuration (Configuration)** et affichez les changements de configuration et l'historique de validation pour déterminer si votre compte a été utilisé pour effectuer des modifications à votre insu.
2. Sélectionnez **Device (Périphérique)** > **Config Audit (Audit de configuration)** pour comparer la configuration actuelle et celle juste avant le changement de configuration

suspecté effectué à l'aide vos informations d'identification. Vous pouvez également le faire avec Panorama.

*Si votre compte administrateur a été utilisé pour créer un nouveau compte, effectuer un audit de configuration vous aide également à détecter les modifications associées aux comptes non autorisés.*

3. Si vous constatez que les journaux ont été supprimés ou si vous avez des difficultés à déterminer si des modifications inappropriées ont été effectuées à l'aide de votre compte, rétablissez la configuration afin d'obtenir une bonne configuration.

*Avant de valider une configuration précédente, vérifiez qu'elle contient les bons paramètres. Par exemple, la configuration sur laquelle vous revenez peut ne pas contenir les changements récents. Aussi, pensez à appliquer ces modifications après avoir validé la configuration de sauvegarde.*

*Utilisez les meilleures pratiques suivantes pour mieux prévenir les attaques en force brute sur les comptes privilégiés.*

- *Limitez le nombre de tentatives infructueuses autorisées avant le verrouillage d'un compte privilégié par le pare-feu en définissant le nombre d'échecs de connexion et la durée de verrouillage (min) dans le profil d'authentification ou dans les paramètres d'authentification pour l'interface de gestion (**Device (Périphérique) > Setup (Configuration) > Management (Gestion) > Authentication Settings (Paramètres d'authentification)**).*
- Utilisation des profils de gestion d'interface pour limiter l'accès.
- *Appliquez l'utilisation de* mots de passe complexes *pour les comptes privilégiés.*

## Gestion et surveillance des tâches administratives

Le Gestionnaire des tâches affiche des détails sur toutes les opérations initiées par vous et les autres administrateurs (par exemple, les validations manuelles) ou initiées par le pare-feu (telles que la génération de rapports planifiés) depuis le dernier redémarrage du pare-feu. Vous pouvez utiliser le Gestionnaire des tâches pour résoudre les échecs des opérations, étudier les avertissements associés aux validations terminées, afficher les détails sur les validations mises en file d'attente ou annuler les validations en attente.

*Vous pouvez également afficher les* Journaux du système *pour surveiller les événements système sur le pare-feu ou afficher* Journaux de configuration *pour surveiller les changements de configuration du pare-feu.*

**STEP 1 |** Cliquez sur **Tasks (Tâches)** au bas de l'interface web.

**STEP 2 |** **Show (Afficher)**uniquement les tâches **Running (en cours d'exécution)** (en cours) ou **All (Toutes)** les tâches (option par défaut). Facultativement, vous pouvez filtrer les tâches par type :

- **Jobs (Travaux)** : Les validations initiées par l'administrateur, les validations initiées par le pare-feu et les téléchargements et installations de logiciels ou de contenu.
- **Reports (Rapports)** : Rapports planifiés.
- **Log Requests (Requêtes de journal)** : Requêtes de journal que vous déclenchez en accédant au **Dashboard (Tableau de bord)** ou à une page de **Monitor (Surveillance)**.

**STEP 3 |** Effectuez l'une des actions suivantes :

- **Affichez ou masquez les détails de la tâche** (par défaut, le gestionnaire des tâches affiche le type, l'État, l'heure de début et les messages pour chaque tâche. Pour voir l'heure de fin et l'ID du travail pour une tâche, vous devez configurer manuellement l'affichage pour exposer ces colonnes. Pour afficher ou masquer une colonne, ouvrez la liste déroulante dans un en-tête de colonne, sélectionnez **Colonnes**, puis cochez ou décochez les noms de colonnes si nécessaire.
- **Examinez les avertissements ou les échecs** — Lisez les écritures de la colonne messages pour les détails de la tâche. Si la colonne indique `Too many messages (trop de messages)`, cliquez sur l'entrée dans la colonne Type pour afficher plus d'informations.
- **Affichez une description de validation**— si un administrateur a entré une description lors de la configuration d'une validation, vous pouvez cliquer sur **Commit Description (valider la description)** dans la colonne messages pour afficher la description.
- **Vérifiez la position d'une validation dans la file d'attente** : la colonne messages indique la position dans la file d'attente des validations en cours.
- **Annuler la validation en attente** : Cliquez sur **Clear Commit Queue (effacer la file d'attente de validation)**pour annuler toutes les validations en attente (disponible uniquement pour les rôles administratifs prédéfinis). Pour annuler une validation individuelle, cliquez sur **x** dans la colonne action (la validation reste dans la file d'attente jusqu'à ce que le pare-feu la retire). Vous ne pouvez pas annuler les validations qui sont en cours.

## Validation et Prévisualisation des modifications de configuration de pare-feu

Une validation est le processus par lequel des modifications en attente d'être apportées à la configuration du pare-feu sont activées. Vous pouvez filtrer les modifications en attente par l'administrateur ou l'***emplacement*** et ensuite prévisualiser, valider ou confirmer uniquement ces modifications. Les emplacements peuvent être des systèmes virtuels spécifiques, des politiques et des objets partagés ou des paramètres de périphériques et de réseau partagés.

Le pare-feu met en attente les demandes de validation afin que vous puissiez lancer une nouvelle validation lorsqu'une validation précédente est en cours. Le pare-feu exécute les validations dans l'ordre dans lequel elles sont initiées, mais donne la priorité aux validations que le pare-feu initie automatiquement, comme les actualisations du nom de domaine complet. Cependant, si la file d'attente possède déjà le nombre maximum de validations lancées par l'administrateur, vous devez attendre que le pare-feu termine le traitement d'une validation en attente avant d'en lancer une nouvelle. Pour annuler des validations en attente ou pour voir les détails des validations, quel que soit leur état, reportez-vous à la section Gestion et surveillance des tâches administratives.

Lorsque vous lancez une validation, le pare-feu vérifie la validité des modifications avant de les activer. La sortie de validation affiche les conditions qui bloquent la validation (erreurs) ou qui sont importantes à savoir (avertissements). Par exemple, la validation peut indiquer une destination d'itinéraire non valide que vous devez corriger pour que la validation réussisse. Le processus de validation vous permet de trouver et de corriger les erreurs avant la validation (il ne modifie pas la configuration en cours d'exécution). Cette option est utile si vous avez une fenêtre de validation fixe et que vous souhaitez vous assurer que la validation sera une réussite exempte d'erreur.

Lorsqu'ils sont activés et gérés par un serveur de gestion Panorama™, les pare-feu gérés testent localement la configuration validée localement ou transmise depuis Panorama pour vérifier que les nouvelles modifications n'interrompent pas la connexion entre Panorama et le pare-feu géré. Si la configuration validée rompt la connexion entre Panorama et un pare-feu géré, la validation par le pare-feu échoue automatiquement et la configuration active précédente est alors rétablie. De plus, les pare-feu gérés par un serveur de gestion Panorama testent leur connexion à Panorama toutes les 60 minutes et si un pare-feu géré détecte qu'il ne peut plus se connecter avec succès à Panorama, il revient à la configuration précédente.

*Les opérations Confirmer, Valider, Prévisualiser, Enregistrer et Rétablir ne s'appliquent qu'aux modifications apportées après la dernière validation. Pour rétablir les configurations à leur état d'avant la dernière validation, vous devez* charger une configuration précédemment sauvegardée.

*Pour empêcher plusieurs administrateurs d'effectuer des modifications de configuration lors des sessions simultanées, voir* gérer les verrous pour restreindre les modifications de configuration.

**STEP 1 |** Configurez l'étendue des modifications apportées à la configuration que vous allez valider, confirmer ou prévisualiser.

1. Cliquez sur **Commit (Valider)** en haut de l'interface Web.
2. Sélectionnez l'une des options suivantes :
   - **Commit All Changes (Valider tous les changements)** (par défaut) : applique la validation à tous les changements pour lesquels vous détenez des privilèges d'administrateur. Vous ne pouvez filtrer manuellement l'étendue de validation lorsque vous sélectionnez cette option. Au lieu de cela, le rôle d'administrateur affecté au compte que vous avez utilisé pour vous connecter détermine l'étendue de validation.
   - **Commit Changes Made By (Valider les changements apportés par)** : vous permet de filtrer l'étendue de validation par administrateur ou emplacement. Le rôle administrateur affecté au compte que vous avez utilisé pour vous connecter détermine les changements que vous pouvez filtrer.

   *Pour valider les changements d'autres administrateurs, le compte que vous utilisez pour vous connecter doit s'être vu affecté le rôle de super-utilisateur ou un* profil de rôle administrateur *pour lequel le privilège de* ***Commit For Other Admins (Valider pour le compte d'autres administrateurs)*** *doit être activé.*
3. (Facultatif) Pour filtrer l'étendue de validation par administrateur, sélectionnez **Commit Changes Made By (Valider les changements apportés par)**, cliquez sur le lien adjacent, sélectionnez les administrateurs, puis cliquez sur **OK**.

4. (Facultatif) Pour filtrer par emplacement, sélectionnez **Commit Changes Made By (Valider les changements apportés par)** et supprimez les changements que vous souhaitez exclure de l'étendue de validation.

   *Si des dépendances entre les changements de configuration que vous avez inclus et ceux que vous avez exclus entraînent une erreur de validation, effectuez une validation qui comprend tous les changements. Par exemple, lorsque vous validez des modifications apportées à un système virtuel, vous devez inclure les modifications de tous les administrateurs qui ont ajouté, supprimé ou repositionné des règles pour la même base de règles dans ce système virtuel.*

**STEP 2 |** Prévisualisez les modifications que la validation activera.

Cela peut être utile si, par exemple, vous ne vous souvenez pas de tous vos changements et vous n'êtes pas sûr de vouloir tous les activer.

Le pare-feu compare les configurations que vous avez sélectionnées dans la Commit Scope (Étendue de validation) de la configuration en cours d'exécution. La fenêtre de prévisualisation affiche les configurations côte à côte et utilise un code couleur pour indiquer quelles modifications sont des ajouts (en vert), des modifications (en jaune) ou des suppressions (en rouge).

**Preview Changes (Prévisualiser les modifications)** et sélectionnez les **Lines of Context (Lignes du contexte)**, soit le nombre de lignes (des fichiers de configuration comparés) à afficher avant et après chaque différence mise en surbrillance. Ces lignes supplémentaires vous aident à corréler la sortie de prévisualisation dans les paramètres de l'interface Web. Fermez la fenêtre d'aperçu lorsque vous avez terminé l'examen des modifications.

*Étant donné que les résultats de prévisualisation s'affichent dans une nouvelle fenêtre de navigateur, votre navigateur doit autoriser les fenêtres contextuelles. Si la fenêtre de prévisualisation ne s'ouvre pas, reportez-vous à la documentation de votre navigateur pour connaître les étapes permettant d'autoriser les fenêtres contextuelles.*

**STEP 3 |** Prévisualisez les paramètres individuels pour lesquels vous effectuez des modifications,

ce qui peut s'avérer utile si vous souhaitez connaître les détails des changements, comme les types de paramètres et la personne qui les a modifiés.

1. Cliquez sur **Change Summary (Récapitulatif des modifications)**.
2. (Facultatif) **Group By (Regrouper par)** nom de colonne (comme le **Type** de paramètre).
3. **Close (Fermez)** la boîte de dialogue Change Summary (Récapitulatif des modifications) lorsque vous avez terminé l'examen des modifications.

**STEP 4 |** Confirmez les modifications avant de procéder à la validation afin d'en garantir la réussite.

1. **Validate Changes (Validez les modifications)**.

   Les résultats présentent toutes les erreurs et tous les avertissements qu'une validation afficherait.
2. Résolvez les erreurs que les résultats de validation identifient.

**STEP 5 |** Validez vos modifications de configuration.

**Commit (Confirmez)** vos modifications pour les valider et les rendre actives.

*Pour afficher les détails des validations en attente (que vous pouvez toujours annuler), en cours d'exécution, terminées ou qui ont échouées, reportez-vous à la section* Gestion et surveillance des tâches administratives.

# Exportation des données du tableau de configuration

Exportez les règles de politique, les objets de configuration et les signatures de Panorama™ et des pare-feu pour démontrer votre conformité réglementaire aux auditeurs externes, pour mener des examens périodiques de la configuration des pare-feu et pour générer des rapports sur les politiques des pare-feu. Cette approche vous permet d'éviter de donner aux auditeurs un accès direct à vos pare-feu et à vos appareils, de faire des captures d'écran ou d'accéder à l'API XML pour générer des rapports de configuration. À partir de l'interface Web, vous pouvez exporter les données du tableau de configuration propres aux configurations des politiques, des objets, du réseau, du pare-feu et de Panorama ainsi que les exceptions de signatures qui se trouvent dans les profils de sécurité Antivirus, Antispyware et Protection contre les vulnérabilités, soit au format PDF ou CSV.

L'exportation du tableau de configuration fonctionne de la même manière qu'une fonction d'impression : vous ne pouvez réimporter les fichiers générés dans Panorama ou dans le pare-feu. Lorsque vous exportez les données en tant que fichier PDF et que les données du tableau dépassent 50 000 lignes, les données sont alors divisées en plusieurs fichiers PDF (par exemple, report-name>_part1.pdf et report-name>_part2.pdf) Lorsque vous exportez les données dans un fichier CSV, elles sont exportées dans un seul fichier. Ces formats d'exportation vous permettent d'appliquer des filtres qui correspondent à vos critères d'établissement de rapports et de chercher dans les rapports PDF afin de trouver rapidement des données spécifiques. De plus, lorsque vous exportez les données du tableau de configuration, un journal système est généré pour consigner l'événement.

**STEP 1 |** Lancez l'interface Web et déterminez les données de configuration que vous devez exporter.

**STEP 2 |** Appliquez les filtres au besoin pour produire les données de configuration que vous devez exporter et cliquez sur **PDF/CSV**.


**STEP 3 |** Configurez le rapport d'Exportation du tableau de configuration :

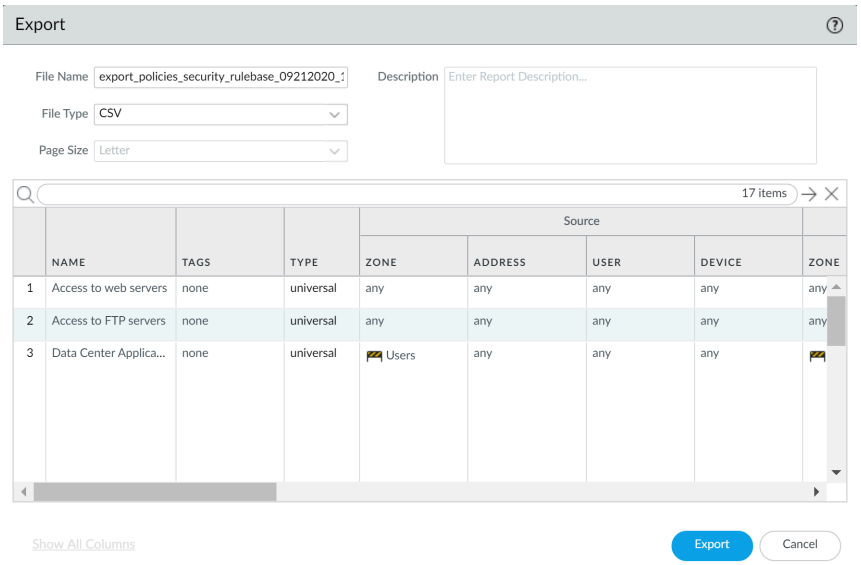
1. Saisissez un **File Name (Nom de fichier)**.
2. Sélectionnez le **File Type (Type de fichier)**.
3. (Facultatif) Saisissez une Description de rapport.
4. Confirmez que les données du tableau de configuration correspondent aux filtres que vous avez appliqués.

*Sélectionnez **Show All Columns (Montrer toutes les colonnes)** pour montrer tous les filtres appliqués.*

**STEP 4 |** **Export (Exportez)** les données du tableau de configuration.

L'exportation du tableau de configuration fonctionne de la même manière qu'une fonction d'impression : vous ne pouvez réimporter les fichiers générés dans Panorama ou dans le pare-feu.




**STEP 5 |** Sélectionnez l'emplacement où enregistrer le fichier exporté.

## Utilisation de la recherche globale pour effectuer une recherche sur le serveur de gestion du pare-feu ou de Panorama

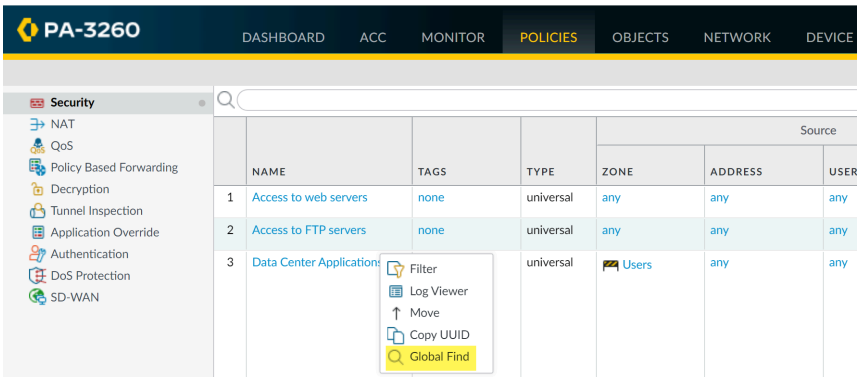
La recherche globale vous permet de rechercher une chaîne particulière, telle qu'une adresse IP, un nom d'objet, un nom de règle de politique, un ID de menace, un UUID ou un nom d'application, dans la configuration candidate sur un pare-feu ou Panorama. En plus de rechercher des paramètres et objets de configuration, vous pouvez rechercher par ID de tâche ou type de tâche pour les validations manuelles effectuées par les administrateurs ou les validations automatiques effectuées par le pare-feu ou Panorama. Les résultats de la recherche sont regroupés par catégorie et fournissent des liens vers l'emplacement de la configuration dans l'interface Web, de manière à pouvoir trouver facilement tous les endroits où la chaîne a été référencée. Les résultats de la recherche vous permettent également d'identifier d'autres objets qui dépendent du terme ou de la chaîne de recherche, ou lui font référence. Par exemple, pour déprécier un profil de sécurité, saisissez le nom du profil dans la recherche globale pour rechercher toutes les instances du profil, puis cliquez sur chaque instance pour accéder à la page de configuration et apportez la modification nécessaire. Toutes les références sont supprimées et vous pouvez alors supprimer le profil. Vous pouvez effectuer cette opération pour chaque élément de configuration qui a des dépendances.

Regardez la vidéo.

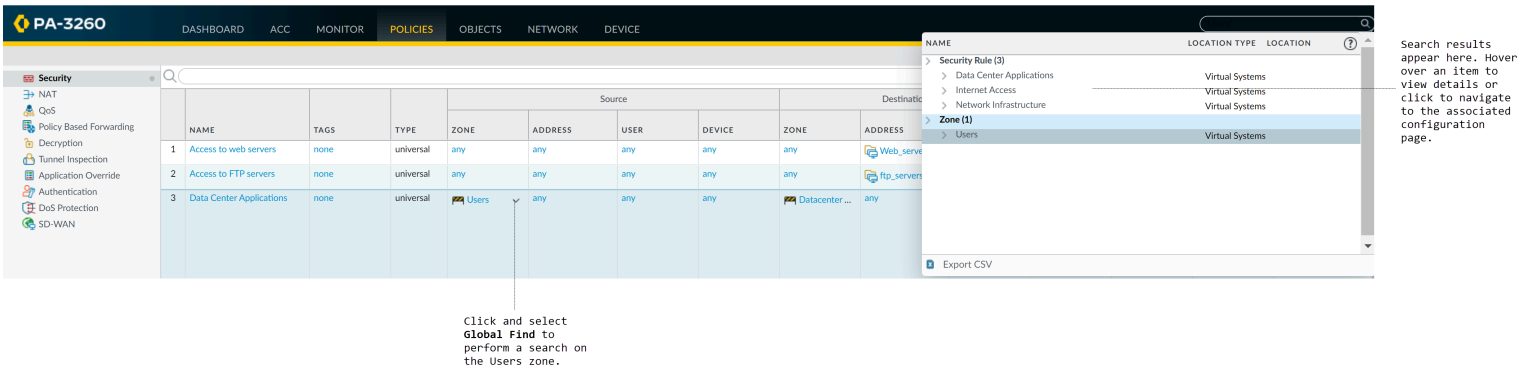
*La recherche globale ne recherche aucun contenu dynamique (tel que les journaux, les plages d'adresses ou les adresses DHCP allouées). Dans le cas de DHCP, vous pouvez faire porter la recherche sur un attribut de serveur DHCP, tel que l'entrée NS, mais vous ne pouvez pas rechercher d'adresses allouées aux utilisateurs. La recherche globale ne recherche pas de noms d'utilisateurs ou de groupes identifiés par User-ID, à moins que l'utilisateur/le groupe ne soit défini dans une politique. En général, vous pouvez faire porter la recherche uniquement sur du contenu que le pare-feu écrit dans la configuration.*

- Lancez la recherche globale en cliquant sur l'icône **Search (Rechercher)** située dans le coin supérieur droit de l'interface Web.


- Pour accéder à la Recherche globale depuis une zone de configuration, sélectionnez la liste déroulante en regard d'un élément, puis **Global Find (Recherche globale)**.




Par exemple, cliquez sur **Global Find (Recherche globale)** dans une zone nommée **Users (Utilisateurs)** pour rechercher chaque emplacement où la zone est référencée dans la configuration candidate. La capture d'écran suivante affiche les résultats de la recherche pour la zone Users :




Conseils de recherche :

- Si vous effectuez une recherche sur un pare-feu avec plusieurs systèmes virtuels ou si des Types de rôle d'administration personnalisés sont définis, la recherche globale renvoie

uniquement les résultats des zones du pare-feu pour lesquelles l'administrateur dispose d'autorisations. La même chose s'applique aux groupes de périphériques sur Panorama.

- Les espaces entre les termes de la recherche sont traités comme des opérations ET. Par exemple, si vous faites porter la recherche sur une **`politique d'entreprise`**, les résultats de la recherche incluent les instances où les termes entreprise et politique existent dans la configuration.
- Pour rechercher une expression exacte, mettez-la entre guillemets.
- N'entrez pas plus de cinq mots-clés ou utilisez une correspondance de phrase exacte avec des guillemets.
- Pour relancer une ancienne recherche, cliquez sur l'icône Rechercher (située dans le coin supérieur droit de l'interface Web). Une liste des 20 dernières recherches s'affiche alors. Cliquez sur un élément dans la liste pour relancer cette recherche. L'historique de recherche est unique pour chaque compte administrateur.
- Pour chercher un UUID, vous devez copier et coller l'UUID.

# Gérez les Verrous pour Restreindre les Modifications de Configuration

Vous pouvez utiliser des verrous de configuration pour empêcher les autres administrateurs de modifier la configuration candidate ou de valider les modifications de configuration jusqu'à ce que vous supprimiez manuellement le verrou ou que le pare-feu le supprime automatiquement (après une validation). Les verrous garantissent que les administrateurs ne rendent pas les modifications contradictoires aux mêmes paramètres ou paramètres interdépendants pendant les sessions de connexion simultanées.

***Le pare-feu met en files d'attente de validation les requêtes et les exécute dans l'ordre où les administrateurs lancent les validations. Pour plus de détails, voir*** Validation et Prévisualisation des modifications de configuration de pare-feu***. Pour afficher le statut de la tâche reportez-vous à la section*** Gestion et surveillance des tâches administratives**.**

1. Voir les détails sur les verrous actuels.

   Par exemple, vous pouvez vérifier si d'autres administrateurs ont défini des verrous et lire les commentaires qu'ils ont entrés pour expliquer les verrous.

   Cliquez sur le verrou  en haut de l'interface Web. Un nombre adjacent indique le nombre de verrous actuels.

- Verrouillez une configuration.
  1. Cliquez sur le verrou en haut de l'interface Web.

     *L'icône varie selon que les verrous existants sont ou ne sont pas définis.*

  2. **Take a Lock (Prenez un verrou)** et sélectionnez le **Type** de verrou :
     - **Config (Configuration)**: empêche d'autres administrateurs de modifier la configuration candidate.
     - **Commit (Verrou de validation)** – Empêche d'autres administrateurs de valider des modifications apportées à la configuration candidate.
  3. (Pare-feu avec plusieurs systèmes virtuels uniquement) Sélectionner un **Location (Emplacement)** pour verrouiller la configuration pour un système virtuel spécifique ou l'emplacement **Shared (partagé)**.
  4. (Facultatif) Comme meilleure pratique, entrez un **Comment (Commentaire)** afin que les autres administrateurs comprennent la raison du verrouillage.
  5. Cliquez sur **OK** et **Close (Fermez)**.

- Déverrouiller une configuration.

  Seul un super-utilisateur ou l'administrateur qui a verrouillé la configuration peut la déverrouiller manuellement. Toutefois, le pare-feu supprime automatiquement un verrou après l'exécution de l'opération de validation.

  1. Cliquez sur le verrou en haut de l'interface Web.
  2. Sélectionnez l'entrée de verrou dans la liste.
  3. Cliquez sur **Remove Lock (supprimer le verrou)**, **OK**, et **Close (fermer)**.

- Configurez le pare-feu pour qu'il applique automatiquement un verrou de validation lorsque vous modifiez la configuration candidate. Ce paramètre s'applique à tous les administrateurs.
  1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les paramètres généraux.
  2. Sélectionnez **Automatically Acquire Commit Lock (Acquérir automatiquement un verrou de validation)**, puis cliquez sur **OK** et **Commit (Valider)**.

# Gestion des sauvegardes de configuration

La configuration en cours sur le pare-feu comprend tous les paramètres que vous avez validés et qui sont donc actifs, tels que les règles de stratégie qui bloquent ou autorisent actuellement différents types de trafic sur votre réseau. La configuration candidate est une copie de la configuration en cours plus les modifications inactives effectuées après la dernière validation. La sauvegarde des versions de la configuration en cours d'exécution ou candidate vous permet de restaurer ultérieurement ces versions. Par exemple, si une validation montre que la configuration candidate actuelle a plus d'erreurs que vous ne souhaitez réparer, vous pouvez restaurer une configuration candidate précédente. Vous pouvez également revenir à la configuration en cours sans enregistrer d'abord une sauvegarde. Si vous devez exporter des parties spécifiques de la configuration pour une révision ou un audit interne, vous pouvez exporter les données de la table de configuration.

***Reportez-vous à la section*** Validation et Prévisualisation des modifications de configuration aux pare-feu ***pour plus de détails sur les opérations de validation.***

- Sauvegarde et exportation de configurations de pare-feu
- Annuler des modifications apportées à la configuration d'un pare-feu

## Sauvegarde et exportation de configurations de pare-feu

Sauvegarder une copie de la configuration candidate au stockage permanent dans le pare-feu vous donne la possibilité de revenir plus tard à cette version (reportez-vous à la section Annuler des modifications apportées à la configuration d'un pare-feu). Cela s'avère utile pour conserver des modifications qui risqueraient autrement d'être perdues en cas d'événement système ou d'action administrateur entraînant le redémarrage du pare-feu. Après redémarrage, PAN-OS revient à la version actuelle de la configuration active, que le pare-feu sauvegarde dans un fichier nommé running-config.xml. Sauvegarder une copie s'avère également utile lorsque vous souhaitez rétablir les paramètres d'une configuration du pare-feu antérieure à la version actuelle de la configuration active. Le pare-feu n'enregistre pas automatiquement la configuration candidate au stockage permanent. Vous devez enregistrer manuellement la configuration du candidat comme un fichier instantané par défaut (snapshot.xml) ou comme un fichier instantané personnalisé. Le pare-feu sauvegarde le fichier instantané en local mais vous pouvez l'exporter vers un hôte externe.

*Vous n'avez pas à sauvegarder une copie de configuration pour annuler les modifications apportées depuis la dernière validation ou le dernier redémarrage ; il suffit de sélectionner* ***Config (Configuration)*** *>* ***Revert Changes (Annulez les modifications)*** *(reportez-vous à la section* Annuler des modifications apportées à la configuration d'un pare-feu*).*

*Lorsque vous modifiez des paramètres et que vous cliquez sur* ***OK****, le pare-feu met à jour la version candidate mais ne sauvegarde pas d'instantané de copie.*

*De plus, le fait de sauvegarder des modifications ne les active pas. Afin d'activer des modifications, effectuez une validation (reportez-vous à la section* Validation et prévisualisation des modifications de configuration apportées aux pare-feu*).*

*Palo Alto Networks vous conseille d'effectuer une sauvegarde de toute configuration importante sur un hôte externe au pare-feu.*

**STEP 1 |** Enregistrez un instantané de sauvegarde de la configuration candidate localement si elle contient des modifications que vous souhaitez préserver en cas de redémarrage du pare-feu.

Il s'agit de modifications que vous n'êtes pas prêt à valider, par exemple, des modifications que vous ne pouvez terminer au cours de la session de connexion actuelle.

Pour remplacer l'instantané par défaut (.snapshot.xml) avec toutes les modifications apportées par tous les administrateurs, effectuez l'une des tâches suivantes :

- Sélectionnez **Device (Périphérique)** > **Setup (Paramétrage)** > **Operations (Opérations)** et **Save candidate configuration (Sauvegardez la version candidate)**.
- Connectez-vous au pare-feu avec un compte administrateur disposant de l'autorisation Super Utilisateur ou un Profil de rôle utilisateur avec le privilège **Save For Other Admins (Sauvegarder pour le compte d'autres administrateurs)** activé. Sélectionnez ensuite **Config (Configuration)** > **Save Changes (Sauvegardez les modifications)** dans la partie supérieure de l'interface web, sélectionnez **Save All Changes (Sauvegardez toutes les modifications)** et **Save (Sauvegardez)**.

Pour créer un instantané qui inclut toutes les modifications apportées par tous les administrateurs, mais sans écraser le fichier instantané par défaut :

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)** et **Save named configuration snapshot (enregistrez l'instantané de configuration nommé)**.
2. Saisissez le **Name (Nom)** du nouveau fichier de configuration ou celui existant.
3. Cliquez sur **OK** et **Close (Fermez)**.

Pour sauvegarder uniquement certaines modifications apportées à la configuration candidate sans écraser des parties du fichier instantané par défaut :

1. Connectez-vous au pare-feu avec un compte administrateur disposant de privilèges d'accès requis pour sauvegarder les modifications souhaitées.
2. Sélectionnez **Config (Configuration)** > **Save Changes (Sauvegardez les modifications)** dans la partie supérieure de l'interface web.
3. Sélectionnez **Save Changes Made By (Sauvegardez les modifications apportées par)**.

4. Pour filtrer la portée d'enregistrement par administrateur, cliquez sur **<administrator-name> (nom de l'administrateur)**, choisissez les administrateurs, et cliquez sur **OK**.
5. Pour filtrer le champ de sauvegardes par emplacement, effacer tout emplacement à exclure. Les emplacements peuvent être des systèmes virtuels spécifiques, des politiques et des objets partagés ou des paramètres de périphériques et de réseau partagés.
6. Cliquez sur **Save (Enregistrer)**, spécifiez le **Name (Nom)** d'un nouveau fichier de configuration ou d'un fichier de configuration existant et cliquez sur **OK**.

**STEP 2 |** Exportez une configuration candidate, une configuration en cours d'exécution, ou les informations relatives à l'état du pare-feu vers un hôte externe ou vers le pare-feu.

Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)** et cliquez sur une option d'exportation :

- **Export named configuration snapshot (Exporter l'instantané de configuration nommée)** - exportez la configuration en cours d'exécution, un instantané de configuration candidate nommé ou une configuration précédemment importée (candidate ou en cours d'exécution). Le pare-feu exporte la configuration sous forme de fichier XML avec le **Name (Nom)** que vous avez indiqué.
- **Export configuration version (Exporter la version de configuration)** - sélectionnez une **Version** de la configuration en cours d'exécution pour l'exporter sous forme de fichier XML. Le pare-feu crée une version à chaque fois que vous validez des modifications de configuration.
- **Export Device state (Exporter l'état du périphérique)** - exportez les informations relatives à l'état du pare-feu sous la forme d'un module. Outre la configuration active, les informations relatives à l'état comprennent le groupe de périphériques et les paramètres du modèle poussés par Panorama. Si le pare-feu est un portail GlobalProtect, les informations comprennent également des informations relatives au certificat, une liste des satellites et les informations d'authentification des satellites. Si vous remplacez un pare-feu ou un portail, vous pouvez restaurer les informations exportées relatives au remplacement en important le module d'état.

## Annuler des modifications apportées à la configuration d'un pare-feu

Les opérations d'annulation remplacent la configuration candidate actuelle avec des réglages d'une autre configuration. Annuler des modifications s'avère utile lorsque vous voulez revenir sur des modifications apportées à tous les paramètres en une seule opération plutôt que de reconfigurer manuellement chaque paramètre.

Vous pouvez annuler des modifications en cours apportées au pare-feu depuis la dernière validation. Le pare-feu fournit l'option de filtrer les modifications en cours en fonction des administrateurs ou des ***emplacements***. Les emplacements peuvent être des systèmes virtuels spécifiques, des politiques et des objets partagés ou des paramètres de périphériques et de réseau partagés. Si vous avez créé un instantané pour une configuration candidate qui est antérieure à la configuration active (reportez-vous à Sauvegarde et exportation de configurations de pare-feu), vous pouvez aussi revenir à cet instantané. Revenir à un instantané vous permet de restaurer une configuration candidate existant avant la dernière validation. Le pare-feu enregistre automatiquement une nouvelle version de la configuration active lorsque vous validez des modifications, et vous pouvez rétablir n'importe laquelle de ces versions.

- Revenir à la configuration active (fichier nommé running-config.xml).

  Cette opération annule les modifications apportées à la configuration candidate depuis la dernière validation.

  Pour annuler toutes les modifications apportées par tous les administrateurs, effectuez l'une des tâches suivantes :

  - Sélectionnez **Device (Périphérique)** > **Setup (Paramétrage)** > **Operations (Opérations)**, **Revert to running configuration (Revenir à la dernière configuration enregistrée)**, et cliquez sur **Yes (Oui)** pour confirmer l'opération.
  - Connectez-vous au pare-feu avec un compte administrateur disposant de l'autorisation Super Utilisateur ou un Profil de rôle utilisateur avec le privilège **Commit For Other Admins (Valider pour le compte d'autres administrateurs)** activé. Sélectionnez ensuite **Config (Configuration)** > **Revert Changes (Annuler les modifications)** dans la partie supérieure de l'interface web, sélectionnez **Revert All Changes (Annulez toutes les modifications)** et **Revert (Annulez)**.

  Pour annuler uniquement des changements spécifiques à la configuration candidate :

  1. Connectez-vous au pare-feu avec un compte administrateur disposant de privilèges d'accès requis pour annuler les modifications souhaitées.

     *Les privilèges contrôlant les opérations de validation contrôlent également les opérations d'annulation.*
  2. Sélectionnez **Config (Configuration)** > **Revert Changes (Annulez les modifications)** dans la partie supérieure de l'interface web.
  3. Sélectionnez **Revert Changes Made By (Annulez les modifications apportées par)**.
  4. Pour filtrer le champ d'annulations par administrateur, cliquez sur **<administrator-name> (nom de l'administrateur)**, choisissez les administrateurs, et cliquez sur **OK**.
  5. Pour filtrer le champ d'annulations par emplacement, effacez tout emplacement à exclure.
  6. **Revert (Annulez)** les modifications.

- Revenir à l'instantané par défaut de la configuration candidate.

  Il s'agit de l'instantané que vous créez ou écrasez lorsque vous cliquez sur **Config (Configuration)** > **Save Changes (Sauvegardez les modifications)** dans la partie supérieure de l'interface web.

  1. Sélectionnez **Device (Périphérique)** > **Setup (Paramétrage)** > **Operations (Opérations)** et **Revert to last saved configuration (Revenir à la dernière configuration enregistrée)**.
  2. Cliquez sur **Yes (Oui)** pour confirmer l'opération.
  3. (Facultatif) Cliquez sur **Commit (Validez)** pour remplacer la configuration active avec l'instantané.

- Revenir à une version précédente de la configuration active qui est stockée sur le pare-feu.

  Le pare-feu crée une version à chaque fois que vous validez des modifications de configuration.

  1. Sélectionnez **Device (Périphérique)** > **Setup (Paramétrage)** > **Operations (Opérations)** et **Load configuration version (Chargez la version de la configuration)**.
  2. Sélectionnez une **Version** de configuration et cliquez sur **OK**.
  3. (Facultatif) Cliquez sur **Commit (Validez)** pour remplacer la configuration active avec la version que vous venez de rétablir.

- Revenir à l'un des états suivants :

  - Version au nom personnalisé de la configuration active que vous avez importé antérieurement.
  - Instantané au nom personnalisé de la configuration candidate (plutôt que l'instantané par défaut).

  1. Sélectionnez **Device (Périphérique)** > **Setup (Paramétrage)** > **Operations (Opérations)** et cliquez sur **Load named configuration snapshot (Chargez l'instantané de la configuration)**.
  2. Sélectionnez le **Name (Nom)** de l'instantané et cliquez sur **OK**.
  3. (Facultatif) Cliquez sur **Commit (Validez)** pour remplacer la configuration active avec l'instantané.

- Revenir à une configuration en cours d'exécution ou une configuration candidate que vous avez précédemment exportée vers un hôte externe.

  1. Sélectionnez **Device (Périphérique)** > **Setup (Paramétrage)** > **Operations (Opérations)**, cliquez sur **Import named configuration snapshot (Importez l'instantané de configuration)**, **Browse (Accédez)** au fichier de configuration sur l'hôte externe, puis cliquez sur **OK**.
  2. Cliquez sur **Load named configuration snapshot (Charger l'instantané de la configuration)**, sélectionnez le **Name (Nom)** du fichier de configuration que vous venez d'importer et cliquez sur **OK**.
  3. (Facultatif) Cliquez sur **Commit (Validez)** pour remplacer la configuration active avec l'instantané que vous venez d'importer.

- Restaurez les informations relatives à l'état que vous avez exportées d'un pare-feu.

  Outre la configuration active, les informations relatives à l'état comprennent le groupe de périphériques et les paramètres du modèle poussés par Panorama. Si le pare-feu est un portail GlobalProtect, les informations comprennent également des informations relatives au certificat, une liste des satellites et les informations d'authentification des satellites. Si vous remplacez un pare-feu ou un portail, vous pouvez restaurer les informations relatives au remplacement en important le module d'état.

  Informations sur l'état de l'importation :

  1. Sélectionnez **Device (Périphérique)** > **Setup (Paramétrage)** > **Operations (Opérations)**, cliquez sur **Import device state (Importez l'état du périphérique)**, **Browse (Accédez)** au module d'état, puis cliquez sur **OK**.

2. (Facultatif) Cliquez sur **Commit (Validez)** pour appliquer les informations relatives à l'état importé à la configuration active.

# Gestion des administrateurs de pare-feu

Les comptes administrateurs spécifient les rôles et les méthodes d'authentification des administrateurs des pare-feu Palo Alto Networks. Chaque pare-feu Palo Alto Networks dispose d'un compte administrateur par défaut prédéfini (admin), qui offre un accès complet en lecture/écriture (également appelé accès super utilisateur) au pare-feu.

***Il est recommandé de créer un compte administrateur distinct pour chaque personne qui a besoin d'accéder aux fonctions d'administration ou de génération de rapports du pare-feu. Cela vous permet de mieux protéger le pare-feu contre la configuration non autorisée et d'activer la journalisation des actions de chaque administrateur. Veillez à suivre les Meilleures pratiques pour sécuriser l'accès administratif afin de vous assurer que vous sécurisez l'accès administratif à vos pare-feu et aux autres appareils de sécurité d'une manière qui empêche les attaques réussies.***

- Types de rôles administrateur
- Configuration d'un profil de rôle administrateur
- Authentification administrateur
- Configurer l'authentification et les comptes administrateurs
- Configurer le suivi de l'activité de l'administrateur

## Types de rôles administrateur

Un ***rôle*** définit le type d'accès au pare-feu dont dispose l'administrateur. Les types d'administrateurs sont les suivants :

- **Basé sur le rôle** : rôles personnalisés que vous pouvez configurer pour un contrôle d'accès plus granulaire aux zones fonctionnelles de l'interface Web, de la CLI et de l'API XML. Par exemple, vous pouvez créer un profil de rôle administrateur pour votre personnel d'exécution qui fournit un accès au pare-feu et aux zones de configuration réseau de l'interface Web, ainsi qu'un profil distinct pour vos administrateurs de sécurité qui offre un accès aux définitions des politiques de sécurité, journaux et rapports. Sur un pare-feu prenant en charge la fonction de systèmes virtuels multiples, vous pouvez décider si le rôle définit l'accès à tous les systèmes virtuels ou à des systèmes virtuels donnés. Lorsque de nouvelles fonctionnalités sont ajoutées au projet, vous devez mettre les rôles à jour en ajoutant les privilèges d'accès correspondants : le pare-feu n'ajoute pas automatiquement les nouvelles fonctionnalités aux définitions de rôles personnalisés. Pour plus d'informations sur les privilèges que vous pouvez configurer pour les rôles administrateur personnalisés, reportez-vous à la section Référence : accès administrateur à l'interface Web.
- **Dynamique** : rôles intégrés qui permettent d'accéder au pare-feu. Lors de l'ajout de nouvelles fonctionnalités, le pare-feu met automatiquement à jour les définitions des rôles dynamiques. Vous ne les mettez jamais à jour manuellement. Le tableau suivant répertorie les privilèges d'accès associés aux rôles dynamiques.

| Rôle dynamique | Privilèges |
|---|---|
| Super utilisateur | Accès complet au pare-feu, notamment la définition de nouveaux comptes administrateur ainsi que de systèmes virtuels. Vous devez posséder des privilèges de super utilisateur pour créer un utilisateur administratif avec privilèges de super utilisateur. |
| Super utilisateur (lecture seule) | Accès en lecture seule au pare-feu. |
| Administrateur du périphérique | Accès complet à tous les paramètres du pare-feu, sauf pour la définition de nouveaux comptes ou systèmes virtuels. |
| Administrateur du périphérique (lecture seule) | Accès en lecture seule à l'ensemble des paramètres du pare-feu, sauf aux profils de mot de passe (aucun accès) et aux comptes administrateur (seul le compte connecté est visible). |
| Administrateur du système virtuel | Accès aux systèmes virtuels spécifiques du pare-feu pour créer et gérer des aspects particuliers des systèmes virtuels. Un administrateur du système virtuel n'a pas accès aux interfaces de réseau, aux VLAN, aux câbles virtuels, aux routeurs virtuels, aux tunnels IPSec, aux tunnels GRE, à DHCP, au proxy Dns, à QoS, à LLDP ou aux profils réseaux. |
| Rôle administrateur du système virtuel (lecture seule) | Accès en lecture seule aux systèmes virtuels spécifiques du pare-feu et aux aspects particuliers des systèmes virtuels. Un administrateur du système virtuel ayant un accès en lecture seule n'a pas accès aux interfaces de réseau, aux VLAN, aux câbles virtuels, aux routeurs virtuels, aux tunnels IPSec, aux tunnels GRE, à DHCP, au proxy Dns, à QoS, à LLDP ou aux profils réseaux. |

## Configuration d'un profil de rôle administrateur

Les profils de rôle administrateur vous permettent de définir des privilèges d'accès administrateur granulaires pour garantir la protection des informations d'entreprise sensibles et la vie privée des utilisateurs finaux.

*Suivez le principe de l'accès au moindre privilège et créez des profils de Rôle d'administrateur qui permettent aux administrateurs d'accéder uniquement aux zones de l'interface de gestion auxquelles ils ont besoin d'accéder pour effectuer leurs tâches.*

**STEP 1 |** Sélectionnez **Device (Périphérique)** > **Admin Roles (Rôles administrateur)**, puis cliquez sur **Add (Ajouter)**.

**STEP 2 |** Saisissez un **Name (Nom)** pour identifier le rôle.

**STEP 3 |** Pour l'étendue du **Role (Rôle)**, sélectionnez **Device (Périphérique)** ou **Virtual System (Système virtuel)**.

**STEP 4 |** Dans l'onglet **Web UI (Interface Web)** et/ou **REST API**, cliquez sur l'icône de chaque zone fonctionnelle pour sélectionner le paramètre souhaité : Activer, Lecture seule ou Désactiver. Pour l'onglet **XML API**, sélectionnez Activer ou Désactiver. Pour plus d'informations sur les options **Web UI (Interface Web)**, reportez-vous à la section Privilèges d'accès à l'interface Web.

**STEP 5 |** Dans l'onglet **Command Line (Ligne de commande)**, sélectionnez une option d'accès à la CLI. L'étendue du **Role (Rôle)** contrôle les options disponibles :

- Rôle du **Device (périphérique)** :
  - **None (Aucun)** : l'accès à la CLI n'est pas autorisé (par défaut).
  - **superuser (superutilisateur)** : accès complet. Peut définir de nouveaux comptes administrateur et systèmes virtuels. Seul un superutilisateur peut créer des utilisateurs administrateurs avec des privilèges de superutilisateur.
  - **superreader (super-lecteur)** : Accès complet en lecture seule.
  - **deviceadmin (administrateur de périphérique)** : accès complet à tous les paramètres, à l'exception de la définition de nouveaux comptes ou systèmes virtuels.
  - **devicereader (lecteur de périphérique)** :Accès en lecture seule à l'ensemble des paramètres du pare-feu, sauf aux profils de mot de passe (aucun accès) et aux comptes administrateur (seul le compte connecté est visible).
- Rôle de **Virtual System (Système virtuel)** :
  - **None (Aucun)** : l'accès n'est pas autorisé (par défaut).
  - **vsysadmin** : a accès aux systèmes virtuels spécifiques du pare-feu pour créer et gérer des aspects particuliers des systèmes virtuels. Ne permet pas l'accès aux fonctions au niveau du pare-feu ou au niveau du réseau, y compris le routage statique et dynamique, les adresses IP d'interface, les tunnels IPSec, les VLAN, les câbles virtuels, les routeurs virtuels, les tunnels GRE, DCHP, DNS Proxy, QoS, LLDP ou les profils réseau.
  - **vsysreader** : accès en lecture seule à des systèmes virtuels spécifiques à des aspects spécifiques des systèmes virtuels. Ne permet pas l'accès aux fonctions au niveau du pare-feu ou au niveau du réseau, y compris le routage statique et dynamique, les adresses IP d'interface, les tunnels IPSec, les VLAN, les câbles virtuels, les routeurs virtuels, les tunnels GRE, DCHP, DNS Proxy, QoS, LLDP ou les profils réseau.

**STEP 6 |** Cliquez sur **OK** pour enregistrer le profil.

**STEP 7 |** Affectez le rôle à un administrateur. Reportez-vous à la section Configuration du compte administrateur du pare-feu.

## Exemple de construction de Profil de rôle d'administrateur

Cet exemple montre un profil de Rôle d'administrateur pour un responsable du centre d'opérations de sécurité (SOC) qui a besoin d'un accès pour enquêter sur les problèmes potentiels. Le Gestionnaire SOC a besoin d'un accès en lecture à de nombreuses zones du pare-feu, mais n'a généralement pas besoin d'un accès en écriture. L'exemple couvre les quatre onglets du profil de rôle d'administrateur et chaque étape décrit pourquoi le profil active ou désactive une zone d'accès particulière au gestionnaire SOC.

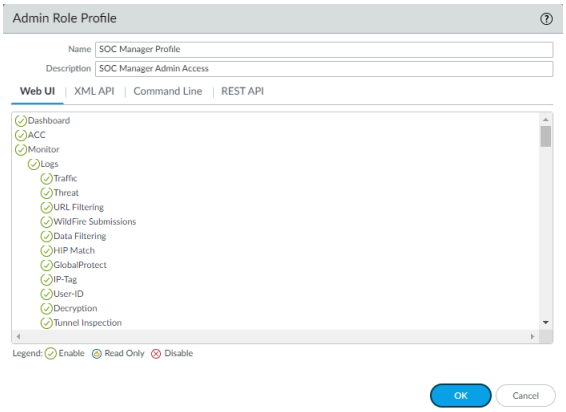
 

*Ceci est un exemple de profil pour un gestionnaire SOC fictif. Configurez les profils de Rôle d'administrateur pour vos administrateurs en fonction des fonctions qu'ils gèrent et de l'accès requis pour faire leur travail. N'activez pas les accès inutiles. Créez des profils distincts pour chaque groupe administratif qui partage les mêmes tâches et pour les administrateurs qui ont des tâches uniques. Chaque administrateur doit avoir le niveau d'accès exact requis pour accomplir ses tâches et aucun accès au-delà.*

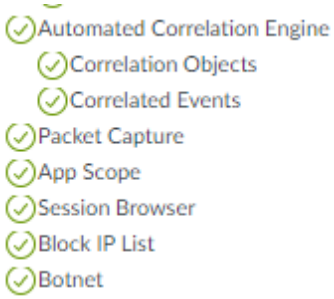
**STEP 1 |** Configurez les autorisations d'accès à l'interface utilisateur Web. Chaque extrait de l'écran de l'interface utilisateur Web affiche une zone différente d'autorisations de l'interface utilisateur Web. Les autorisations sont répertoriées par onglet de pare-feu, dans l'ordre dans lequel vous voyez les onglets dans l'interface utilisateur Web, suivis des autorisations pour d'autres actions.

Les zones **Dashboard (tableau de bord)**, **ACC** et **Monitor (surveillance)** > **Logs (journaux)** du pare-feu ne contiennent pas d'éléments de configuration. Tous les objets sont informatifs (vous pouvez uniquement les basculer entre activer et désactiver car ils sont déjà en lecture seule). Étant donné que le gestionnaire SOC doit enquêter sur les problèmes potentiels, le gestionnaire SOC doit accéder aux informations de ces onglets.

Le nom et la description du profil permettent de comprendre facilement l'objectif du profil. Cette capture n'affiche pas toutes les autorisations de **Logs (journaux)**, mais elles sont toutes activées pour ce profil.



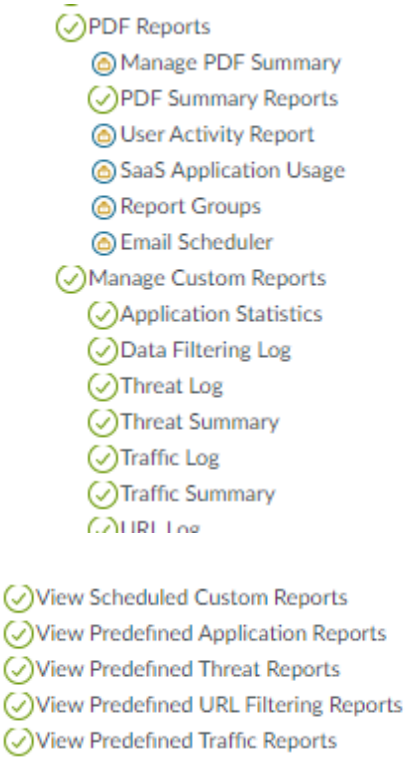

La capture suivante affiche les autorisations pour des objets plus informatifs dans l'onglet **Monitor (Surveiller)**. Le gestionnaire SOC utilise ces outils pour enquêter sur les problèmes potentiels et nécessite donc un accès.




Les deux captures suivantes affichent les autorisations pour les rapports PDF, les rapports personnalisés et les rapports prédéfinis dans l'onglet **Monitor (Surveiller)**. Alors que le SOC Manager a besoin d'accéder aux rapports PDF pour collecter des informations, dans cet exemple, le SOC Manager n'a pas besoin de configurer les rapports, donc l'accès est défini en lecture seule

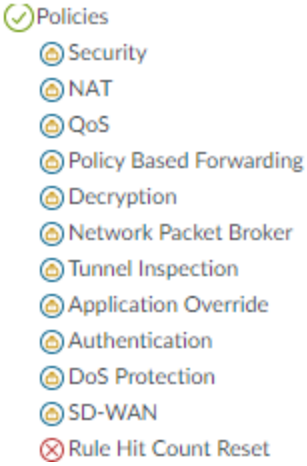
(les rapports récapitulatifs ne sont pas configurables). Cependant, le gestionnaire SOC doit gérer les rapports personnalisés pour enquêter sur des problèmes potentiels spécifiques, de sorte que des autorisations d'accès complètes sont accordées pour tous les rapports personnalisés (y compris ceux qui ne sont pas affichés dans le snip). Enfin, le gestionnaire SOC a besoin d'accéder à des rapports prédéfinis pour enquêter sur les problèmes potentiels.




Étant donné que le gestionnaire SOC est un enquêteur et non un administrateur qui configure le pare-feu, les autorisations pour l'onglet **Policies (Politiques)** sont en lecture seule, à l'exception de la réinitialisation du nombre d'accès à la règle. La réinitialisation du nombre d'accès à la règle ne fait pas partie des tâches du gestionnaire SOC (et la modification du nombre d'accès pourrait affecter négativement ou dérouter les autres administrateurs), donc l'accès est désactivé. L'accès

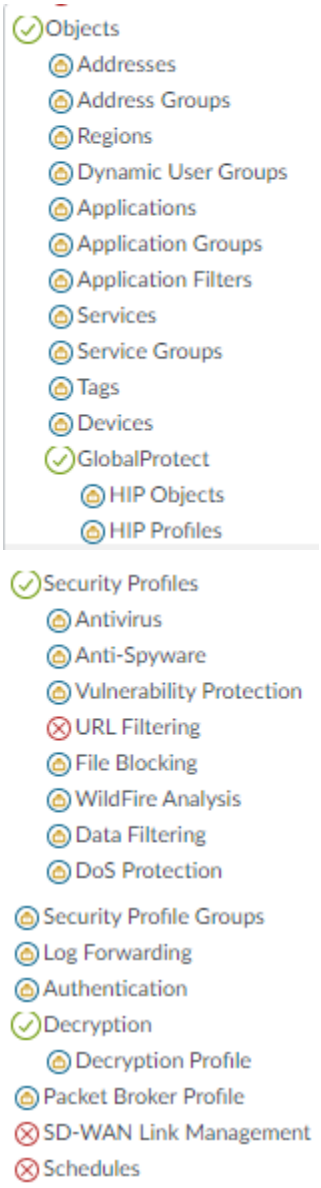
en lecture permet au gestionnaire SOC d'enquêter sur la construction d'une stratégie qui, selon lui, peut avoir causé un problème.




Les autorisations pour l'onglet **Objects (Objets)** sont également en lecture seule pour la même raison : le travail du gestionnaire SOC ne nécessite pas de configuration, aucune autorisation de configuration n'est donc attribuée. Pour les zones qui ne sont pas incluses dans les tâches du gestionnaire SOC, l'accès est désactivé. Dans cet exemple, le gestionnaire SOC dispose d'un accès en lecture seule pour enquêter sur les configurations d'objets pour tous les objets, à l'exception du **URL Filtering (filtrage d'URL)**, de la **SD-WAN Link Management (Gestion**

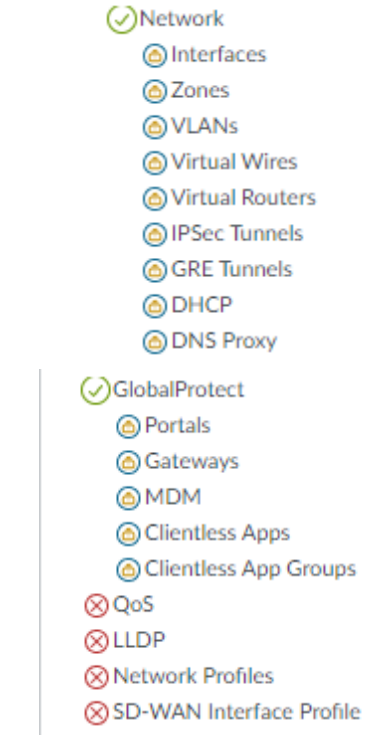
**des liens SD-WAN)** et des **Schedules (planifications)**, qui sont sous le contrôle de différents administrateurs dans cet exemple.



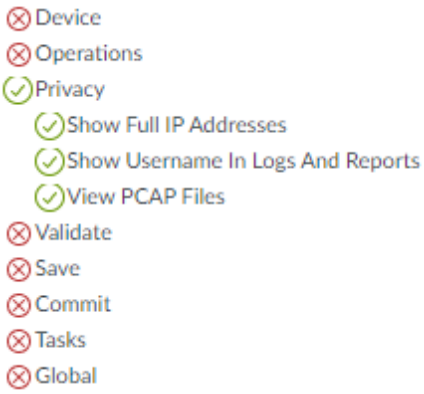

Pour les autorisations de l'onglet **Network (Réseau)**, le scénario est similaire : le gestionnaire SOC n'a besoin de configurer aucun des objets, mais peut avoir besoin d'informations pour enquêter sur les problèmes, de sorte qu'un accès en lecture seule est attribué aux zones que le gestionnaire SOC peut avoir besoin d'enquêter. Dans cet exemple, l'accès est désactivé pour les

profils QoS, LLDP, Network Profiles ou SD-WAN Interface car ces éléments ne font pas partie des tâches du gestionnaire SOC.



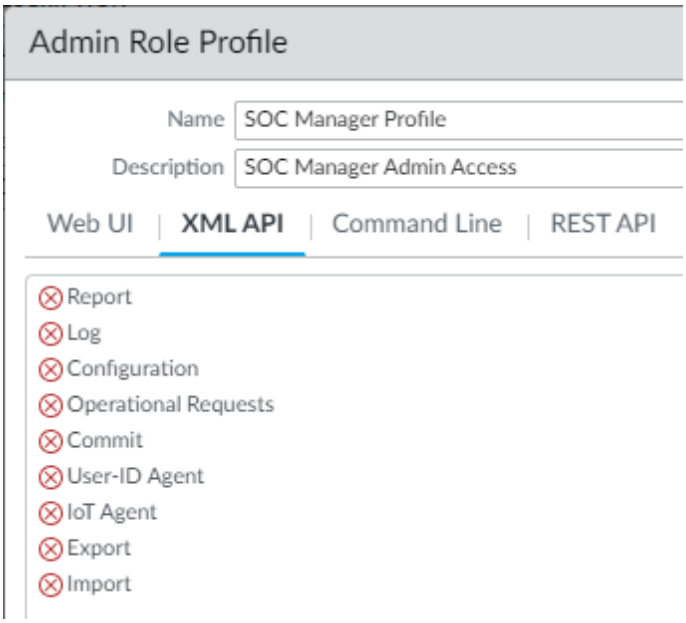

Dans cet exemple, le gestionnaire SOC n'a pas besoin d'accéder aux fonctionnalités de l'onglet **Device (Périphérique)** à des fins d'enquête, de sorte que toutes les autorisations de l'onglet **Device (Périphérique)** sont bloquées. De plus, l'enquête ne nécessite aucune action de validation ni accès à aucune des actions restantes, de sorte que ces autorisations sont également bloquées.



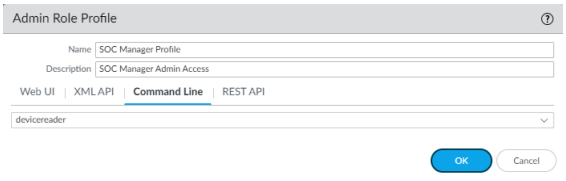
**STEP 2 |** Configurez les autorisations d'accès à l'API XML.

L'extrait suivant montre que toutes les autorisations de l'API XML sont désactivées pour le gestionnaire SOC, car le gestionnaire SOC n'accède pas au pare-feu à l'aide des commandes de l'API XML.




**STEP 3 |** Configurez les autorisations d'accès à la ligne de commande (CLI).

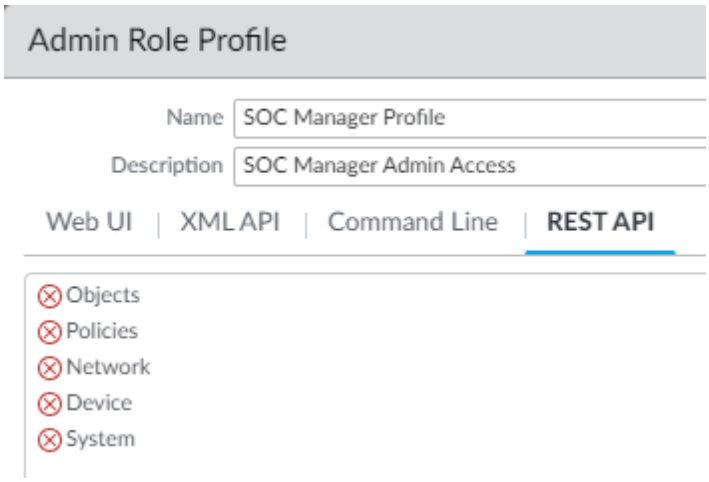
Les autorisations d'accès CLI sont en lecture seule pour le gestionnaire SOC, car le gestionnaire SOC a besoin d'accéder aux journaux et à d'autres outils de surveillance et doit également pouvoir voir certaines configurations afin d'enquêter sur les problèmes potentiels. Cependant, le gestionnaire SOC ne configure pas le pare-feu, donc aucune autorisation de configuration n'est attribuée. Le niveau d'accès est défini sur **devicereader** au lieu de **superreader** car le gestionnaire SOC n'a pas besoin d'accéder aux profils de mot de passe ou à d'autres comptes administratifs.



**STEP 4 |** Configurez les autorisations d'accès à l'API REST.

Le gestionnaire SOC n'accède pas au pare-feu à l'aide des commandes API REST, donc tous les accès API REST sont désactivés.




## Authentification administrateur

Vous pouvez configurer les types d'authentification et d'autorisation suivants (affectation des rôles et des domaines d'accès) pour les administrateurs du pare-feu :

| Méthode d'authentifica | Méthode d'autorisation | Description |
|---|---|---|
| Local | Local | Les informations d'identification du compte administrateur et les méthodes d'authentification se trouvent localement sur le pare-feu. Vous pouvez définir les comptes avec ou sans base de données d'utilisateurs qui se trouve localement sur le pare-feu. Reportez-vous à la section Authentification locale pour connaître les avantages et les désavantages liés à l'utilisation d'une base de données locale. Vous utilisez le pare-feu pour gérer l'affectation des rôles, mais les domaines d'accès ne sont pas pris en charge. Pour obtenir de plus amples précisions, consultez la section Configuration de l'authentification locale ou externe des administrateurs du pare-feu. |
| Clé SSH | Local | Les comptes administrateur se trouvent localement sur le pare-feu, mais l'authentification à la CLI est basée sur des certificats SSH. Vous utilisez le pare-feu pour gérer l'affectation des rôles, mais les domaines d'accès ne sont pas pris en charge. Pour obtenir de plus amples précisions, reportez-vous à la section Configuration de l'authentification administrateur basée sur les clés SSH pour la CLI. |
| Certificats | Local | Les comptes administrateur se trouvent localement sur le pare-feu, mais l'authentification à l'interface Web est basée sur des certificats clients. Vous utilisez le pare-feu pour gérer l'affectation |

| Méthode d'authentifica | Méthode d'autorisation | Description |
|---|---|---|
| | | des rôles, mais les domaines d'accès ne sont pas pris en charge. Pour obtenir de plus amples précisions, consultez la section Configuration de l'authentification administrateur basée sur les certificats pour l'interface Web. |
| Service externe | Local | Les comptes administrateur que vous définissez localement sur le pare-feu servent de références aux comptes définis sur un serveur d'authentification à plusieurs facteurs, SAML, Kerberos, TACACS+, RADIUS ou LDAP externe. Le serveur externe effectue l'authentification. Vous utilisez le pare-feu pour gérer l'affectation des rôles, mais les domaines d'accès ne sont pas pris en charge. Pour obtenir de plus amples précisions, consultez la section Configuration de l'authentification locale ou externe des administrateurs du pare-feu. |
| Service externe | Service externe | Les comptes administrateur définis sur un serveur SAML, TACACS + ou RADIUS externe. Le serveur effectue l'authentification et l'autorisation. Pour l'autorisation, vous définissez les Vendor-Specific Attributes (Attributs spécifiques au fournisseur ; VSA) sur le serveur TACACS+ ou RADIUS, ou les attributs SAML sur le serveur SAML. PAN-OS mappe les attributs aux rôles d'administrateur, aux domaines d'accès, aux groupes d'utilisateurs et aux systèmes virtuels que vous définissez sur le pare-feu. Pour plus de détails, reportez-vous aux sections :<br>• Configuration de l'authentification SAML<br>• Configuration de l'authentification TACACS+<br>• Configuration de l'authentification RADIUS |

## Configurer l'authentification et les comptes administrateurs

Si vous avez déjà configuré un profil d'authentification (voir la section Configuration d'un profil et d'une séquence d'authentification) ou que vous n'avez pas besoin d'un tel profil pour authentifier les administrateurs, vous êtes prêt à passer à la configuration du compte administrateur du pare-feu. Sinon, effectuez l'une des autres procédures énumérées ci-dessous pour configurer les comptes administrateurs pour des types spécifiques d'authentification.

- Configuration du compte administrateur du pare-feu
- Configuration de l'authentification locale ou externe des administrateurs du pare-feu
- Configuration de l'authentification administrateur basée sur les certificats pour l'interface Web
- Configuration de l'authentification administrateur basée sur les clés SSH pour la CLI
- Configuration du délai de vie de la clé API

## Configuration du compte administrateur du pare-feu

Les comptes administrateur précisent les rôles et les méthodes d'authentification des administrateurs du pare-feu. C'est le service que vous utilisez pour affecter des rôles et effectuer l'authentification qui vous permet de déterminer si vous devez ajouter les comptes sur le pare-feu, sur un serveur externe, ou sur les deux (reportez-vous à la section Authentification administrateur). Si la méthode d'authentification dépend d'une base de données qui se trouve localement sur le pare-feu ou d'un service externe, vous devez configurer un profil d'authentification avant d'ajouter un compte administrateur (reportez-vous à la section Configuration de l'authentification et des comptes administrateur). Si vous avez déjà configuré le profil d'authentification ou si vous utiliserez l'authentification locale sans avoir recours à une base de données qui se trouve localement sur le pare-feu, effectuez les étapes suivantes pour ajouter un compte administrateur sur le pare-feu.

*Créez un compte administrateur distinct pour chaque personne qui a besoin d'accéder aux fonctions d'administration ou de génération de rapports du pare-feu. Cela vous permet de mieux protéger le pare-feu contre la configuration non autorisée et d'activer la journalisation des actions de chaque administrateur.*

*Veillez à suivre les Meilleures pratiques pour sécuriser l'accès administratif afin de vous assurer que vous sécurisez l'accès administratif à vos pare-feu et aux autres appareils de sécurité d'une manière qui empêche les attaques réussies.*

**STEP 1 |** Modifiez le nombre de comptes d'administrateur pris en charge.

Configurez le nombre total de sessions de comptes d'administration simultanées prises en charge pour un pare-feu en mode de fonctionnement normal ou en mode FIPS-CC. Vous pouvez autoriser jusqu'à quatre sessions de compte d'administration simultanées ou configurer le pare-feu pour prendre en charge un nombre illimité de sessions de compte d'administration simultanées.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Authentication Settings (Paramètres d'authentification).
2. Modifiez le **Max Session Count (nombre maximal de sessions)** pour spécifier le nombre de sessions simultanées prises en charge (la plage est de **0** à **4**) autorisée pour tous les comptes d'administrateur et d'utilisateur.

   Entrez **0** pour configurer le pare-feu afin qu'il prend en charge un nombre illimité de comptes d'administration.
3. Modifiez la **Max Session Time (durée maximale de session)** en minutes pour un compte administratif. La valeur par défaut est `720` minutes.
4. Cliquez sur **OK**.

5. **Commit** (Valider).

*Vous pouvez également configurer le nombre total de sessions simultanées prises en charge en vous* logging in to the firewall CLI (connectant à l'interface de ligne de commande du pare-feu)**.**

```
admin> configure
```

```
admin# set deviceconfig setting management admin-session
 max-session-count <0-4>
```

```
admin# set deviceconfig setting management admin-session
 max-session-time <0, 60-1499>
```

```
admin# commit
```

**STEP 2 |** Sélectionnez **Device (Périphérique)** > **Administrators (Administrateurs)** et **Add (Ajoutez)** un compte.

**STEP 3 |** Saisissez un **Name (Nom)** d'utilisateur.

Si le pare-feu se sert d'une base de données d'utilisateurs locale pour authentifier le compte, saisissez le nom que vous avez donné au compte dans la base de données (reportez-vous à la section Ajoutez le groupe d'utilisateurs à la base de données locale).

**STEP 4 |** Sélectionnez une séquence ou un **Authentication Profile (Profil d'authentification)** si vous avez configuré l'un ou l'autre pour l'administrateur.

Si le pare-feu se sert de l'authentification locale sans avoir recours à une base de données d'utilisateurs locale pour authentifier le compte, sélectionnez **None (Aucun)** (par défaut) et entrez un **Password (Mot de passe)**.

**STEP 5 |** Sélectionnez le **Administrator Type (Type d'administrateur)**.

Si vous avez configuré un rôle personnalisé pour l'utilisateur, sélectionnez **Role Based (Basé sur les rôles)**, puis choisissez le **Profile (Profil)** de rôle administrateur. Sinon, sélectionnez **Dynamic (Dynamique)** (par défaut) et choisissez un rôle dynamique. Si le rôle dynamique est **virtual system administrator (administrateur du système virtuel)**, ajoutez un ou plusieurs systèmes virtuels que l'administrateur du système virtuel est autorisé à gérer.

**STEP 6 |** (Facultatif) Sélectionnez un **Password Profile (Profil de mot de passe)** pour les administrateurs que le pare-feu authentifie localement sans dépendre d'une base de données d'utilisateurs locale. Pour plus de détails, voir la section Définissez un profil de mot de passe.

**STEP 7 |** Cliquez sur **OK**, puis sur **Commit (Valider)**.

## Configuration de l'authentification locale ou externe des administrateurs du pare-feu

Vous pouvez utiliser l'authentification locale ou les services d'authentification externe pour authentifier les administrateurs qui accèdent au pare-feu. Ces méthodes d'authentification invitent les administrateurs à répondre à une ou plusieurs demandes d'authentification, par exemple, une page d'ouverture de session où ils doivent saisir un nom d'utilisateur et un mot de passe.

***Si vous utilisez un service externe pour gérer l'authentification et l'autorisation (affectations des rôles et des domaines d'accès), reportez-vous aux sections suivantes :***

- Configuration de l'authentification SAML
- Configuration de l'authentification TACACS+
- Configuration de l'authentification RADIUS

***Pour authentifier les administrateurs sans un mécanisme de demande/réponse, vous pouvez procédez à la*** configuration de l'authentification administrateur basée sur les certificats pour l'interface Web ***et à la*** configuration de l'authentification administrateur basée sur les clés SSH pour la CLI**.**

**STEP 1 |** (Authentification externe uniquement) Autorisez le pare-feu à se connecter à un serveur externe pour authentifier les administrateurs.

Configurez un profil de serveur :

- Ajoutez un profil de serveur RADIUS.

  Si le pare-feu s'intègre à un service Multi-Factor Authentication (authentification à plusieurs facteurs ; MFA) via RADIUS, vous devez ajouter un profil de serveur RADIUS. Dans ce cas, le service MFA fournit tous les facteurs d'authentification (demandes). Si le pare-feu s'intègre à un service MFA via l'API d'un fournisseur, vous pouvez tout de même utiliser un profil de serveur RADIUS pour le premier facteur, mais des profils de serveur MFA sont requis pour les facteurs supplémentaires.
- Ajoutez un profil de serveur MFA.
- Ajoutez un profil de serveur TACACS+.
- Ajoutez un profil de serveur d'IDP en SAML. Vous ne pouvez combiner la single sign-on (Ouverture de session unique ; SSO) Kerberos à la SSO SAML ; vous ne pouvez utiliser qu'un seul type de service SSO.
- Ajoutez un profil de serveur Kerberos.
- Ajoutez un profil de serveur LDAP.

**STEP 2 |** (Authentification à l'aide d'une base de données locale uniquement) Configurez une base de données d'utilisateurs qui se trouve localement sur le pare-feu.

1. Ajoutez le compte utilisateur à la base de données locale.
2. (Facultatif) Ajoutez le groupe d'utilisateurs à la base de données locale.

**STEP 3 |** (Authentification locale uniquement) Définissez les paramètres de complexité des mots de passe et d'expiration.

Ces paramètres protègent le pare-feu d'un accès non autorisé, car ils font en sorte qu'il soit plus difficile pour les pirates de deviner les mots de passe.

1. Définissez les paramètres de complexité des mots de passe et d'expiration globaux qui s'appliquent à tous les administrateurs locaux. Les paramètres ne s'appliquent pas aux comptes de la base de données locale pour lesquels vous avez indiqué un hachage du mot de passe plutôt qu'un mot de passe (consultez la section Authentification locale).
   1. Sélectionnez **Device (Périphérique)** > **Setup (Paramétrage)** > **Management (Gestion)** et modifiez les paramètres de complexité minimale de mot de passe.
   2. Sélectionnez **Enabled (Activé)**.
   3. Définissez les paramètres de mot de passe et cliquez sur **OK**.
2. Définissez un profil de mot de passe.

   Vous affectez le profil aux comptes administrateur pour lesquels vous souhaitez remplacer les paramètres d'expiration des mots de passe globaux. Les profils sont disponibles uniquement aux comptes qui ne sont pas associés à une base de données locale (reportez-vous à la section Authentification locale).
   1. Sélectionnez **Device (Périphérique)** > **Password Profiles (Profils de mots de passe)** et **Add (ajoutez)** un profil.
   2. Saisissez un **Name (Nom)** pour identifier le profil.
   3. Définissez les paramètres d'expiration des mots de passe et cliquez sur **OK**.

**STEP 4 |** (SSO Kerberos uniquement) Créez un keytab Kerberos.

Un keytab est un fichier qui contient des informations concernant le compte Kerberos du pare-feu. Pour prendre en charge la SSO Kerberos, votre réseau doit être doté d'une infrastructure Kerberos.

**STEP 5 |** Configurez un profil d'authentification.

*Si vos comptes administrateurs sont stockés dans de multiples types de serveurs, vous pouvez créer un profil d'authentification pour chaque type et ajouter tous les profils à une séquence d'authentification.*

Configuration d'un profil et d'une séquence d'authentification. Dans le profil d'authentification, indiquez le **Type** de service d'authentification et les paramètres connexes :

- **Service externe** : sélectionnez le **Type** de service externe et sélectionnez le **Server Profile (Profil de serveur)** que vous avez créé pour celui-ci.
- **Authentification à l'aide d'une base de données locale** : définissez le **Type (Type)** sur **Local Database (Base de données locale)**.
- **Authentification locale sans base de données** : définissez le **Type (Type)** sur **None (Aucune)**.
- **Kerberos SSO (SSO Kerberos)** : spécifiez la **Kerberos Realm (Partition Kerberos)** et **Import (Importez)** le **Kerberos Keytab (Keytab Kerberos)**.

**STEP 6 |** Affectez le profil ou la séquence d'authentification à un compte administrateur.

1. Configuration du compte administrateur du pare-feu.
   - Affectez le **Authentication Profile (Profil d'authentification)** ou la séquence d'authentification que vous avez configuré.
   - (Authentification à l'aide de la base de données locale uniquement) Précisez le **Name (Nom)** du compte utilisateur que vous avez ajouté à la base de données locale.
2. **Commit (Validez)** vos modifications.
3. (Facultatif) Procédez à la Vérification de la connectivité du serveur d'authentification pour vérifier que le pare-feu peut se servir de profil d'authentification pour authentifier les administrateurs.

## Configuration de l'authentification administrateur basée sur les certificats pour l'interface Web

Comme alternative plus sûre à l'authentification par mot de passe à l'interface Web du pare-feu, vous pouvez configurer l'authentification basée sur les certificats pour les comptes locaux d'administrateur sur le pare-feu. L'authentification basée sur les certificats implique l'échange et la vérification d'une signature numérique à la place d'un mot de passe.

***La configuration de l'authentification basée sur les certificats pour un administrateur désactive les informations de connexion nom d'utilisateur/mot de passe de tous les administrateurs sur le pare-feu ; les administrateurs ont alors besoin du certificat pour se connecter.***

**STEP 1 |** Générez un certificat de Certificate Authority (autorité de certification - CA) sur le pare-feu.

Vous utiliserez ce certificat CA pour signer le certificat client de chaque administrateur.

Création d'un certificat CA racine auto-signé.

***Vous pouvez éventuellement procéder à l'**Importation d'un certificat et d'une clé privée** du certificat AC de votre entreprise ou du certificat CA d'un tiers.***

**STEP 2 |** Configurez un profil de certificat pour sécuriser l'accès à l'interface web.

Configuration d'un profil de certificat.

- Définissez le champ **Username (Nom d'utilisateur)** sur **Subject (Objet)**.
- Dans la section CA Certificates (Certificats CA), **Add (Ajoutez)** le **CA Certificate (Certificat CA)** que vous venez de créer ou d'importer.

**STEP 3 |** Configurez le pare-feu pour utiliser le profil de certificat pour l'authentification des administrateurs.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Authentication Settings (Paramètres d'authentification).
2. Sélectionnez le **Certificate Profile (Profil de certificat)** que vous avez créé pour authentifier les administrateurs et cliquez sur **OK (OK)**.

**STEP 4 |** Configurez les comptes administrateurs pour utiliser l'authentification du certificat client.

Pour chaque administrateur qui accédera à l'interface Web du pare-feu, effectuez la configuration du compte administrateur du pare-feu, puis sélectionnez **Use only client certificate authentication (Utiliser uniquement l'authentification du certificat client)**.

Si vous avez déjà déployé des certificats client générés par votre CA d'entreprise, passez à l'étape 8. Sinon, passez à l'étape 5.

**STEP 5 |** Générez un certificat client pour chaque administrateur.

Génération d'un certificat. Dans la liste déroulante **Signed By (Signé par)**, sélectionnez un certificat CA racine auto-signé.

**STEP 6 |** Exportez le certificat client.

1. Exportation d'un certificat et d'une clé privée.
2. **Commit (Validez)** vos modifications. Le pare-feu redémarre et met fin à votre session de connexion. Par la suite, les administrateurs peuvent accéder à l'interface web uniquement depuis des systèmes clients qui ont le certificat client que vous avez généré.

**STEP 7 |** Importez le certificat client dans le système client de chaque administrateur qui accédera à l'interface web.

Reportez-vous à la documentation de votre navigateur Web.

**STEP 8 |** Vérifiez que les administrateurs peuvent accéder à l'interface web.

1. Ouvrez l'adresse IP du pare-feu dans le navigateur de l'ordinateur qui dispose du certificat client.
2. Lorsque vous y êtes invité, sélectionnez le certificat que vous avez importé et cliquez sur **OK**. Le navigateur affiche un avertissement de certificat.
3. Ajoutez le certificat à la liste des exceptions du navigateur.
4. Cliquez sur **Login (Connexion)**. L'interface Web doit apparaître sans vous inviter à saisir de nom d'utilisateur ni de mot de passe.

## Configuration de l'authentification administrateur basée sur les clés SSH pour la CLI

Pour les utilisateurs qui utilisent Secure Shell (coquille sécurisée ; SSH) pour accéder à la CLI d'un pare-feu Palo Alto Networks, les clés SSH fournissent une méthode authentification plus sécurisée que les mots de passe. Les clés SSH éliminent pratiquement le risque d'attaques par force brute, permettent l'authentification à deux facteurs (clé et phrase secrète) et n'envoient pas de mots de passe sur le réseau. Les clés SSH permettent également des scripts automatisés pour accéder à l'ILC.

**STEP 1 |** Utilisez l'outil de génération de clé SSH pour créer une paire de clés asymétriques sur le système client de l'administrateur.

Les formats de clés pris en charge sont IETF SECSH et OpenSSH. Les algorithmes pris en charge sont DSA (1 024 bits) et RSA (768 à 4 096 bits).

Pour connaître les commandes permettant de générer une paire de clés, reportez-vous à la documentation de votre client SSH.

La clé publique et la clé privée sont des fichiers distincts. Enregistrez-les dans un emplacement auquel le pare-feu peut accéder. Pour plus de sécurité, entrez un mot de passe pour chiffrer la clé privée. Le pare-feu invite l'administrateur à saisir cette phrase secrète lors de la connexion.

**STEP 2 |** Configurez le compte administrateur pour utiliser l'authentification de clé publique.

1. Configuration du compte administrateur du pare-feu.
   - Configurez la méthode d'authentification de secours à utiliser en cas d'échec de l'authentification de clé SSH. Si vous avez configuré un **Authentication Profile (Profil d'authentification)** pour l'administrateur, sélectionnez-le dans la liste déroulante. Si vous sélectionnez **None (Aucun)**, vous devez saisir un **Password (Mot de passe)** et **Confirm Password (Confirmez le mot de passe)**.
   - Sélectionnez **Use Public Key Authentication (SSH) (Utiliser l'authentification par clé publique (SSH))**, cliquez sur **Import Key (Importer la clé)**, **Browse (Naviguez)** vers la clé publique que vous venez de générer, et cliquez sur **OK (OK)**.
2. **Commit (Validez)** vos modifications.

**STEP 3 |** Configurez le client SSH pour utiliser la clé privée pour l'authentification sur le pare-feu.

Effectuez cette tâche sur le système client de l'administrateur. Pour connaître les étapes, reportez-vous à la documentation de votre client SSH.

**STEP 4 |** Vérifiez que l'administrateur peut accéder à la CLI du pare-feu à l'aide de l'authentification de clé SSH.

1. Utilisez le navigateur du système client de l'administrateur pour accéder à l'adresse IP du pare-feu.
2. Connectez-vous à la CLI du pare-feu en tant qu'administrateur. Après avoir saisi un nom d'utilisateur, vous verrez la sortie suivante (la valeur de clé est un exemple) :

   ```
   Authenticating with public key “dsa-key-20130415”
   ```
3. À l'invite, saisissez la phrase secrète que vous avez définie lors de la création des clés.

## Configuration du délai de vie de la clé API

Les clés API sur le pare-feu et Panorama vous permettent d'authentifier les appels API à l'API XML et à l'API REST. Comme ces clés donnent accès au pare-feu et à Panorama, qui sont des éléments essentiels de votre posture de sécurité, il est recommandé de spécifier un délai de vie de la clé API pour entraîner la rotation régulière des clés. Après avoir spécifié le délai de vie de la clé, lors de la regénération d'un clé API, chaque clé est unique.

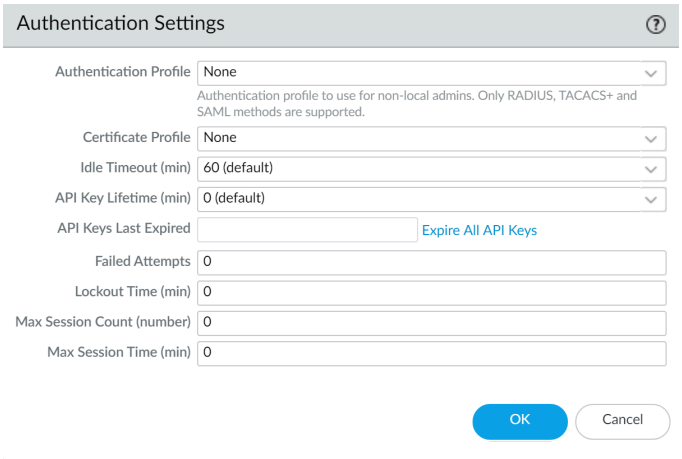
En plus de définir un délai de vie de la clé qui vous invite à regénérer périodiquement de nouvelles clés, vous pouvez également révoquer toutes les clés API actuellement valides dans l'éventualité où

une ou plusieurs clés sont compromises. La révocation des clés est un moyen de faire expirer toutes les clés qui sont actuellement valides.

**STEP 1 |** Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)**.

**STEP 2 |** Modifiez les paramètres d'authentification pour spécifier le **API Key Lifetime (min) [Délai de vie de la clé API (min)]**.



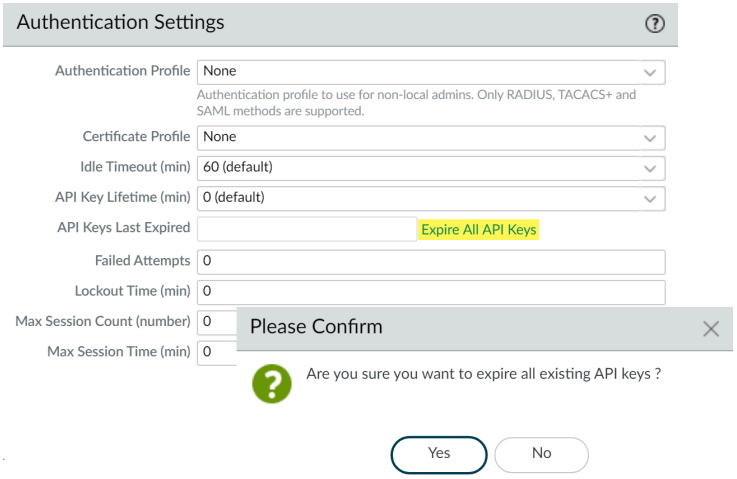

Définissez le délai de vie de la clé API pour qu'il offre une protection contre une compromission et pour réduire les effets d'une exposition accidentelle. Par défaut, le délai de vie de la clé API est défini sur 0, ce qui veut dire que les clés n'expirent jamais. Pour vous assurer que vos clés font souvent l'objet d'une rotation et que chaque clé est unique lorsque régénérée, vous devez spécifier une période de validité qui se situe entre 1 et 525 600 minutes. Reportez-vous aux politiques d'audit et de conformité de votre entreprise pour déterminer la manière dont vous devriez spécifier la durée de vie pendant laquelle vos clés API sont valides.

**STEP 3 |** **Commit (Validez)** les modifications.

**STEP 4 |** (Pour révoquer toutes les clés API) Sélectionnez **Expire all API Keys (Faire expirer toutes les clés API)** pour réinitialiser toutes les clés API qui sont actuellement valides.

Si vous avez uniquement défini un délai de vie de la clé et que vous souhaitez réinitialiser toutes les clés API pour qu'elles respectent la nouvelle durée, vous pouvez faire expirer toutes les clés existantes.




Lors de la confirmation, les clés sont révoqués et vous pouvez voir l'horodatage correspondant à la **API Keys Last Expired (Dernière expiration des clé API)**.

# Configurer le suivi de l'activité de l'administrateur

Suivez l'activité de l'administrateur sur l'interface Web du pare-feu et la CLI pour obtenir des rapports d'activité en temps réel sur votre pare-feu. Si vous avez des raisons de croire qu'un compte administrateur est compromis, vous disposez d'un historique complet de l'endroit où ce compte administrateur a navigué dans l'interface Web ou des commandes opérationnelles qu'il a exécutées afin que vous puissiez analyser en détail et répondre à toutes les actions entreprises par l'administrateur compromis.

Lorsqu'un événement se produit, un journal d'audit est généré et transmis au serveur syslog spécifié chaque fois qu'un administrateur navigue dans l'interface Web ou lorsqu'une operational command(commande opérationnelle) est exécutée dans l'interface de ligne de commande. Un journal d'audit est généré pour chaque navigation ou commande exécutée. Prenez par exemple si vous souhaitez créer un nouvel objet d'adresse. Un journal d'audit est généré lorsque vous cliquez sur **Objects (Objets)**, et un deuxième journal d'audit est généré lorsque vous cliquez ensuite sur Adresses.

Les journaux d'audit ne sont visibles que sous forme de syslogs transmis à votre serveur syslog et ne peuvent pas être affichés dans l'interface Web du pare-feu. Les journaux d'audit ne peuvent être transférés qu'à un serveur syslog, ne peuvent pas être transférés à Cortex Data Lake (CDL) et ne sont pas stockés localement sur le pare-feu.

**STEP 1 |** Configurez un profil de serveur syslog pour transférer les journaux d'audit de l'activité de l'administrateur sur le pare-feu.

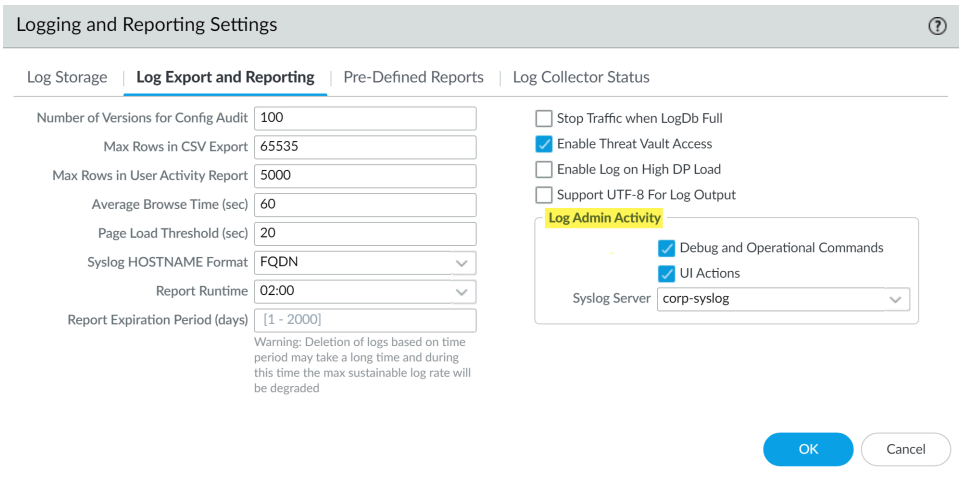
Cette étape est requise pour stocker avec succès les journaux d'audit pour le suivi de l'activité de l'administrateur sur le pare-feu.

1. Log in to the firewall web interface (Connectez-vous à l'interface Web du pare-feu).
2. Configure a syslog server profile (Configurez un profil de serveur Syslog).

**STEP 2 |** Configurer le suivi de l'activité de l'administrateur.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Logging and Reporting Settings (paramètres de journalisation et de génération de rapports).
2. Onglet **Log Export and Reporting (Exportation des journaux et génération de rapports)**.
3. Dans la section Activité de l'administrateur de journaux, configurez l'activité d'administrateur à suivre.
   - **Operational Commands (Commandes opérationnelles)** : générez un journal d'audit lorsqu'un administrateur exécute une commande opérationnelle ou de débogage dans la CLI ou une commande opérationnelle déclenchée à partir de l'interface Web. Consultez la CLI Operational Command Hierarchy (hiérarchie des commandes opérationnelles) de l'interface de ligne de commande pour obtenir la liste complète des commandes opérationnelles et de débogage de PAN-OS.
   - **UI Actions (Actions de l'interface utilisateur)** : générez un journal d'audit lorsqu'un administrateur navigue dans l'interface Web. Cela inclut la navigation entre les onglets de configuration, ainsi que les objets individuels dans un onglet.

     Par exemple, un journal d'audit est généré lorsqu'un administrateur navigue de l'**ACC** vers l'onglet **Policies (Politiques)**. De plus, un journal d'audit est généré lorsqu'un administrateur navigue depuis **Objects (Objets)** > **Addresses (Adresses)** vers **Objects (Objets)** > **Tags (Etiquettes)**.
   - **Syslog Server (Serveur Syslog)** : sélectionnez un profil de serveur syslog cible pour transférer les journaux d'audit.
4. Cliquez sur **OK**.
5. Sélectionnez **Commit (Valider)**.



# Référence : accès administrateur à l'interface Web

Vous pouvez configurer des privilèges pour l'ensemble d'un pare-feu, ou pour un ou plusieurs systèmes virtuels (sur les plates-formes qui prennent en charge plusieurs systèmes virtuels). Dans la désignation du paramètre **Device (Périphérique)** ou **Virtual System (Système virtuel)**, vous pouvez configurer des privilèges pour les rôles administrateur personnalisés, qui sont plus granulaires que les privilèges fixes associés à un rôle administrateur dynamique.

La configuration des privilèges à un niveau granulaire permet de s'assurer que les administrateurs de niveau inférieur ne puissent pas accéder à certaines informations. Vous pouvez créer des rôles personnalisés pour les administrateurs de pare-feu (reportez-vous à la section Configurer un Compte Administrateur de Pare-Feu), pour les administrateurs de Panorama ou les administrateurs de modèles et de groupes de périphériques (reportez-vous au Guide de l'administrateur Panorama). Appliquez le rôle administrateur à un compte administrateur à base de rôle personnalisé là où vous pouvez affecter un ou plusieurs systèmes virtuels. Les rubriques suivantes décrivent les privilèges que vous pouvez configurer pour les rôles administrateur personnalisés :

- Privilèges d'accès à l'interface Web
- Privilèges d'accès à l'interface Web de Panorama

## Privilèges d'accès à l'interface Web

Si vous souhaitez empêcher un administrateur basé sur les rôles d'accéder à des onglets spécifiques sur l'interface Web, vous pouvez désactiver l'onglet et l'administrateur ne le verra jamais lorsqu'il se connectera via le compte administrateur basé sur les rôles associé. Par exemple, vous pouvez créer un profil de rôle administrateur pour votre personnel d'exécution qui fournit un accès aux onglets **Device (Périphérique)** et **Network (Réseau)** uniquement et un profil séparé pour vos administrateurs de sécurité qui offre un accès aux onglets **Object (Objet)**, **Policy (Politique)** et **Monitor (Surveillance)**.

Un rôle administrateur peut s'appliquer au niveau **Device (Équipement)** ou **Virtual System (Système virtuel)** comme défini par la case d'option **Device (Équipement)** ou **Virtual System (Système virtuel)**. Si vous sélectionnez **Virtual System (Système virtuel)**, l'administrateur auquel ce profil est affecté est limité au(x) système(s) virtuel(s) auquel(auxquels) il ou elle est affecté(e). De plus, seul l'onglet **Device (Périphérique)** > **Setup (Configuration)** > **Services (Services)** > **Virtual Systems (Systèmes virtuels)** est accessible à cet utilisateur, pas l'onglet **Global (Global)**.

Les rubriques suivantes décrivent comment définir les privilèges de rôle administrateur pour les différentes parties de l'interface Web :

- Définir l'accès aux onglets de l'interface Web
- Octroi d'un accès granulaire à l'onglet Surveillance
- Octroi d'un accès granulaire à l'onglet Politiques
- Octroi d'un accès granulaire à l'onglet Objets
- Octroi d'un accès granulaire à l'onglet Réseau
- Octroi d'un accès granulaire à l'onglet Équipement
- Définition des paramètres de la vie privée des utilisateurs dans le profil de rôle administrateur
- Restriction de l'accès administrateur aux fonctions de validation et de confirmation

- Octroi d'un accès granulaire aux paramètres généraux
- Octroi d'un accès granulaire à l'onglet Panorama
- Fournir un Accès granulaire aux paramètres des opérations

## Définir l'accès aux onglets de l'interface Web

Le tableau suivant explique les privilèges d'accès de haut niveau que vous pouvez affecter à un profil de rôle administrateur au niveau (**Device (Périphérique)** > **Admin Roles (Rôles administrateur)**). Vous pouvez activer, désactiver ou définir les droits d'accès en lecture seul aux onglets de premier niveau de l'interface Web.

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| Tableau de bord | Contrôle l'accès à l'onglet **Dashboard (Tableau de bord)**. Si vous désactivez ce privilège, l'administrateur ne verra pas l'onglet et ne pourra pas accéder aux widgets du Tableau de bord. | Oui | Non | Oui |
| ACC | Contrôle l'accès à l'Application Command Center (centre de commande des applications - ACC) Si vous désactivez ce privilège, l'onglet **ACC** ne sera pas affiché dans l'interface Web. N'oubliez pas que, si vous souhaitez protéger la vie privée de vos utilisateurs tout en fournissant toujours un accès à l'ACC, vous pouvez désactiver l'option **Privacy (Vie privée)** > **Show Full IP Addresses (Afficher les adresses IP en intégralité)** et/ou l'option **Show User Names In Logs And Reports (Afficher les noms des utilisateurs dans les journaux et les rapports)**. | Oui | Non | Oui |
| surveiller | Contrôle l'accès à l'onglet **Monitor (Surveillance)**. Si vous désactivez ce privilège, l'administrateur ne verra pas l'onglet **Monitor (Surveillance)** et ne pourra pas accéder aux journaux, captures de paquets, informations de session, rapports ou à Appscope. Pour un contrôle plus granulaire des informations de surveillance que l'administrateur peut afficher, laissez l'option Surveillance activée, puis activez ou désactivez des nœuds spécifiques dans l'onglet comme décrit dans la section | Oui | Non | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | Octroi d'un accès granulaire à l'onglet Surveillance. | | | |
| Politiques | Contrôle l'accès à l'onglet **Policies (Politiques)**. Si vous désactivez ce privilège, l'administrateur ne verra pas l'onglet **Policies (Politiques)** et n'aura accès à aucune information sur les politiques. Pour un contrôle plus granulaire des informations de politiques que l'administrateur peut afficher, par exemple pour activer l'accès à un type de politique spécifique ou pour activer l'accès en lecture seule aux informations de politiques, laissez l'option **Policies (Politiques)** activée, puis activez ou désactivez des nœuds spécifiques dans l'onglet comme décrit dans la section Octroi d'un accès granulaire à l'onglet Politiques. | Oui | Non | Oui |
| Objets | Contrôle l'accès à l'onglet **Objects (Objets)**. Si vous désactivez ce privilège, l'administrateur ne verra pas l'onglet **Objects (Objets)** et ne pourra pas accéder aux objets, profils de sécurité, profils de transfert de journal, profils de décryptage, ou calendriers. Pour un contrôle plus granulaire des objets que l'administrateur peut afficher, laissez l'option **Objects (Objets)** activée, puis activez ou désactivez des nœuds spécifiques dans l'onglet comme décrit dans la section Octroi d'un accès granulaire à l'onglet Objets. | Oui | Non | Oui |
| Réseau | Contrôle l'accès à l'onglet **Network (Réseau)**. Si vous désactivez ce privilège, l'administrateur ne verra pas l'onglet **Network (Réseau)** et ne pourra pas accéder aux informations de configuration des éléments tels que : interface, zone, VLAN, câble virtuel, routeur virtuel, tunnel IPsec, DHCP, serveur proxy DNS, GlobalProtect, ni aux informations de configuration QoS ou aux profils réseau. Pour un contrôle plus granulaire des objets que l'administrateur peut afficher, laissez l'option **Network (Réseau)** activée, | Oui | Non | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | puis activez ou désactivez des nœuds spécifiques dans l'onglet comme décrit dans la section Octroi d'un accès granulaire à l'onglet Réseau. | | | |
| Périphérique | Contrôle l'accès à l'onglet **Device (Périphérique)**. Si vous désactivez ce privilège, l'administrateur ne verra pas l'onglet **Device (Périphérique)** et ne pourra pas accéder aux informations de configuration au niveau du pare-feu, telles que User-ID, haute disponibilité, et aux informations de configuration des profils ou des certificats de serveur. Pour un contrôle plus granulaire des objets que l'administrateur peut afficher, laissez l'option **Objects (Objets)** activée, puis activez ou désactivez des nœuds spécifiques dans l'onglet comme décrit dans la section Octroi d'un accès granulaire à l'onglet Périphérique.<br><br>*Vous ne pouvez pas activer l'accès aux nœuds **Admin Roles (Rôles administrateur)** ou **Administrators (Administrateurs)** pour un administrateur basé sur les rôles, même si vous activez un accès complet à l'onglet **Device (Périphérique)**.* | Oui | Non | Oui |

## Octroi d'un accès granulaire à l'onglet Surveillance

Dans certains cas, vous pouvez autoriser l'administrateur à afficher certaines zones, mais pas toutes, de l'onglet **Monitor (Surveillance)**. Par exemple, vous pouvez limiter les administrateurs des opérations aux journaux de configuration et journaux système uniquement, parce qu'ils ne contiennent pas de données utilisateur sensibles. Bien que cette section de la définition du rôle administrateur indique les zones de l'onglet **Monitor (Surveillance)** que l'administrateur peut afficher, vous pouvez aussi combiner des privilèges de cette section aux privilèges de la vie privée, tels que la désactivation de la capacité à afficher les noms d'utilisateurs dans les journaux et les rapports. Cependant, n'oubliez pas que tous les rapports générés par le système afficheront toujours les noms d'utilisateurs et les adresses IP, même si vous désactivez cette fonctionnalité dans le rôle. Pour cette raison, si vous ne souhaitez pas que l'administrateur puisse afficher les informations confidentielles de l'utilisateur, désactivez l'accès aux rapports spécifiques conformément aux instructions fournies dans le tableau suivant.

Le tableau suivant répertorie les niveaux d'accès de l'onglet **Monitor (Surveillance)** et les rôles administrateur pour lesquels ils sont disponibles.

*Les rôles Modèle et Groupe de périphériques peuvent afficher uniquement les données de journaux des groupes de périphériques qui se trouvent dans les domaines d'accès affectés à ces rôles.*

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lecture seule | Désact |
|---|---|---|---|---|---|
| surveiller | Active ou désactive l'accès à l'onglet **Surveillance**. Si ce privilège est désactivé, l'administrateur ne verra pas cet onglet ni aucun des journaux ou rapports qui lui sont associés. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Journaux | Active ou désactive l'accès à tous les fichiers journaux. Vous pouvez aussi laisser ce privilège activé puis désactiver des journaux spécifiques si vous ne souhaitez pas que l'administrateur puisse les afficher. N'oubliez pas que, si vous souhaitez protéger la vie privée de vos utilisateurs tout en fournissant toujours un accès à un ou plusieurs des journaux, vous pouvez désactiver l'option **Privacy (Vie privée)** > **Show Full IP Addresses (Montrer les adresses IP en intégralité)** et/ou l'option **Show User Names In Logs And Reports (Montrer les noms des utilisateurs dans les journaux et les rapports)**. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Trafic | Indique si l'administrateur peut afficher les journaux du trafic. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Prévention | Indique si l'administrateur peut afficher les journaux des menaces. | Pare-feu : Oui<br>Panorama : Oui | Oui | Non | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lecture seule | Désact |
|---|---|---|---|---|---|
| | | Modèle/Groupe de périphériques : Oui | | | |
| Filtrage des URL | Indique si l'administrateur peut afficher les journaux de filtrage des URL. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Envois WildFire | Indique si l'administrateur peut afficher les journaux WildFire. Ces journaux ne sont disponibles que si vous disposez d'un abonnement WildFire. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Filtrage des données | Indique si l'administrateur peut afficher les journaux de filtrage des données. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Correspondance HIP | Indique si l'administrateur peut afficher les journaux de correspondance HIP. Les journaux de correspondance HIP ne sont disponibles que si vous disposez d'une licence GlobalProtect (abonnement). | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| GlobalProtect | Indique si l'administrateur peut afficher les journaux des menaces. Les journaux de correspondance HIP ne sont disponibles que si vous disposez d'une licence GlobalProtect (abonnement). | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| User-id | Indique si l'administrateur peut afficher les journaux d'ID utilisateur. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lecture seule | Désact |
|---|---|---|---|---|---|
| GTP | Indique si l'opérateur de réseau mobile peut voir les journaux GTP. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Inspection des tunnels | Indique si l'administrateur peut afficher les journaux d'inspection des tunnels. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| SCTP | Indique si l'opérateur du réseau mobile peut voir les journaux Stream Control Transmission Protocol (protocole de transmission de contrôle de flux ; SCTP).<br>*Vous devez activer SCTP sur Panorama (**Device (Périphérique) > Setup (Configuration) > Management (Gestion)**) avant de pouvoir contrôler l'accès administrateur aux journaux SCTP, aux rapports personnalisés ou aux rapports prédéfinis pour le Groupe/Modèle de Panorama et du périphérique.* | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Configuration | Indique si l'administrateur peut afficher les journaux de configuration. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Non | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lecture seule | Désact |
|---|---|---|---|---|---|
| system | Indique si l'administrateur peut afficher les journaux de système. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Non | Oui |
| Alarmes | Indique si l'administrateur peut afficher les alarmes générées par le système. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Authentification | Indique si l'administrateur peut afficher les journaux d'authentification. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Non | Oui |
| Moteur de corrélation automatique | Active ou désactive l'accès aux objets de corrélation et aux journaux des événements corrélés générés sur le pare-feu. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Objets de corrélation | Indique si l'administrateur peut afficher et activer/désactiver les objets de corrélation. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Événements corrélés | Spécifie si l'administrateur peut afficher et activer/désactiver les événements de corrélation. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Capture de paquets | Indique si l'administrateur peut afficher les captures de paquets (pcaps) à partir de l'onglet **Monitor (Surveillance)**. N'oubliez pas que les captures de paquets sont des données de flux brutes et peuvent à ce titre contenir les adresses IP des utilisateurs. La désactivation des privilèges **Show Full IP** | Pare-feu : Oui<br>Panorama : Non<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lecture seule | Désact |
|---|---|---|---|---|---|
| | **Addresses (Montrer les adresses IP en intégralité)** ne masquera pas l'adresse IP dans la pcap, c'est pourquoi vous devez désactiver le privilège Captures de paquets si vous êtes soucieux de la vie privée de l'utilisateur. | | | | |
| App-Scope | Indique si l'administrateur peut afficher les outils de visibilité et d'analyse App-Scope. L'activation du privilège Appscope autorise l'accès à tous les diagrammes du **Appscope**. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Navigateur de session | Indique si l'administrateur peut parcourir et filtrer les sessions en cours sur le pare-feu. N'oubliez pas que le navigateur de session affiche des données de flux brutes et qu'elles peuvent à ce titre contenir les adresses IP des utilisateurs. La désactivation des privilèges **Show Full IP Addresses (Montrer les adresses IP en intégralité)** ne masquera pas l'adresse IP dans le navigateur de session, c'est pourquoi vous devez désactiver le privilège **Session Browser (Navigateur de session)** si vous êtes soucieux de la vie privée de l'utilisateur. | Pare-feu : Oui<br>Panorama : Non<br>Modèle/Groupe de périphériques : Non | Oui | Non | Oui |
| Liste d'adresses IP bloquées. | Indique si l'administrateur peut afficher la liste d'adresses IP bloquées (Activer ou Lecture Seule) et effacer des entrées de la liste (Activer). Si vous désactivez ce paramètre, l'administrateur ne pourra pas afficher ou effacer des entrées de la liste d'adresses bloquées. | Pare-feu : Oui<br>Panorama : sous l'interface utilisateur Commutation de Contexte : Oui<br>Modèle : Oui | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lecture seule | Désact |
|---|---|---|---|---|---|
| Botnet (Réseau de robots) | Indique si l'administrateur peut générer et afficher des rapports d'analyse du Botnet ou afficher des rapports du Botnet en mode lecture seule. La désactivation des privilèges **Show Full IP Addresses (Montrer les adresses IP en intégralité)** ne masquera pas l'adresse IP dans les rapports d'analyse du Botnet programmés, c'est pourquoi vous devez désactiver le privilège **Botnet** si vous êtes soucieux de la vie privée de l'utilisateur. | Pare-feu : Oui<br>Panorama : Non<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |
| Rapports PDF | Active ou désactive l'accès à tous les rapports PDF. Vous pouvez aussi laisser ce privilège activé puis désactiver les rapports PDF spécifiques si vous ne souhaitez pas que l'administrateur puisse les afficher. N'oubliez pas que, si vous souhaitez protéger la vie privée de vos utilisateurs tout en fournissant toujours un accès à un ou plusieurs des rapports, vous pouvez désactiver l'option **Privacy (Vie privée)** > **Show Full IP Addresses (Montrer les adresses IP en intégralité)** et/ou l'option **Show User Names In Logs And Reports (Montrer les noms des utilisateurs dans les journaux et les rapports)**. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Gérer le récapitulatif PDF | Indique si l'administrateur peut afficher, ajouter ou supprimer des définitions dans les rapports récapitulatifs au format PDF. Avec l'accès en lecture seule, l'administrateur peut afficher des définitions dans les rapports récapitulatifs au format PDF, mais ne peut ni les ajouter ni les supprimer. Si vous désactivez cette option, l'administrateur ne | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lecture seule | Désact |
|---|---|---|---|---|---|
| | peut ni afficher les définitions dans les rapports, ni les ajouter, ni les supprimer. | | | | |
| rapports récapitulatifs au format PDF | Indique si l'admin peut afficher les rapports de récapitulation PDF générés dans **Monitor (Surveillance)** > **Reports (Rapports)**. Si vous désactivez cette option, la catégorie **PDF Summary Reports (Rapports de récapitulation PDF)** ne sera pas affichée dans le nœud **Reports (Rapports)**. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Rapport d'activités des utilisateurs | Indique si l'administrateur peut afficher, ajouter ou supprimer des définitions dans les rapports d'activités des utilisateurs et télécharger les rapports. Grâce à l'accès en lecture seule, l'administrateur peut afficher des définitions dans les rapports d'activités des utilisateurs, mais ne peut ni les ajouter, ni les supprimer, ni les télécharger. Si vous désactivez cette option, l'administrateur ne peut pas afficher cette catégorie de rapports PDF. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Oui | Oui |
| Rapport d'utilisation de l'application SaaS | Indique si l'administrateur peut afficher, ajouter ou supprimer un rapport d'utilisation de l'application SaaS. Avec l'accès en lecture seule, l'administrateur peut afficher des définitions dans les rapports d'utilisation de l'application SaaS, mais ne peut ni les ajouter ni les supprimer. Si vous désactivez cette option, l'administrateur ne peut ni afficher les définitions dans les rapports, ni les ajouter, ni les supprimer. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lecture seule | Désact |
|---|---|---|---|---|---|
| Groupes de rapports | Indique si l'administrateur peut afficher, ajouter ou supprimer des définitions dans les groupes de rapports. Grâce à l'accès en lecture seule, l'administrateur peut afficher des définitions dans les groupes de rapports, mais ne peut ni les ajouter ni les supprimer. Si vous désactivez cette option, l'administrateur ne peut pas afficher cette catégorie de rapports PDF. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Oui | Oui |
| Planificateur de messagerie | Indique si l'administrateur peut planifier les groupes de rapports pour la messagerie. Comme les rapports générés qui sont envoyés par courrier électronique peuvent contenir des données utilisateur sensibles qui ne sont pas supprimées en désactivant l'option **Privacy (Vie privée)** > **Show Full IP Addresses (Montrer les adresses IP en intégralité)** et/ou les options **Show User Names In Logs And Reports (Montrer les noms des utilisateurs dans les journaux et les rapports)** et comme ils peuvent aussi afficher des données de journaux auxquelles l'administrateur n'a pas accès, vous devez désactiver l'option **Email Scheduler (Planificateur de messagerie)** si vous avez des exigences concernant la vie privée des utilisateurs. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Oui | Oui |
| Gérer les rapports personnalisés | Active ou désactive l'accès à toutes les fonctionnalités des rapports personnalisés. Vous pouvez aussi laisser ce privilège activé puis désactiver des catégories spécifiques de rapports personnalisés auxquelles vous ne souhaitez pas que | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lecture seule | Désact |
|---|---|---|---|---|---|
| | l'administrateur puisse avoir accès. N'oubliez pas que, si vous souhaitez protéger la vie privée de vos utilisateurs tout en fournissant toujours un accès à un ou plusieurs des rapports, vous pouvez désactiver l'option **Privacy (Vie privée)** > **Show Full IP Addresses (Montrer les adresses IP en intégralité)** et/ou l'option **Show User Names In Logs And Reports (Montrer les noms des utilisateurs dans les journaux et les rapports)**.<br><br>*Les rapports dont la génération est planifiée plutôt que les rapports générés sur demande afficheront l'adresse IP et les informations utilisateur. Dans ce cas, assurez-vous de limiter l'accès aux zones correspondantes dans les rapports. De plus, la fonctionnalité de rapport personnalisé ne limite pas la capacité à générer des rapports contenant des données des journaux exclus du rôle administrateur.* | | | | |
| Statistiques d'application | Indique si l'administrateur peut créer un rapport personnalisé qui inclut des données issues de la | Pare-feu : Oui<br>Panorama : Oui | Oui | Non | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lecture seule | Désact |
|---|---|---|---|---|---|
| | base de données de statistiques d'application. | Modèle/Groupe de périphériques : Oui | | | |
| Journal de filtrage des données | Indique si l'administrateur peut créer un rapport personnalisé qui inclut des données issues des journaux de filtrage des données. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| journal de menaces | Indique si l'administrateur peut créer un rapport personnalisé qui inclut des données issues des journaux des menaces. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Récapitulatif des menaces | Indique si l'administrateur peut créer un rapport personnalisé qui inclut des données issues de la base de données de récapitulatifs des menaces. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| journal du trafic | Indique si l'administrateur peut créer un rapport personnalisé qui inclut des données issues des journaux du trafic. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Récapitulatif du trafic | Indique si l'administrateur peut créer un rapport personnalisé qui inclut des données issues de la base de données de récapitulatifs du trafic. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Journal des URL | Indique si l'administrateur peut créer un rapport personnalisé qui inclut des données issues des journaux de filtrage des URL. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Correspondance HIP | Indique si l'administrateur peut créer un rapport personnalisé qui inclut des données issues du journal de correspondance HIP. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lecture seule | Désact |
|---|---|---|---|---|---|
| GlobalProtect | Indique si l'administrateur peut créer un rapport personnalisé qui inclut des données issues des journaux des menaces. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Journal WildFire | Indique si l'administrateur peut créer un rapport personnalisé qui inclut des données issues des journaux WildFire. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Journal GTP | Indique si l'opérateur de réseau mobile peut créer un rapport personnalisé qui inclut des données issues des journaux GTP. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Récapitulatif GTP | Indique si l'opérateur de réseau mobile peut créer un rapport personnalisé qui inclut des données issues des journaux GTP. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Journal des tunnels | Indique si l'administrateur peut créer un rapport personnalisé qui inclut des données issues des journaux d'inspection des tunnels. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Récapitulatif des tunnels | Indique si l'administrateur peut créer un rapport personnalisé qui inclut des données issues de la base de données de récapitulatif des tunnels. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Journaux SCTP | Indique si l'opérateur de réseau mobile peut créer un rapport personnalisé qui inclut des données issues des journaux SCTP. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Récapitulatif SCTP | Indique si l'opérateur de réseau mobile peut créer un rapport personnalisé qui | Pare-feu : Oui<br>Panorama : Oui | Oui | Non | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lecture seule | Désact |
|---|---|---|---|---|---|
| | inclut des données issues du récapitulatif SCTP. | Modèle/Groupe de périphériques : Oui | | | |
| User-ID | Indique si l'administrateur peut créer un rapport personnalisé qui inclut des données issues des journaux d'ID utilisateur. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Authentification | Indique si l'administrateur peut créer un rapport personnalisé qui inclut des données issues des journaux d'authentification. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Afficher les rapports personnalisés planifiés | Indique si l'admin peut afficher un rapport personnalisé dont la génération a été planifiée. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Afficher les rapports d'application prédéfinis | Indique si l'administrateur peut afficher des rapports d'application. Les privilèges de la vie privée n'ont pas d'impact sur les rapports disponibles sur le nœud **Monitor (Surveillance)** > **Reports (Rapports)**, c'est pourquoi vous devez désactiver l'accès aux rapports si vous avez des exigences concernant la vie privée des utilisateurs. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Afficher les rapports de menaces prédéfinis | Indique si l'admin peut afficher des rapports de menaces. Les privilèges de la vie privée n'ont pas d'impact sur les rapports disponibles sur le nœud **Monitor (Surveillance)** > **Reports (Rapports)**, c'est pourquoi vous devez désactiver l'accès aux rapports si vous avez des exigences concernant la vie privée des utilisateurs. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Afficher les rapports | Indique si l'administrateur peut afficher des rapports de filtrage | Pare-feu : Oui | Oui | Non | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lecture seule | Désact |
|---|---|---|---|---|---|
| de filtrage d'URL prédéfinis | des URL. Les privilèges de la vie privée n'ont pas d'impact sur les rapports disponibles sur le nœud **Monitor (Surveillance)** > **Reports (Rapports)**, c'est pourquoi vous devez désactiver l'accès aux rapports si vous avez des exigences concernant la vie privée des utilisateurs. | Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | | | |
| Afficher les rapports de trafic prédéfinis | Indique si l'administrateur peut afficher des rapports du trafic. Les privilèges de la vie privée n'ont pas d'impact sur les rapports disponibles sur le nœud **Monitor (Surveillance)** > **Reports (Rapports)**, c'est pourquoi vous devez désactiver l'accès aux rapports si vous avez des exigences concernant la vie privée des utilisateurs. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Afficher les rapports GTP prédéfinis | Indique si l'opérateur de réseau mobile peut voir les rapports GTP. Les privilèges de la vie privée n'ont pas d'impact sur les rapports disponibles sur le nœud **Monitor (Surveillance)** > **Reports (Rapports)**, c'est pourquoi vous devez désactiver l'accès aux rapports si vous avez des exigences concernant la vie privée des utilisateurs. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Afficher les rapports SCTP prédéfinis | Indique si l'opérateur de réseau mobile peut voir les rapports SCTP. Les privilèges de la vie privée n'ont pas d'impact sur les rapports disponibles sur le nœud **Monitor (Surveillance)** > **Reports (Rapports)**, c'est pourquoi vous devez désactiver l'accès aux rapports si vous avez des exigences concernant la vie privée des utilisateurs. | Pare-feu : Oui<br>Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |

## Octroi d'un accès granulaire à l'onglet Politiques

Si vous activez l'option Politiques dans le profil de rôle administrateur, vous pouvez ensuite activer, désactiver, ou fournir un accès en lecture seule à des nœuds spécifiques au sein de l'onglet si nécessaire pour le rôle administrateur que vous définissez. En autorisant l'accès à un type de politique spécifique, vous activez la capacité d'afficher, ajouter ou supprimer des règles de politique. En activant l'accès en lecture seule à une politique spécifique, vous autorisez l'administrateur à afficher la base de règles de politique correspondante, mais pas à ajouter ou supprimer des règles. La désactivation de l'accès à un type de politique spécifique empêche l'administrateur d'afficher la base des règles de politique.

Comme la politique qui est basée sur des utilisateurs spécifiques (par nom d'utilisateur ou adresse IP) doit être explicitement définie, les paramètres de la vie privée qui désactivent la capacité d'afficher les adresses IP en intégralité ou les noms d'utilisateurs ne s'appliquent pas à l'onglet Politiques. C'est pourquoi vous devez autoriser l'accès à l'onglet Politiques uniquement aux administrateurs qui sont exclus des restrictions concernant la vie privée de l'utilisateur.

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| Sécurité | Activez ce privilège pour autoriser l'administrateur à afficher, ajouter et/ou supprimer des règles de sécurité. Définissez le privilège sur Lecture seule si vous souhaitez que l'administrateur puisse afficher les règles, mais pas les modifier. Pour empêcher l'administrateur d'afficher la base de règles de sécurité, désactivez ce privilège. | Oui | Oui | Oui |
| NAT | Activez ce privilège pour autoriser l'administrateur à afficher, ajouter et/ou supprimer des règles NAT. Définissez le privilège sur Lecture seule si vous souhaitez que l'administrateur puisse afficher les règles, mais pas les modifier. Pour empêcher l'administrateur d'afficher la base de règles NAT, désactivez ce privilège. | Oui | Oui | Oui |
| QoS | Activez ce privilège pour autoriser l'administrateur à afficher, ajouter et/ou supprimer des règles QoS. Définissez le privilège sur Lecture seule si vous souhaitez que l'administrateur puisse afficher les règles, mais pas les modifier. Pour empêcher l'administrateur d'afficher la base de règles QoS, désactivez ce privilège. | Oui | Oui | Oui |
| Policy-Based Forwarding | Activez ce privilège pour autoriser l'administrateur à afficher, ajouter et/ | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| (transfert basé sur une politique - PBF) | ou supprimer des règles Policy-Based Forwarding (transfert basé sur une politique - PBF). Définissez le privilège sur Lecture seule si vous souhaitez que l'administrateur puisse afficher les règles, mais pas les modifier. Pour empêcher l'administrateur d'afficher la base de règles PBF, désactivez ce privilège. | | | |
| Déchiffrement | Activez ce privilège pour autoriser l'administrateur à afficher, ajouter et/ou supprimer des règles de décryptage. Définissez le privilège sur Lecture seule si vous souhaitez que l'administrateur puisse afficher les règles, mais pas les modifier. Pour empêcher l'administrateur d'afficher la base de règles de décryptage, désactivez ce privilège. | Oui | Oui | Oui |
| Broker de paquets réseau | Activez ce privilège pour autoriser l'administrateur à afficher, ajouter et/ou supprimer des règles de politique de Broker de paquets. Définissez le privilège sur Lecture seule si vous souhaitez que l'administrateur puisse afficher les règles, mais pas les modifier. Pour empêcher l'administrateur de voir la base de règles du Broker de paquets de réseau dans l'interface, désactivez ce privilège. | Oui | Oui | Oui |
| Inspection des tunnels | Activez ce privilège pour autoriser l'administrateur à afficher, ajouter et/ou supprimer des règles d'inspection des tunnels. Définissez le privilège sur Lecture seule si vous souhaitez que l'administrateur puisse afficher les règles, mais pas les modifier. Pour empêcher l'administrateur d'afficher la base de règles d'inspection des tunnels, désactivez ce privilège. | Oui | Oui | Oui |
| Contrôle prioritaire sur l'application | Activez ce privilège pour autoriser l'administrateur à afficher, ajouter et/ou supprimer des règles de politique de contrôle prioritaire sur l'application. Définissez le privilège sur Lecture seule si vous souhaitez que l'administrateur puisse afficher les règles, mais pas les modifier. | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | Pour empêcher l'administrateur d'afficher la base de règles de contrôle prioritaire sur l'application, désactivez ce privilège. | | | |
| Authentification | Activez ce privilège pour autoriser l'administrateur à afficher, ajouter et/ou supprimer des règles d'authentification. Définissez le privilège sur Lecture seule si vous souhaitez que l'administrateur puisse afficher les règles, mais pas les modifier. Pour empêcher l'administrateur d'afficher la base de règles d'authentification, désactivez ce privilège. | Oui | Oui | Oui |
| Protection DoS | Activez ce privilège pour autoriser l'administrateur à afficher, ajouter et/ou supprimer des règles de protection DoS. Définissez le privilège sur Lecture seule si vous souhaitez que l'administrateur puisse afficher les règles, mais pas les modifier. Pour empêcher l'administrateur d'afficher la base de règles de protection DoS, désactivez ce privilège. | Oui | Oui | Oui |
| SD-WAN | Activez ce privilège pour autoriser l'administrateur à afficher, ajouter et/ou supprimer des règles de politique SD-WAN. Définissez le privilège sur Lecture seule si vous souhaitez que l'administrateur puisse afficher les règles, mais pas les modifier. Pour empêcher l'administrateur d'afficher la base de règles de politique SD-WAN, désactivez ce privilège. | Oui | Oui | Oui |

## Octroi d'un accès granulaire à l'onglet Objets

Un ***objet*** est un conteneur qui regroupe des valeurs spécifiques de politique de filtrage, telles que les adresses IP, URL, applications ou services, pour une définition simplifiée des règles. Par exemple, un objet adresse peut contenir des définitions d'adresses IP spécifiques pour les serveurs Web et d'applications dans votre zone DMZ.

Au moment de déterminer d'autoriser ou non l'accès à l'onglet Objets dans son ensemble, vous devrez déterminer si l'administrateur doit avoir des responsabilités de définition des politiques. Si ce n'est pas le cas, l'administrateur n'a probablement pas besoin d'accéder à l'onglet. Toutefois, si l'administrateur peut avoir besoin de créer une politique, vous pouvez activer l'accès à l'onglet puis définir des privilèges d'accès granulaires au niveau du nœud.

En activant l'accès à un nœud spécifique, vous accordez à l'administrateur le privilège d'afficher, ajouter et supprimer le type d'objet correspondant. En accordant l'accès en lecture seule, vous autorisez l'administrateur à afficher les objets déjà définis, mais pas à en créer ou en supprimer. La désactivation d'un nœud empêche l'administrateur d'afficher le nœud dans l'interface Web.

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| Adresses | Indique si l'administrateur peut afficher, ajouter ou supprimer des objets adresse à utiliser dans une politique de sécurité. | Oui | Oui | Oui |
| Groupes d'adresses | Indique si l'administrateur peut afficher, ajouter ou supprimer des objets groupe d'adresses à utiliser dans une politique de sécurité. | Oui | Oui | Oui |
| Régions | Indique si l'administrateur peut afficher, ajouter ou supprimer des objets régions à utiliser dans une politique de sécurité, de décryptage ou DoS. | Oui | Oui | Oui |
| Applications | Indique si l'administrateur peut afficher, ajouter ou supprimer des objets application à utiliser dans une politique. | Oui | Oui | Oui |
| Groupes d'application | Indique si l'administrateur peut afficher, ajouter ou supprimer des objets groupe d'applications à utiliser dans une politique. | Oui | Oui | Oui |
| Filtres de l'application | Indique si l'administrateur peut afficher, ajouter ou supprimer des filtres d'applications pour simplifier les recherches récurrentes. | Oui | Oui | Oui |
| Services | Indique si l'administrateur peut afficher, ajouter ou supprimer des objets service à utiliser dans la création de règles de politique qui limitent les nombres de ports qu'une application peut utiliser. | Oui | Oui | Oui |
| Groupes de services | Indique si l'admin peut afficher, ajouter ou supprimer des objets groupe de services à utiliser dans une politique de sécurité. | Oui | Oui | Oui |
| Étiquettes | Indique si l'administrateur peut afficher, ajouter ou supprimer des étiquettes qui ont été définies sur le périphérique. | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| GlobalProtect | Indique si l'administrateur peut afficher, ajouter ou supprimer des objets et des profils HIP. Vous pouvez limiter l'accès aux deux types d'objets au niveau de GlobalProtect, ou accorder un contrôle plus granulaire en activant le privilège GlobalProtect et en limitant l'accès aux objets ou profils HIP. | Oui | Non | Oui |
| Objets HIP | Indique si l'administrateur peut afficher, ajouter ou supprimer des objets HIP, qui sont utilisés pour définir les profils HIP. Les objets HIP génèrent aussi des journaux de correspondance HIP. | Oui | Oui | Oui |
| Applications sans client | Indique si l'administrateur peut afficher, ajouter, modifier ou supprimer des applications VPN GlobalProtect sans client. | Oui | Oui | Oui |
| Groupes d'applications sans client | Indique si l'administrateur peut afficher, ajouter, modifier ou supprimer des groupes d'applications VPN GlobalProtect sans client. | Oui | Oui | Oui |
| Profils HIP | Indique si l'administrateur peut afficher, ajouter ou supprimer des profils HIP à utiliser dans une politique de sécurité et/ou pour la génération de journaux de correspondance HIP. | Oui | Oui | Oui |
| Listes dynamiques externes | Indique si l'administrateur peut afficher, ajouter ou supprimer des listes dynamiques externes à utiliser dans une politique de sécurité. | Oui | Oui | Oui |
| Objets personnalisés | Indique si l'administrateur peut afficher les signatures personnalisées contre les logiciels espions et les vulnérabilités. Vous pouvez limiter l'accès soit pour activer soit pour désactiver l'accès à toutes les signatures personnalisées à ce niveau, ou accorder un contrôle plus granulaire en activant le privilège Objets personnalisés et en limitant l'accès à chaque type de signature. | Oui | Non | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| Modèles de données | Indique si l'administrateur peut afficher, ajouter ou supprimer des signatures de modèles de données personnalisées à utiliser lors de la création de profils de protection contre les vulnérabilités personnalisés. | Oui | Oui | Oui |
| Logiciel espion | Indique si l'administrateur peut afficher, ajouter ou supprimer des signatures de logiciels espions personnalisées à utiliser lors de la création de profils de protection contre les vulnérabilités personnalisés. | Oui | Oui | Oui |
| Vulnérabilité | Indique si l'administrateur peut afficher, ajouter ou supprimer des signatures de vulnérabilités personnalisées à utiliser lors de la création de profils de protection contre les vulnérabilités personnalisés. | Oui | Oui | Oui |
| URL Category (Catégorie d'URL) | Indique si l'administrateur peut afficher, ajouter ou supprimer des catégories d'URL personnalisées à utiliser dans une politique. | Oui | Oui | Oui |
| Profils de sécurité | Indique si l'administrateur peut afficher les profils de sécurité. Vous pouvez limiter l'accès soit pour activer soit pour désactiver l'accès à tous les profils de sécurité à ce niveau, ou accorder un contrôle plus granulaire en activant le privilège Profils de sécurité et en limitant l'accès à chaque type de profil. | Oui | Non | Oui |
| Antivirus | Indique si l'administrateur peut afficher, ajouter ou supprimer des profils antivirus. | Oui | Oui | Oui |
| Antispyware | Indique si l'administrateur peut afficher, ajouter ou supprimer des profils antispyware. | Oui | Oui | Oui |
| Protection contre les vulnérabilités | Indique si l'administrateur peut afficher, ajouter ou supprimer des profils de protection contre les vulnérabilités. | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| Filtrage des URL | Indique si l'administrateur peut afficher, ajouter ou supprimer des profils de filtrage des URL. | Oui | Oui | Oui |
| Blocage des fichiers | Indique si l'administrateur peut afficher, ajouter ou supprimer des profils de blocage de fichiers. | Oui | Oui | Oui |
| Analyse WildFire | Indique si l'administrateur peut afficher, ajouter ou supprimer des profils d'analyse Wildfire. | Oui | Oui | Oui |
| Filtrage des données | Indique si l'administrateur peut afficher, ajouter ou supprimer des profils de filtrage des données. | Oui | Oui | Oui |
| Protection DoS | Indique si l'administrateur peut afficher, ajouter ou supprimer des profils de protection DoS. | Oui | Oui | Oui |
| Protection GTP | Indique si l'opérateur du réseau mobile peut afficher, ajouter ou supprimer des profils de protection GTP. | Oui | Oui | Oui |
| Protection SCTP | Indique si l'opérateur du réseau mobile peut afficher, ajouter ou supprimer des profils de protection Stream Control Transmission Protocol (protocole de transmission de contrôle de flux ; SCTP). | Oui | Oui | Oui |
| Groupes de profils de sécurité | Indique si l'administrateur peut afficher, ajouter ou supprimer des groupes de profils de sécurité. | Oui | Oui | Oui |
| Transfert des journaux | Indique si l'administrateur peut afficher, ajouter ou supprimer des profils de transfert des journaux. | Oui | Oui | Oui |
| Authentification | Indique si l'administrateur peut afficher, ajouter ou supprimer des objets avec mise en place d'authentification. | Oui | Oui | Oui |
| Profil de décryptage | Indique si l'administrateur peut afficher, ajouter ou supprimer des profils de décryptage. | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| Gestion des liens SD-WAN | Indique si l'administrateur peut ajouter ou supprimer des profils de Qualité de chemin, Qualité SaaS, Distribution de trafic et Correction des erreurs. | Oui | Non | Oui |
| Path Quality Profile (Profil de qualité du chemin d'accès) | Indique si l'administrateur peut afficher, ajouter ou supprimer des profils Qualité de chemin SD-WAN. | Oui | Oui | Oui |
| Profil de qualité SaaS | Indique si l'administrateur peut afficher, ajouter ou supprimer des profils de qualité Saas SD-WAN. | Oui | Oui | Oui |
| Profil de distribution du trafic | Indique si l'administrateur peut afficher, ajouter ou supprimer des profils de distribution du trafic SD-WAN. | Oui | Oui | Oui |
| Profil de correction des erreurs | Indique si l'administrateur peut afficher, ajouter ou supprimer des profils de correction d'erreur SD-WAN. | Oui | Oui | Oui |
| Profil du broker de paquets | Indique si l'administrateur peut afficher, ajouter ou supprimer des profils de Broker de paquets. | Oui | Oui | Oui |
| Calendriers | Indique si l'administrateur peut afficher, ajouter ou supprimer des calendriers pour limiter une politique de sécurité à une date et/ou plage horaire spécifiques. | Oui | Oui | Oui |

## Octroi d'un accès granulaire à l'onglet Réseau

Au moment de déterminer d'autoriser ou non l'accès à l'onglet **Network (Réseau)** dans son ensemble, vous devrez déterminer si l'administrateur doit avoir des responsabilités d'administration réseau, y compris pour l'administration de GlobalProtect. Si ce n'est pas le cas, l'administrateur n'a probablement pas besoin d'accéder à l'onglet.

Vous pouvez aussi définir un accès à l'onglet **Network (Réseau)** au niveau du nœud. En activant l'accès à un nœud spécifique, vous accordez à l'administrateur le privilège d'afficher, ajouter et supprimer les configurations du réseau correspondantes. En accordant l'accès en lecture seule, vous autorisez l'administrateur à afficher les configurations déjà définies, mais pas à en créer en ou supprimer. La désactivation d'un nœud empêche l'administrateur d'afficher le nœud dans l'interface Web.

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| Interfaces | Indique si l'administrateur peut afficher, ajouter ou supprimer des configurations d'interface. | Oui | Oui | Oui |
| Zones | Indique si l'administrateur peut afficher, ajouter ou supprimer des zones. | Oui | Oui | Oui |
| vlans | Indique si l'administrateur peut afficher, ajouter ou supprimer des VLAN. | Oui | Oui | Oui |
| Câbles virtuels | Indique si l'administrateur peut afficher, ajouter ou supprimer des câbles virtuels. | Oui | Oui | Oui |
| Routeurs virtuels | Indique si l'administrateur peut afficher, ajouter ou supprimer des routeurs virtuels. | Oui | Oui | Oui |
| Tunnels IPSec | Indique si l'administrateur peut afficher, ajouter ou supprimer des configurations de tunnel IPSec. | Oui | Oui | Oui |
| Tunnels GRE | Indique si l'administrateur peut afficher, ajouter ou supprimer des configurations de tunnel GRE. | Oui | Oui | Oui |
| DHCP | Indique si l'administrateur peut afficher, ajouter ou supprimer des configurations de serveur DHCP et de relais DHCP. | Oui | Oui | Oui |
| Proxy DNS | Indique si l'administrateur peut afficher, ajouter ou supprimer des configurations de serveur proxy DNS. | Oui | Oui | Oui |
| GlobalProtect | Indique si l'administrateur peut afficher, ajouter ou modifier des configurations de portail et de passerelle GlobalProtect. Vous pouvez désactiver l'accès aux fonctions GlobalProtect complètement, ou vous pouvez activer le privilège GlobalProtect puis limiter le rôle aux zones de configuration du portail ou de la passerelle. | Oui | Non | Oui |
| Portails | Indique si l'administrateur peut afficher, ajouter, modifier ou supprimer des configurations de portail GlobalProtect. | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| Passerelles | Indique si l'administrateur peut afficher, ajouter, modifier ou supprimer des configurations de passerelle GlobalProtect. | Oui | Oui | Oui |
| Gestionnaire de périphériques mobiles | Indique si l'administrateur peut afficher, ajouter, modifier ou supprimer des configurations de serveur MDM GlobalProtect. | Oui | Oui | Oui |
| Liste d'interdictions de périphérique | Indique si l'administrateur peut afficher, ajouter, modifier ou supprimer des listes d'interdictions de périphérique. | Oui | Oui | Oui |
| Applications sans client | Indique si l'administrateur peut afficher, ajouter, modifier ou supprimer des applications VPN sans client. | Oui | Oui | Oui |
| Groupes d'applications sans client | Indique si l'administrateur peut afficher, ajouter, modifier ou supprimer des groupes d'applications VPN sans client. | Oui | Oui | Oui |
| QoS | Indique si l'administrateur peut afficher, ajouter, modifier ou supprimer des configurations QoS. | Oui | Oui | Oui |
| LLDP | Indique si l'administrateur peut afficher, ajouter, modifier ou supprimer des configurations LLDP. | Oui | Oui | Oui |
| profils réseaux | Définit l'état par défaut pour activer ou désactiver tous les paramètres réseau décrits ci-dessous. | Oui | Non | Oui |
| Crypto IPSec GlobalProtect | Contrôle l'accès au nœud **Network Profiles (Profils réseau)** > **GlobalProtect IPSec Crypto (Crypto IPSec GlobalProtect)**.<br>Si vous désactivez ce privilège, les administrateurs ne verront pas ce nœud ou ne pourront pas configurer les algorithmes d'authentification et de cryptage dans les tunnels VPN entre des clients et une passerelle GlobalProtect.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | profils crypto IPSec GlobalProtect, mais ne peut ni en ajouter ni les modifier. | | | |
| Passerelles IKE | Contrôle l'accès au nœud **Network Profiles (Profils de réseau)** > **IKE Gateways (Passerelles IKE)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **IKE Gateways (Passerelles IKE)** ou ne pourra pas définir les passerelles qui incluent les informations de configuration nécessaires à la négociation du protocole IKE avec les passerelles homologues.<br>Si le privilège est défini sur Lecture seule, vous pouvez afficher les passerelles IKE actuellement configurées, mais vous ne pouvez ni ajouter ni modifier des passerelles. | Oui | Oui | Oui |
| Crypto IPSec | Contrôle l'accès au nœud **Network Profiles (Profils de réseau)** > **IPSec Crypto (Crypto IPSec)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Network Profiles (Profils de réseau)** > **IPSec Crypto (Crypto IPSec)** ou ne pourra pas indiquer des protocoles et des algorithmes pour l'identification, l'authentification et le cryptage dans les tunnels VPN en fonction de la négociation SA IPSec.<br>Si le privilège est défini sur Lecture seule, vous pouvez afficher la configuration crypto IPSec actuellement configurée, mais vous ne pouvez ni ajouter ni modifier une configuration. | Oui | Oui | Oui |
| Crypto IKE | Contrôle la manière dont les périphériques échangent des informations pour garantir une communication sécurisée. Indiquez les protocoles et les algorithmes pour l'identification, l'authentification et le cryptage dans les tunnels VPN en fonction de la négociation SA IPSec (IKEv1 de phase 1). | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| surveiller | Contrôle l'accès au nœud **Network Profiles (Profils de réseau)** > **Monitor (Surveillance)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Network Profiles (Profils de réseau)** > **Monitor (Surveillance)** ou ne pourra pas créer ou modifier un profil de surveillance qui est utilisé pour surveiller les tunnels IPSec et pour surveiller un périphérique d'un saut suivant dans le cadre de règles de transfert basé sur une politique (PBF).<br>Si le privilège est défini sur Lecture seule, vous pouvez afficher la configuration de profil de surveillance actuellement configurée, mais vous ne pouvez ni ajouter ni modifier une configuration. | Oui | Oui | Oui |
| Gestion de l'interface | Contrôle l'accès au nœud **Network Profiles (Profils de réseau)** > **Interface Mgmt (Gestion de l'interface)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Network Profiles (Profils de réseau)** > **Interface Mgmt (Gestion de l'interface)** ou ne pourra pas indiquer les protocoles qui sont utilisés pour la gestion du pare-feu.<br>Si le privilège est défini sur Lecture seule, vous pouvez afficher la configuration de profil de gestion d'interface actuellement configurée, mais vous ne pouvez ni ajouter ni modifier une configuration. | Oui | Oui | Oui |
| protection de zones | Contrôle l'accès au nœud **Network Profiles (Profils de réseau)** > **Zone Protection (Protection de zone)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Network Profiles (Profils de réseau)** > **Zone Protection (Protection de zone)** ou ne pourra pas configurer un profil qui détermine la manière dont le pare-feu répond à des attaques issues de zones de sécurité spécifiées.<br>Si le privilège est défini sur Lecture seule, vous pouvez afficher la configuration de profil de protection de zone actuellement | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | configurée, mais vous ne pouvez ni ajouter ni modifier une configuration. | | | |
| Profil QoS | Contrôle l'accès au nœud **Network Profiles (Profils de réseau)** > **QoS**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Network Profiles (Profils de réseau)** > **QoS** ou ne pourra pas configurer un profil QoS qui détermine la manière dont les classes du trafic QoS sont traitées.<br>Si le privilège est défini sur Lecture seule, vous pouvez afficher la configuration de profil QoS actuellement configurée, mais vous ne pouvez ni ajouter ni modifier une configuration. | Oui | Oui | Oui |
| LLDP Profile (profil LLDP) | Contrôle l'accès au nœud **Network Profiles (Profils de réseau)** > **LLDP**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Network Profiles (Profils de réseau)** > **LLDP** ou ne pourra pas configurer un profil LLDP qui détermine si les interfaces sur le pare-feu peuvent participer à Link Layer Discovery Protocol (protocole de découverte de la couche de liaison - LLDP).<br>Si le privilège est défini sur Lecture seule, vous pouvez afficher la configuration de profil LLDP actuellement configurée, mais vous ne pouvez ni ajouter ni modifier une configuration. | Oui | Oui | Oui |
| Profil BFD | Contrôle l'accès au nœud **Network Profiles (Profils de réseau)** > **BFD Profile (Profil BFD)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Network Profiles (Profils de réseau)** > **BFD Profile (Profil BFD)** ou ne pourra pas créer de profil BFD. Un profil Bidirectional Forwarding Detection (BFD) vous permet de configurer les paramètres à appliquer à un ou plusieurs routages statiques ou à des protocoles de routage. De cette façon, le BFD détecte un lien défectueux ou un | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | BFD distant et permet un basculement extrêmement rapide.<br>Si le privilège est défini sur Lecture seule, vous pouvez afficher les profils BFD actuellement configurés, mais vous ne pouvez pas ajouter ni modifier de profil BFD. | | | |
| Profil d'interface SD-WAN | Contrôle l'accès au nœud du **SD-WAN Interface Profile (profil d'interface SD-WAN)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud du **SD-WAN Interface Profile (profil d'interface SD-WAN)** ou ne pourra pas configurer un profil d'interface SD-WAN. Un profil d'interface SD-WAN définit les caractéristiques des connexions ISP et spécifie la vitesse de la liaison et la fréquence à laquelle le pare-feu surveille la liaison.<br>Si le privilège est défini sur Lecture seule, vous pouvez afficher les profils d'interface SD-WAN actuellement configurés, mais vous ne pouvez pas en ajouter ni en modifier un. | Oui | Oui | Oui |

## Octroi d'un accès granulaire à l'onglet Équipement

Pour définir les privilèges d'accès pour l'onglet **Device (Périphérique)**, lorsque vous créez ou modifiez un profil disposant de droits administrateur (**Device (Périphérique)** > **Admin Roles (Droits Administrateur)**), défilez jusqu'au nœud **Device (Périphérique)** sur l'onglet **WebUI**.

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| setup | Contrôle l'accès au nœud **Setup (Configuration)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Setup (Configuration)** ou ne pourra pas accéder aux informations de configuration des paramètres au niveau du périphérique, notamment celles des onglets Gestion, Opérations, Service, Content-ID, WildFire ou Session. | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | Si le privilège est défini sur Lecture seule, vous pouvez afficher la configuration actuelle, mais vous ne pouvez y apporter aucune modification. | | | |
| Gestion | Contrôle l'accès au nœud **Management (Gestion)**. Si vous désactivez ce privilège, l'administrateur ne pourra pas configurer les paramètres comme le nom d'hôte, le domaine, le fuseau horaire, l'authentification, l'enregistrement et le suivi, les connexions à Panorama, la bannière, le message, ainsi que les paramètres relatifs à la complexité des mots de passe, et bien d'autres encore.<br>Si le privilège est défini sur Lecture seule, vous pouvez afficher la configuration actuelle, mais vous ne pouvez y apporter aucune modification. | Oui | Oui | Oui |
| de production | Contrôle l'accès aux nœuds **Operations (Opérations)** et **Telemetry and Threat Intelligence (Télémétrie et Threat Intelligence)**. Si vous désactivez ce privilège, l'administrateur ne peut pas :<br>• Charger des configurations de pare-feu.<br>• Sauvegarder ou ignorer une configuration de pare-feu.<br>*Ce privilège s'applique uniquement aux options des **Device(Périphérique) > Operations(Opérations)**. Les privilèges Sauvegarder et Valider contrôlent si l'administrateur peut sauvegarder ou ignorer des configurations à travers les options **Config (Configuration) > Save (Sauvegarder)** et **Config (Configuration) > Revert (Ignorer)**.*<br>• Créer des logos personnalisés. | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | • Configurer la supervision SNMP ou les réglages du pare-feu.<br>• Configurer la fonctionnalité Services Statistiques.<br>• Configurer les réglages **Telemetry and Threat Intelligence (Télémétrie et Threat Intelligence)**.<br>Seuls les administrateurs avec le rôle prédéfini de Super-Utilisateur peuvent exporter ou importer des configurations de pare-feu et désactiver le pare-feu.<br>Seuls les administrateurs avec le rôle prédéfini de Super-Utilisateur ou Administrateur Périphérique peuvent redémarrer le pare-feu ou le plan de données.<br>Les administrateurs avec un rôle leur accordant uniquement un accès à des systèmes virtuels spécifiques ne peuvent pas charger, sauvegarder ou ignorer des configurations de pare-feu à travers les options de **Device (Périphérique)** > **Operations (Opérations)**. | | | |
| Services | Contrôle l'accès au nœud **Services**. Si vous désactivez ce privilège, l'administrateur ne pourra pas configurer des services pour les serveurs DNS, pour un serveur de mise à jour, un serveur proxy, un serveur NTP ou configurer des lignes de services.<br>Si le privilège est défini sur Lecture seule, vous pouvez afficher la configuration actuelle, mais vous ne pouvez y apporter aucune modification. | Oui | Oui | Oui |
| Content-ID | Contrôle l'accès au nœud **Content-ID (ID du contenu)**. Si vous désactivez ce privilège, l'administrateur ne pourra pas configurer le filtrage des URL ou l'ID du contenu.<br>Si le privilège est défini sur Lecture seule, vous pouvez afficher la configuration | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | actuelle, mais vous ne pouvez y apporter aucune modification. | | | |
| WildFire | Contrôle l'accès au nœud **WildFire**. Si vous désactivez ce privilège, l'administrateur ne pourra pas configurer les paramètres WildFire.<br>Si le privilège est défini sur Lecture seule, vous pouvez afficher la configuration actuelle, mais vous ne pouvez y apporter aucune modification. | Oui | Oui | Oui |
| Session | Contrôle l'accès au nœud **Session**. Si vous désactivez ce privilège, l'administrateur ne pourra pas configurer les paramètres de session ou de délais d'expiration TCP, UDP ou ICMP, ou configurer le décryptage ou encore configurer des sessions VPN.<br>Si le privilège est défini sur Lecture seule, vous pouvez afficher la configuration actuelle, mais vous ne pouvez y apporter aucune modification. | Oui | Oui | Oui |
| HSM | Contrôle l'accès au nœud **HSM**. Si vous désactivez ce privilège, l'administrateur ne pourra pas configurer le module HSM.<br>Si le privilège est défini sur Lecture seule, vous pouvez afficher la configuration actuelle, mais vous ne pouvez y apporter aucune modification. | Oui | Oui | Oui |
| Haute disponibilité | Contrôle l'accès au nœud **Haute disponibilité (Haute disponibilité)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **High Availability (Haute disponibilité)** ou ne pourra pas accéder aux informations de configuration de haute disponibilité au niveau du périphérique, notamment celles sur les paramètres généraux ou la surveillance des liaisons et des chemins.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de configuration de Haute disponibilité pour le pare-feu, mais n'est | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | pas autorisé à effectuer les procédures de configuration. | | | |
| Audit de configuration | Contrôle l'accès au nœud **Config Audit (Audit de configuration)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Config Audit (Audit de configuration)** ou ne pourra pas accéder aux informations de configuration au niveau du pare-feu. | Oui | Non | Oui |
| Administrateurs | Contrôle l'accès au nœud **Administrators (Administrateurs)**. Cette fonction est uniquement autorisée pour l'accès en lecture seule.<br>Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Administrators (Administrateurs)** ou ne pourra pas accéder aux informations sur son propre compte administrateur.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de configuration sur son propre compte administrateur. Les administrateurs ne pourront pas afficher les informations sur d'autres comptes administrateurs configurés sur le pare-feu. | Non | Oui | Oui |
| Rôles administrateur | Contrôle l'accès au nœud **Admin Roles (Rôles administrateur)**. Cette fonction est uniquement autorisée pour l'accès en lecture seule.<br>Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Admin Roles (Rôles administrateur)** ou ne pourra pas accéder aux informations au niveau du pare-feu concernant la configuration des profils de rôles administrateur.<br>Si vous définissez ce privilège sur Lecture seule, vous pouvez afficher les informations de configuration pour tous les rôles administrateur configurés sur le pare-feu. | Non | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| Profil d'authentification | Contrôle l'accès au nœud **Authentication Profile (Profil d'authentification)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Authentication Profile (Profil d'authentification)** ou ne pourra ni créer ni modifier les profils d'authentification qui définissent les paramètres de base de données locale, RADIUS, TACACS+, LDAP ou Kerberos qui peuvent être associés à des comptes administrateurs. PAN-OS utilise des profils d'authentification pour authentifier les administrateurs de pare-feu et les utilisateurs finaux du portail d'authentification ou GlobalProtect.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de **Authentication Profile (Profil d'authentification)**, mais ne peut ni créer ni modifier un profil d'authentification. | Oui | Oui | Oui |
| Séquence d'authentification | Contrôle l'accès au nœud **Authentication Sequence (Séquence d'authentification)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Authentication Sequence (Séquence d'authentification)** ou ne pourra pas créer ou modifier une séquence d'authentification.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de **Authentication Sequence (Séquence d'authentification)**, mais ne peut ni créer ni modifier une séquence d'authentification. | Oui | Oui | Oui |
| Systèmes virtuels | Contrôle l'accès au nœud **Virtual Systems (Systèmes virtuels)**. Si vous désactivez ce privilège, l'administrateur ne verra pas ou ne pourra pas configurer les systèmes virtuels.<br><br>Si le privilège est défini sur Lecture seule, vous pouvez afficher les systèmes virtuels actuellement configurés, mais vous | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | ne pouvez pas ajouter ni modifier une configuration. | | | |
| Passerelles partagées | Contrôle l'accès au nœud **Shared Gateways (Passerelles partagées)**. Les passerelles partagées permettent aux systèmes virtuels de partager une interface commune pour les communications externes.<br>Si vous désactivez ce privilège, l'administrateur ne verra pas ou ne pourra pas configurer les passerelles partagées.<br>Si le privilège est défini sur Lecture seule, vous pouvez afficher les passerelles partagées actuellement configurées, mais vous ne pouvez pas ajouter ni modifier une configuration. | Oui | Oui | Oui |
| Identification utilisateur | Contrôle l'accès au nœud **User Identification (Identification utilisateur)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **User Identification (Identification utilisateur)** ou ne pourra pas accéder aux informations de configuration d'identification de l'utilisateur au niveau du pare-feu, telles que le mappage d'utilisateur, la sécurité de connexion, les agents User-ID, les agents Terminal Server, les paramètres de mappage de groupe ou les paramètres du portail d'authentification.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de configuration pour le pare-feu, mais n'est pas autorisé à effectuer les procédures de configuration. | Oui | Oui | Oui |
| Source d'informations de machine virtuelle | Contrôle l'accès au nœud **VM Information Source (Source d'informations de machine virtuelle)** qui vous permet de configurer le pare-feu/l'agent User-ID Windows pour collecter l'inventaire de machines virtuelles automatiquement. Si vous désactivez ce privilège, l'administrateur ne verra pas le | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | nœud **VM Information Source (Source d'informations de machine virtuelle)**.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les sources d'informations de machines virtuelles configurées, mais ne peut ni ajouter, ni modifier, ni supprimer les sources.<br>*Ce privilège n'est pas disponible pour les administrateurs de modèles et de groupes de périphériques.* | | | |
| Gestion des certificats | Définit l'état par défaut pour activer ou désactiver tous les paramètres de certificat décrits ci-dessous. | Oui | Non | Oui |
| Certificats | Contrôle l'accès au nœud **Certificates (Certificats)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Certificates (Certificats)** ou ne pourra pas configurer ou accéder aux informations relatives aux certificats du périphérique ou aux autorités de certification de confiance par défaut.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de configuration de certificat pour le pare-feu, mais n'est pas autorisé à effectuer les procédures de configuration. | Oui | Oui | Oui |
| Profil du certificat | Contrôle l'accès au nœud **Certificate Profile (Profil de certificat)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Certificate Profile (Profil de certificat)** ou ne pourra pas créer de profils de certificat.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les profils de certificat qui sont actuellement configurés pour le pare-feu, mais n'est pas autorisé à créer ou modifier un profil de certificat. | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| Répondeur OCSP | Contrôle l'accès au nœud **OCSP Responder (Répondeur OCSP)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **OCSP Responder (Répondeur OCSP)** ou ne pourra pas définir un serveur qui sera utilisé pour vérifier le statut de révocation des certificats émis par le pare-feu.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher la configuration de **OCSP Responder (Répondeur OCSP)** pour le pare-feu, mais n'est pas autorisé à créer ou modifier une configuration de répondeur OCSP. | Oui | Oui | Oui |
| Profil de service SSL/TLS | Contrôle l'accès au nœud **SSL/TLS Service Profile (Profil de service SSL/TLS)**.<br><br>Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud ou ne pourra pas configurer un profil qui spécifie un certificat et une version de protocole ou une plage de versions pour les services de pare-feu utilisant SSL/TLS.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les profils de service SSL/TLS, mais ne peut ni les créer ni les modifier. | Oui | Oui | Oui |
| SCEP | Contrôle l'accès au nœud **SCEP**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud SCEP ou ne pourra pas définir un profil qui spécifie des réglages pour un protocole simple d'enregistrement de certificat (SCEP) pour déployer des certificats uniques de périphérique.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les profils de SCEP, mais ne peut ni les créer ni les modifier. | Oui | Oui | Oui |
| Exclusion du décryptage SSL | Contrôle l'accès au nœud **SSL Decryption Exclusion (Exclusion du décryptage SSL)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | ou ne pourra ni afficher les exclusions du décryptage SSL ni les exclusions personnalisées.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les exclusions du décryptage SSL existantes, mais ne peut ni les créer ni les modifier. | | | |
| Pages de réponse | Contrôle l'accès au nœud **Response Pages (Pages de réponse)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Response Page (Page de réponse)** ou ne pourra pas définir un message HTML personnalisé qui est téléchargé et affiché à la place d'une page Web ou d'un fichier demandé(e).<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher la configuration de **Response Page (Page de réponse)** pour le pare-feu, mais n'est pas autorisé à créer ou modifier une configuration de page de réponse. | Oui | Oui | Oui |
| Paramètres des journaux | Définit l'état par défaut pour activer ou désactiver tous les paramètres des journaux décrits ci-dessous. | Oui | Non | Oui |
| system | Contrôle l'accès au nœud **Log Settings (Paramètres des journaux)** > **System (Système)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Log Settings (Paramètres des journaux)** > **System (Système)** ou ne pourra pas définir quels journaux système le pare-feu transfère à Panorama ou à un périphérique externe (comme un serveur syslog).<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les réglages de **Log Settings (Paramètres des journaux)** > **System (Système)** pour le pare-feu, mais ne peut ni les ajouter, ni les modifier, ni les supprimer. | Oui | Oui | Oui |
| Configuration | Contrôle l'accès au nœud **Log Settings (Paramètres des journaux)** > | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | **Configuration**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Log Settings (Paramètres des journaux)** > **Configuration (Configuration)** ou ne pourra pas définir quels journaux de configuration le pare-feu transfère à Panorama ou à un périphérique externe (comme un serveur syslog).<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les réglages de **Log Settings (Paramètres des journaux)** > **Configuration** pour le pare-feu, mais ne peut ni les ajouter, ni les modifier, ni les supprimer. | | | |
| User-id | Contrôle l'accès au nœud **Log Settings (Paramètres des journaux)** > **User-ID (ID utilisateur)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Log Settings (Paramètres des journaux)** > **User-ID (ID utilisateur)** ou ne pourra pas définir quels journaux User-ID le pare-feu transfère à Panorama ou à un périphérique externe (comme un serveur syslog).<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les réglages de **Log Settings (Paramètres des journaux)** > **User-ID (ID utilisateur)** pour le pare-feu, mais ne peut ni les ajouter, ni les modifier, ni les supprimer. | Oui | Oui | Oui |
| Correspondance HIP | Contrôle l'accès au nœud **Log Settings (Paramètres des journaux)** > **HIP Match (Correspondance HIP)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Log Settings (Paramètres des journaux)** > **HIP Match (Correspondance HIP)** ou ne pourra pas définir quels journaux de correspondance HIP le pare-feu transfère à Panorama ou à un périphérique externe (comme un serveur syslog). Les journaux de correspondance HIP fournissent des renseignements sur les règles de politiques de sécurité qui s'appliquent aux points de terminaison GlobalProtect. | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les réglages de **Log Settings(Paramètres des journaux)** > **HIP** pour le pare-feu, mais ne peut ni les ajouter, ni les modifier, ni les supprimer. | | | |
| GlobalProtect | Contrôle l'accès au nœud **Log Settings (Paramètres des journaux)** > **GlobalProtect**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Log Settings (Paramètres des journaux)** > **GlobalProtect** ou ne pourra pas définir quels journaux GlobalProtect le pare-feu transfère à Panorama ou à un périphérique externe (comme un serveur syslog).<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les réglages de **Log Settings (Paramètres des journaux)** > **GlobalProtect** pour le pare-feu, mais ne peut ni les ajouter, ni les modifier, ni les supprimer. | Oui | Oui | Oui |
| Corrélation | Contrôle l'accès au nœud **Log Settings (Paramètres des journaux)** > **Correlation (Corrélation)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Log Settings (Paramètres des journaux)** > **Correlation (Corrélation)** et ne pourra ni ajouter, supprimer ou modifier les réglages de transmission de journal de corrélation, ni identifier des adresses IP sources ou destinations.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les réglages de **Log Settings (Paramètres des journaux)** > **Correlation (Corrélation)** pour le pare-feu, mais ne peut ni les ajouter, ni les modifier, ni les supprimer. | Oui | Oui | Oui |
| Paramètres d'alarme | Contrôle l'accès au nœud **Log Settings (Paramètres des journaux)** > **Alarm Settings (Paramètres d'alarme)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Log Settings** | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | **(Paramètres des journaux)** > **Alarm Settings (Paramètres d'alarme)** et ne pourra pas configurer les notifications que le pare-feu génère quand une règle de politique de sécurité est attaquée à plusieurs reprises pendant un laps de temps paramétrable.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les réglages de **Log Settings (Paramètres des journaux)** > **Alarm Settings (Paramètres d'alarme)** pour le pare-feu, mais ne peut pas les modifier. | | | |
| Gestion des journaux | Contrôle l'accès au nœud **Log Settings (Paramètres des journaux)** > **Manage Logs (Gestion des journaux)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Log Settings (Paramètres des journaux)** > **Manage Logs (Gestion des journaux)** ou ne pourra pas effacer les journaux indiqués.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de **Log Settings (Paramètres des journaux)** > **Manage Logs (Gestion des journaux)**, mais ne peut effacer aucun journal. | Oui | Oui | Oui |
| Profils de serveur | Définit l'état par défaut pour activer ou désactiver tous les paramètres des profils de serveur décrits ci-dessous. | Oui | Non | Oui |
| Piège SNMP | Contrôle l'accès au nœud **Server Profiles (Profils de serveur)** > **SNMP Trap (Piège SNMP)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Server Profiles (Profils de serveur)** > **SNMP Trap (Piège SNMP)** ou ne pourra pas indiquer une ou plusieurs destinations de pièges SNMP à utiliser pour les entrées du journal système.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de **Server Profiles (Profils de** | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | **serveur)** > **SNMP Trap Logs (Journaux des Pièges SNMP)**, mais ne peut pas indiquer les destinations de pièges SNMP. | | | |
| Syslog | Contrôle l'accès au nœud **Server Profiles (Profils de serveur)** > **Syslog**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Server Profiles (Profils de serveur)** > **Syslog** ou ne pourra pas indiquer un ou plusieurs serveurs Syslog.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de **Server Profiles (Profils de serveur)** > **Syslog**, mais ne peut pas indiquer les serveurs Syslog. | Oui | Oui | Oui |
| Messagerie | Contrôle l'accès au nœud **Server Profiles (Profils de serveur)** > **Email (Messagerie)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Server Profiles (Profils de serveur)** > **Email (Messagerie)** ou ne pourra pas configurer un profil de messagerie qui peut être utilisé pour activer la notification par e-mail pour les entrées du journal système et de configuration.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de **Server Profiles (Profils de serveur)** > **Email (Messagerie)**, mais ne peut pas configurer un profil de serveur de messagerie. | Oui | Oui | Oui |
| HTTP | Contrôle l'accès au nœud **Server Profiles (Profils de serveur)** > **HTTP**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Server Profiles (Profils de serveur)** > **HTTP** ou ne pourra pas configurer un profil de serveur HTTP qui peut être utilisé pour activer le transfert de toute entrée du journal vers des destinations HTTP.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de **Server Profiles (Profils** | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | **de serveur)** > **HTTP**, mais ne peut pas configurer un profil de serveur HTTP. | | | |
| Netflow | Contrôle l'accès au nœud **Server Profiles (Profils de serveur)** > **Netflow**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Server Profiles (Profils de serveur)** > **Netflow** ou ne pourra pas définir un profil de serveur NetFlow, qui indique la fréquence de l'exportation ainsi que les serveurs NetFlow qui recevront les données exportées.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de **Server Profiles (Profils de serveur)** > **Netflow**, mais ne peut pas définir un profil Netflow. | Oui | Oui | Oui |
| RADIUS | Contrôle l'accès au nœud **Server Profiles (Profils de serveur)** > **RADIUS**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Server Profiles (Profils de serveur)** > **RADIUS** ou ne pourra pas configurer les paramètres des serveurs RADIUS identifiés dans les profils d'authentification.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de **Server Profiles (Profils de serveur)** > **RADIUS**, mais ne peut pas configurer les paramètres des serveurs RADIUS. | Oui | Oui | Oui |
| TACACS+ | Contrôle l'accès au nœud **Server Profiles (Profils de serveur)** > **TACACS+**.<br><br>Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud ou ne pourra pas configurer les paramètres des serveurs TACACS+ auxquels les profils d'authentification font référence.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les profils de serveur TACACS+, mais ne peut ni les ajouter ni les modifier. | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| LDAP | Contrôle l'accès au nœud **Server Profiles (Profils de serveur)** > **LDAP**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Server Profiles (Profils de serveur)** > **LDAP** ou ne pourra pas configurer les paramètres des serveurs LDAP à utiliser pour l'authentification par le biais de profils d'authentification.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de **Server Profiles (Profils de serveur)** > **LDAP**, mais ne peut pas configurer les paramètres des serveurs LDAP. | Oui | Oui | Oui |
| Kerberos | Contrôle l'accès au nœud **Server Profiles (Profils de serveur)** > **Kerberos**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Server Profiles (Profils de serveur)** > **Kerberos** ou ne pourra pas configurer un serveur Kerberos qui permet aux utilisateurs de s'authentifier de manière native auprès d'un contrôleur de domaine.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de **Server Profiles (Profils de serveur)** > **Kerberos**, mais ne peut pas configurer les paramètres des serveurs Kerberos. | Oui | Oui | Oui |
| Fournisseur d'identité SAML | Contrôle l'accès au nœud **Server Profiles (Profils de serveur)** > **SAML Identity Provider (Fournisseur d'identité SAML)**. Si vous désactivez ce privilège, l'administrateur ne peut pas afficher ni configurer les profils de serveur de fournisseur d'identité SAML.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de **Server Profiles (Profils de serveur)** > **SAML Identity Provider (Fournisseur d'identité SAML)**, mais ne | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | peut pas configurer les profils de serveur de fournisseur d'identité SAML. | | | |
| Authentification multifacteur | Contrôle l'accès au nœud **Server Profiles (Profils de serveur)** > **Multi Factor Authentication (Authentification multifacteur)**. Si vous désactivez ce privilège, l'administrateur ne peut pas afficher ni configurer les profils de serveur d'authentification multifacteur (MFA).<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de **Server Profiles (Profils de serveur)** > **SAML Identity Provider (Fournisseur d'identité SAML)**, mais ne peut pas configurer les profils de serveur MFA. | | | |
| Base de données locale d'utilisateurs | Définit l'état par défaut pour activer ou désactiver tous les paramètres de la base de données locale d'utilisateurs décrits ci-dessous. | Oui | Non | Oui |
| Users (Utilisateurs) | Contrôle l'accès au nœud **Local User Database (Base de données locale d'utilisateurs)** > **Users (Utilisateurs)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Local User Database (Base de données locale d'utilisateurs)** > **Users (Utilisateurs)** ou ne pourra pas configurer une base de données locale sur le pare-feu pour stocker les informations d'authentification pour les utilisateurs à accès distant, les administrateurs de périphériques, et les utilisateurs du portail d'authentification.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de **Local User Database (Base de données locale d'utilisateurs)** > **Users (Utilisateurs)**, mais ne peut pas configurer une base de données locale sur le pare-feu pour stocker des informations d'authentification. | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| Groupes d'utilisateurs | Contrôle l'accès au nœud **Local User Database (Base de données locale d'utilisateurs)** > **Users (Utilisateurs)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Local User Database (Base de données locale d'utilisateurs)** > **Users (Utilisateurs)** ou ne pourra pas ajouter des informations sur les groupes d'utilisateurs à la base de données locale.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de **Local User Database (Base de données locale d'utilisateurs)** > **Users (Utilisateurs)**, mais ne peut pas ajouter d'informations sur les groupes d'utilisateurs à la base de données locale. | Oui | Oui | Oui |
| Domaine d'accès | Contrôle l'accès au nœud **Access Domain (Domaine d'accès)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Domaine d'accès** ou ne pourra ni créer ni modifier un domaine d'accès.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de **Access Domain (Domaine d'accès)**, mais ne peut ni créer ni modifier un domaine d'accès. | Oui | Oui | Oui |
| Exportation planifiée des journaux | Contrôle l'accès au nœud **Scheduled Log Export (Exportation programmée des journaux)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Scheduled Log Export (Exportation programmée des journaux)** ou ne pourra pas planifier des exportations des journaux et les enregistrer sur un serveur File Transfer Protocol (protocole de transfert de fichiers - FTP) au format CSV ou utiliser la fonction Secure Copy (SCP) pour transférer des données en toute sécurité entre le périphérique et un hôte distant.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de **Scheduled Log Export** | Oui | Non | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | **(Exportation programmée des journaux)**, mais ne peut pas planifier l'exportation des journaux. | | | |
| Logiciels | Contrôle l'accès au nœud **Software (Logiciels)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Software (Logiciel)** ou ne pourra pas afficher les dernières versions du logiciel PAN-OS disponibles chez Palo Alto Networks, lire les notes de chaque version, puis sélectionner la version à télécharger et installer.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de **Software (Logiciels)** mais ne peut pas télécharger ou installer de logiciels. | Oui | Oui | Oui |
| Client GlobalProtect | Contrôle l'accès au nœud **GlobalProtect Client (Client GlobalProtect)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **GlobalProtect Client (Client GlobalProtect)** ou ne pourra pas afficher les versions disponibles de GlobalProtect, télécharger le code ou activer l'application GlobalProtect.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les versions du **GlobalProtect Client (Client GlobalProtect)** disponibles, mais ne peut ni télécharger ni installer le logiciel de l'application. | Oui | Oui | Oui |
| Mises à jour dynamiques | Contrôle l'accès au nœud **Dynamic Updates (Mises à jour dynamiques)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Dynamic Updates (Mises à jour dynamiques)** ou ne pourra pas afficher les dernières mises à jour, lire les notes de publication de chaque mise à jour, ou sélectionner une mise à jour à charger et installer. | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les versions de **Dynamic Updates (Mises à jour dynamiques)** disponibles, lire les notes de version, mais ne peut ni charger ni installer le logiciel. | | | |
| Licences | Contrôle l'accès au nœud **Licences**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Licences** ou ne pourra pas afficher les licences installées ou activer les licences.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les **Licences** installées mais ne peut pas exécuter les fonctions de gestion des licences. | Oui | Oui | Oui |
| Assistance | Contrôle l'accès au nœud **Support**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Support** ou ne pourra pas activer le support ou accéder aux alertes de production et de sécurité de Palo Alto Networks.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher le nœud **Support** et accéder aux alertes de production et de sécurité mais ne peut pas activer le support technique.<br>Seuls les administrateurs avec le rôle prédéfini de Super-Utilisateur peuvent utiliser le nœud **Support** pour générer des fichiers de support technique ou générer et télécharger des fichiers de vidage de statistiques ou des fichiers noyaux. | Oui | Oui | Oui |
| Clé principale et diagnostics | Contrôle l'accès au nœud **Master Key and Diagnostics (Clé principale et diagnostics)**. Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud **Master Key and Diagnostics (Clé principale et diagnostics)** ou ne pourra pas indiquer une clé principale pour crypter les clés privées sur le pare-feu. | Oui | Oui | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher le nœud **Master Key and Diagnostics (Clé principale et diagnostics)** et afficher les informations sur les clés principales qui ont été indiquées, mais ne peut ni ajouter ni modifier une nouvelle configuration de clé principale. | | | |
| Recommandations en matière de politique | Contrôle l'accès aux recommandations de règles de politique **IoT** et **SaaS**. Si vous désactivez ces privilèges, l'administrateur ne peut pas voir le nœud **Policy Recommendation (recommandation de politique)** > **IoT**, le nœud **Policy Recommendation (recommandation de politique)** > **SaaS** ou les deux, selon les privilèges que vous désactivez.<br>Si vous définissez ces privilèges en lecture seule, l'administrateur peut afficher les nœuds mais ne peut pas importer de règles de politique ou modifier des informations. | Oui | Oui | Oui |

## Définition des paramètres de la vie privée des utilisateurs dans le profil de rôle administrateur

Pour définir les données privées d'un utilisateur final auxquelles un administrateur peut accéder, lors de la création ou de la modification d'un profil de rôle administrateur (**Device (Périphérique)** > **Admin Roles (Rôles administrateur)**), faites défiler vers le bas jusqu'à ce que vous atteigniez l'option **Privacy (Vie privée)** à l'onglet **WebUI (Interface Web)**.

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| Vie privée | Définit l'état par défaut pour activer ou désactiver tous les paramètres de la vie privée décrits ci-dessous. | Oui | S. O. | Oui |
| Afficher les adresses IP en intégralité | Lorsque l'option est désactivée, les adresses IP complètes obtenues par le trafic passant par le pare-feu Palo Alto ne sont pas affichées dans les journaux ou les rapports. À la place des adresses IP qui sont normalement affichées, le sous-réseau correspondant s'affiche. | Oui | S. O. | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | *Les rapports programmés qui sont normalement affichés dans l'interface via **Monitor (Surveillance)** > **Reports (Rapports)** et les rapports qui sont envoyés via les messages électroniques planifiés afficheront toujours les adresses IP en intégralité. Compte tenu de cette exception, nous recommandons que les paramètres suivants au sein de l'onglet **Monitor (Surveillance)** soient désactivés : rapports personnalisés, rapports d'applications, rapports de menaces, rapports de filtrage des URL, rapports de trafic et planificateur de messagerie.* | | | |
| Afficher les noms des utilisateurs dans les journaux et les rapports | Lorsque l'option est désactivée, les noms des utilisateurs obtenus par le trafic passant par le pare-feu Palo Alto ne sont pas affichés dans les journaux ou les rapports. Les colonnes dans lesquelles les noms d'utilisateurs doivent normalement être affichés sont vides. | Oui | S. O. | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | *Les rapports programmés qui sont affichés dans l'interface via **Monitor (Surveillance) > Reports (Rapports)** ou les rapports qui sont envoyés via le planificateur de courrier électronique afficheront toujours les noms d'utilisateur. Compte tenu de cette exception, nous recommandons que les paramètres suivants de l'onglet Surveillance soient désactivés : rapports personnalisés, rapports d'applications, rapports de menaces, rapports de filtrage des URL, rapports de trafic et planificateur de messagerie.* | | | |
| Visualiser les fichiers PCAP | Lorsque l'option est désactivée, les fichiers de capture de paquets qui sont normalement disponibles dans les journaux du trafic, des menaces et de filtrage des données, ne sont pas affichés. | Oui | S. O. | Oui |

## Restriction de l'accès administrateur aux fonctions de validation et de confirmation

Pour restreindre l'accès aux fonctions de validation (et d'annulation), de sauvegarde et de confirmation quand vous créez ou modifiez le profil d'un rôle administrateur (**Device (Périphérique) > Admin Roles (Rôles Administrateur)**), défilez jusqu'aux options **Commit (Valider)**, **Save (Sauvegarder)**, et **Validate (Confirmer)** dans l'onglet **WebUI**.

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| Valider | Définit l'état par défaut pour activer ou désactiver tous les privilèges de validation et d'annulation décrits ci-dessous. | Oui | S. O. | Oui |
| Périphérique | Lorsque l'option est désactivée, un administrateur ne peut pas valider ou annuler les éventuelles modifications apportées à la configuration du pare-feu, y compris ses propres modifications. | Oui | S. O. | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| Valider pour les autres administrateurs | Lorsque l'option est désactivée, un administrateur ne peut pas valider ou annuler les éventuelles modifications apportées à la configuration du pare-feu par d'autres administrateurs. | Oui | S. O. | Oui |
| Save (Enregistrer) | Définit l'état par défaut pour activer ou désactiver toutes les privilèges d'opérations de sauvegarde décrits ci-dessous. | Oui | S. O. | Oui |
| Enregistrement partiel | Lorsque l'option est désactivée, un administrateur ne peut pas sauvegarder les éventuelles modifications apportées à la configuration du pare-feu par tout administrateur, y compris par lui-même ou elle-même. | Oui | S. O. | Oui |
| Enregistrer pour les autres administrateurs. | Lorsque l'option est désactivée, un administrateur ne peut pas sauvegarder les éventuelles modifications apportées à la configuration du pare-feu par d'autres administrateurs. | Oui | S. O. | Oui |
| Appliquer | Lorsque l'option est désactivée, un administrateur ne peut pas confirmer une configuration. | Oui | S. O. | Oui |

## Octroi d'un accès granulaire aux paramètres généraux

Pour définir le niveau d'accès de l'administrateur et des paramètres généraux, lorsque vous créez ou modifiez un profil disposant de droits administrateur (**Device (Périphérique)** > **Admin Roles (Droits Administrateur)**), défilez jusqu'à l'option **Global** sur l'onglet **WebUI**.

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| Globale | Définit l'état par défaut pour activer ou désactiver tous les paramètres généraux décrits ci-dessous. En réalité, ce paramètre est actuellement prévu pour les Alarmes système uniquement. | Oui | S. O. | Oui |
| Alarmes système | Lorsque l'option est désactivée, un administrateur ne peut pas afficher ou acquitter les alarmes qui sont générées. | Oui | S. O. | Oui |

## Octroi d'un accès granulaire à l'onglet Panorama

Le tableau suivant répertorie les niveaux d'accès de l'onglet **Panorama** et les rôles administrateur Panorama pour lesquels ils sont disponibles. Les administrateurs de pare-feu ne peuvent accéder à aucun de ces privilèges.

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| setup | Indique si l'administrateur peut afficher ou modifier les informations relatives à la configuration de Panorama, dont **Management (Gestion)**, **Operations (Opérations)** et **Telemetry (Télémétrie)**, **Services**, ID du contenu, **WildFire**, Session, ou **HSM**.<br>Si vous :<br>• définissez le privilège sur Lecture seule, l'administrateur peut afficher les informations, mais ne peut pas les modifier.<br>• désactivez ce privilège, l'administrateur ne peut ni afficher ni modifier ces informations. | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |
| Haute disponibilité | Indique si l'administrateur peut afficher et gérer les paramètres High Availability (haute disponibilité - HD) du serveur de gestion Panorama.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de configuration HD du serveur de gestion Panorama, mais ne peut pas les gérer.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les paramètres de configuration HD du serveur de gestion Panorama. | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| Audit de configuration | Indique si l'administrateur peut exécuter les audits de configuration Panorama. Si vous désactivez ce privilège, l'administrateur ne peut pas exécuter les audits de configuration Panorama. | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Non | Oui |
| Administrateurs | Indique si l'administrateur peut afficher les informations des comptes administrateurs Panorama.<br>Vous ne pouvez pas activer l'accès complet à cette fonction, uniquement l'accès en lecture seule. (Seuls les administrateurs Panorama disposant d'un rôle dynamique peuvent ajouter, modifier ou supprimer les administrateurs Panorama.) Avec l'accès en lecture seule, l'administrateur peut afficher les informations de son propre compte mais pas d'autres comptes administrateurs Panorama.<br>Si vous désactivez ce privilège, l'administrateur ne peut afficher aucune information de comptes administrateurs Panorama, y compris celles de son propre compte. | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Non | Oui | Oui |
| Rôles administrateur | Indique si l'administrateur peut afficher les rôles administrateur Panorama.<br>Vous ne pouvez pas activer l'accès complet à cette fonction, uniquement l'accès en lecture seule. (Seuls les administrateurs Panorama disposant d'un rôle dynamique peuvent ajouter, modifier ou supprimer les rôles Panorama | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Non | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | personnalisés.) Avec l'accès en lecture seule, l'administrateur peut afficher les configurations de rôle administrateur Panorama, mais ne peut pas les gérer.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les rôles administrateur Panorama. | | | | |
| Domaine d'accès | Indique si l'administrateur peut afficher, modifier, ajouter, supprimer ou cloner des configurations de domaines d'accès pour les administrateurs Panorama. (Ce | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | privilège contrôle uniquement l'accès à la configuration des domaines d'accès, pas l'accès aux groupes de périphériques, aux modèles et aux environnements de pare-feu affectés aux domaines d'accès.)<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les configurations de domaine d'accès Panorama, mais ne peut pas les gérer.<br><br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les configurations de domaine d'accès Panorama. | *Affectez des domaines d'accès aux administrateurs de modèles et de groupes de périphériques afin qu'ils puissent accéder aux données de configuration et de surveillance des groupes de périphériques, des modèles et des environnements de pare-feu affectés à ces domaines d'accès.* | | | |
| Profil d'authentification | Indique si l'administrateur peut afficher, ajouter, modifier, supprimer ou cloner des profils d'authentification pour les administrateurs Panorama.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les profils | Panorama : Oui<br><br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | d'authentification Panorama, mais ne peut pas les gérer.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les profils d'authentification Panorama. | | | | |
| Séquence d'authentification | Indique si l'administrateur peut afficher, ajouter, modifier, supprimer ou cloner des séquences d'authentification pour les administrateurs Panorama.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les séquences d'authentification Panorama, mais ne peut pas les gérer.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les séquences d'authentification Panorama. | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |
| Identification utilisateur | Indique si l'administrateur peut configurer la sécurité de connexion du User-ID et afficher, modifier ou supprimer des points de redistribution des données (comme des agents User-ID).<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les réglages des points de redistribution du User-ID et de la sécurité de sa connexion, mais ne peut pas les gérer.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les réglages des points de redistribution du User-ID et de la sécurité de sa connexion. | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| Périphériques gérés | Indique si l'administrateur peut afficher, ajouter, modifier, identifier ou supprimer des pare-feu en tant que périphériques gérés et y installer des mises à jour logicielles ou du contenu.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les pare-feu gérés, mais ne peut ni les ajouter, ni les supprimer, ni les identifier, ni y installer des mises à jour.<br><br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher, ni ajouter, ni modifier, ni identifier, ni supprimer les pare-feu gérés, ni y installer des mises à jour.<br><br>***Un administrateur disposant de privilèges de*** Déploiement de périphériques ***peut toujours utiliser* Panorama > Device Deployment (Déploiement de périphériques) *pour installer des mises à jour sur les pare-feu gérés.*** | Panorama : Oui<br><br>Modèle/Groupe de périphériques : Oui | Oui<br><br>(Non pour les administrateurs de modèles et de groupes de périphériques) | Oui | Oui |
| Modèles | Indique si l'administrateur peut afficher, modifier, ajouter ou supprimer des modèles et des piles de modèles. | Panorama : Oui<br><br>Modèle/Groupe de périphériques : Oui | Oui<br><br>(Non pour les administrateurs | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les configurations de modèles et de piles, mais ne peut pas les gérer.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les configurations de modèles et de piles. | *Les administrateurs de modèles et de groupes de périphériques peuvent afficher uniquement les modèles et les piles qui se trouvent dans les domaines d'accès affectés à ces administrateurs.* | de modèles et de groupes de périphériques) | | |
| Groupes de périphériques | Indique si l'administrateur peut afficher, modifier, ajouter ou supprimer des groupes de périphériques. | Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les configurations des groupes de périphériques, mais ne peut pas les gérer.<br><br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les configurations des groupes de périphériques. | *Les administrateurs de modèles et de groupes de périphériques peuvent accéder uniquement aux groupes de périphériques qui se trouvent dans les domaines d'accès affectés à ces administrateurs.* | | | |
| Collecteurs gérés | Indique si l'administrateur peut afficher, modifier, ajouter ou supprimer des collecteurs gérés.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les configurations de collecteurs gérés, mais ne peut pas les gérer.<br><br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher, ni modifier, ni ajouter, ni supprimer les configurations de collecteurs gérés. | Panorama : Oui<br><br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | *Un administrateur disposant de privilèges de Déploiement de périphériques peut toujours utiliser **Panorama > Device Deployment (Déploiement de périphériques)** pour installer des mises à jour sur les collecteurs gérés.* | | | | |
| Groupes de collecteurs | Indique si l'administrateur peut afficher, modifier, ajouter ou supprimer des groupes de collecteurs.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les groupes de collecteurs, mais ne peut pas les gérer.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les groupes de collecteurs. | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |
| VMware Service Manager | Indique si l'administrateur peut afficher et modifier les paramètres de VMware Service Manager.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les paramètres, mais ne peut effectuer aucune procédure de configuration ou opérationnelle associée.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher les paramètres ni effectuer de procédure de | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | configuration ou opérationnelle associée. | | | | |
| Gestion des certificats | Définit l'état par défaut, activé ou désactivé, de tous les privilèges de gestion des certificats Panorama. | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Non | Oui |
| Certificats | Indique si l'administrateur peut afficher, modifier, générer, supprimer, révoquer, renouveler ou exporter des certificats. Ce privilège indique également si l'administrateur peut importer ou exporter des clés HA.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les certificats Panorama, mais ne peut pas les gérer, tout comme les clés HD.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les certificats Panorama et les clés HD. | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |
| Profil du certificat | Indique si l'administrateur peut afficher, ajouter, modifier, supprimer ou cloner des profils de certificat Panorama.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les profils de certificat Panorama, mais ne peut pas les gérer.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les profils de certificat Panorama. | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |
| Profil de service SSL/TLS | Indique si l'administrateur peut afficher, ajouter, modifier, supprimer ou cloner des profils de service SSL/TLS. | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les profils de service SSL/TLS, mais ne peut pas les gérer.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les profils de service SSL/TLS. | | | | |
| Paramètres des journaux | Définit l'état par défaut, activé ou désactivé, de tous les privilèges de paramètres des journaux. | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Non | Oui |
| system | Indique si l'administrateur peut afficher et configurer les paramètres de transfert des journaux système vers des services externes (serveurs Syslog, de messagerie, de pièges SNMP ou HTTP).<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les paramètres de transfert des journaux système, mais ne peut pas les gérer.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les paramètres. | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | *Ce privilège se rapporte uniquement aux journaux système que génèrent Panorama et les Collecteurs de Journaux. Le privilège des* Groupes de Collecteurs *(**Panorama** > **Collector Groups (Groupes de Collecteurs)**) contrôle le transfert des journaux systèmes que les collecteurs de journaux reçoivent des pare-feu. Le privilège **Device (Périphérique)** > **Log Settings (Paramètres des journaux)** >* Système *contrôle le transfert des journaux depuis les pare-feux directement vers les services externes (sans agrégation dans les Collecteurs de Journaux).* | | | | |
| Configuration | Indique si l'administrateur peut afficher et configurer les paramètres de transfert des journaux de configuration vers des services externes (serveurs Syslog, de messagerie, de pièges SNMP ou HTTP). | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les paramètres de transfert des journaux de configuration, mais ne peut pas les gérer.<br><br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les paramètres. | | | | |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | *Ce privilège se rapporte uniquement aux journaux de configuration que génèrent Panorama et les Collecteurs de Journaux. Le privilège des* Groupes de Collecteurs *(**Panorama** > **Collector Groups (Groupes de Collecteurs)**) contrôle le transfert des journaux de configuration que les collecteurs de journaux reçoivent des pare-feux. Le privilège **Device (Périphérique)** > **Log Settings (Paramètres des journaux)** >* Configuration *contrôle le transfert des journaux depuis les pare-feu directement vers les services externes (sans agrégation dans les Collecteurs de Journaux).* | | | | |
| User-id | Indique si l'administrateur peut afficher et configurer les paramètres de transfert des journaux de User-ID vers des services externes | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | (serveurs Syslog, de messagerie, de pièges SNMP ou HTTP).<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les paramètres de transfert des journaux de configuration, mais ne peut pas les gérer.<br><br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les paramètres. | | | | |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | *Ce privilège se rapporte uniquement aux journaux de User-ID que génère Panorama. Le privilège des* Groupes de Collecteurs *(**Panorama** > **Collector Groups (Groupes de Collecteurs)**) contrôle le transfert des journaux de User-ID que les collecteurs de journaux reçoivent des pare-feux. Le privilège **Device (Périphérique)** > **Log Settings (Paramètres des journaux)** >* User-ID *contrôle le transfert des journaux depuis les pare-feux directement vers les services externes (sans agrégation dans les Collecteurs de Journaux).* | | | | |
| Correspondance HIP | Indique si l'administrateur peut afficher et configurer les paramètres de transfert des journaux de correspondance HIP depuis un équipement virtuel Panorama en mode Legacy vers des services externes (serveurs Syslog, de messagerie, de pièges SNMP ou HTTP). | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les paramètres de transfert des journaux de correspondance HIP, mais ne peut pas les gérer.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les paramètres.<br>*Le privilège des* Groupes de Collecteurs *(**Panorama** > **Collector Groups (Groupes de Collecteurs)**) contrôle le transfert des journaux de correspondance HIP que les collecteurs de journaux reçoivent des pare-feu. Le privilège **Device (Périphérique) > Log Settings (Paramètres des journaux)s** >* Correspondance HIP *contrôle le transfert des journaux depuis les pare-feux directement vers les services externes (sans agrégation dans les Collecteurs de Journaux).* | | | | |
| GlobalProtect | Indique si l'administrateur peut afficher et configurer les paramètres de transfert des | Panorama : Oui | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | journaux GlobalProtect depuis un appareil virtuel Panorama en mode Legacy vers des services externes (serveurs Syslog, de messagerie, de traps SNMP ou HTTP).<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les paramètres de transfert des journaux GlobalProtect, mais ne peut pas les gérer.<br><br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les paramètres. | Modèle/Groupe de périphériques : Non | | | |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | *Le privilège des* Groupes de Collecteurs *(**Panorama** > **Collector Groups (Groupes de Collecteurs)**) contrôle le transfert des journaux GlobalProtect que les collecteurs de journaux reçoivent des pare-feux. Le privilège **Device (Périphérique)** > **Log Settings (Paramètres des journaux)s** > **GlobalProtect** contrôle le transfert des journaux depuis les pare-feux directement vers les services externes (sans agrégation dans les Collecteurs de Journaux).* | | | | |
| Corrélation | Indique si l'administrateur peut afficher et configurer les paramètres de transfert des journaux de Corrélation depuis un équipement virtuel Panorama en mode Legacy vers des services externes (serveurs Syslog, de messagerie, de pièges SNMP ou HTTP).<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les paramètres de transfert des | Panorama : Oui<br><br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | journaux de corrélation, mais ne peut pas les gérer.<br><br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les paramètres.<br><br>*Le privilège des Groupes de Collecteurs (**Panorama > Collector Groups (Groupes de Collecteurs)**) contrôle le transfert des journaux de Corrélation depuis un appareil M-Series ou un appareil virtuel en mode Panorama.* | | | | |
| Trafic | Indique si l'administrateur peut afficher et configurer les paramètres de transfert des journaux de Trafic depuis un équipement virtuel Panorama en mode Legacy vers des services externes (serveurs Syslog, de messagerie, de pièges SNMP ou HTTP).<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les paramètres de transfert des journaux du trafic, mais ne peut pas les gérer.<br><br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les paramètres. | Panorama : Oui<br><br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | *Le privilège des* Groupes de Collecteurs *(**Panorama > Collector Groups (Groupes de Collecteurs)**) contrôle le transfert des journaux de Trafic que les collecteurs de journaux reçoivent des pare-feu. Le privilège* Transfert de Journaux *(**Objects (Objets) > Log Forwarding (Transfert de Journaux)**) contrôle le transfert des journaux depuis les pare-feu directement vers les services externes (sans agrégation dans les Collecteurs de Journaux).* | | | | |
| Prévention | Indique si l'administrateur peut afficher et configurer les paramètres de transfert des journaux de Menaces depuis un équipement virtuel Panorama en mode Legacy vers des services externes (serveurs Syslog, de messagerie, de pièges SNMP ou HTTP).<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les paramètres de transfert des journaux des menaces, mais ne peut pas les gérer. | Panorama : Oui<br><br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les paramètres.<br><br>*Le privilège des Groupes de Collecteurs (**Panorama > Collector Groups (Groupes de Collecteurs)**) contrôle le transfert des journaux de Menaces que les collecteurs de journaux reçoivent des pare-feu. Le privilège Transfert de Journaux (**Objects (Objets) > Log Forwarding (Transfert de Journaux)**) contrôle le transfert des journaux depuis les pare-feu directement vers les services externes (sans agrégation dans les Collecteurs de Journaux).* | | | | |
| WildFire | Indique si l'administrateur peut afficher et configurer les paramètres de transfert des journaux Wildifre depuis un équipement virtuel Panorama en mode Legacy vers des services externes (serveurs Syslog, de messagerie, de pièges SNMP ou HTTP).<br><br>Si vous définissez ce privilège sur Lecture seule, | Panorama : Oui<br><br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | l'administrateur peut afficher les paramètres de transfert des journaux WildFire, mais ne peut pas les gérer.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les paramètres.<br>*Le privilège des* Groupes de Collecteurs *(**Panorama > Collector Groups (Groupes de Collecteurs)**) contrôle le transfert des journaux WildFire que les collecteurs de journaux reçoivent des pare-feu. Le privilège* Transfert de Journaux *(**Objects (Objets) > Log Forwarding (Transfert de Journaux)**) contrôle le transfert des journaux depuis les pare-feu directement vers les services externes (sans agrégation dans les Collecteurs de Journaux).* | | | | |
| Profils de serveur | Définit l'état par défaut, activé ou désactivé, de tous les privilèges de profils de serveur. | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Non | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | *Ces privilèges concernent uniquement les profils de serveur utilisés pour le transfert des journaux depuis Panorama ou les Collecteurs de Journaux et les profils de serveur utilisés pour l'authentification des administrateurs Panorama. Les privilèges* ***Device (Périphérique)*** > Server Profiles (Profils de serveur) *contrôlent l'accès aux profils de serveur utilisés pour le transfert des journaux directement depuis les pare-feux vers les services externes et l'authentification des administrateurs de pare-feu.* | | | | |
| Piège SNMP | Indique si l'administrateur peut afficher et configurer les profils de serveurs de pièges SNMP.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les profils de serveurs de pièges SNMP, mais ne peut pas les gérer. | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les profils de serveurs de pièges SNMP. | | | | |
| Syslog | Indique si l'administrateur peut afficher et configurer les profils de serveurs Syslog.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les profils de serveurs Syslog, mais ne peut pas les gérer.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les profils de serveurs Syslog. | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |
| Messagerie | Indique si l'administrateur peut afficher et configurer les profils de serveurs de messagerie.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les profils de serveurs de messagerie, mais ne peut pas les gérer.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les profils de serveurs de messagerie. | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |
| RADIUS | Indique si l'administrateur peut afficher et configurer les profils de serveurs RADIUS utilisés pour l'authentification des administrateurs Panorama.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les profils de serveurs RADIUS, mais ne peut pas les gérer.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | afficher ni gérer les profils de serveurs RADIUS. | | | | |
| TACACS+ | Indique si l'administrateur peut afficher et configurer les profils de serveurs TACACS+ utilisés pour l'authentification des administrateurs Panorama.<br>Si vous désactivez ce privilège, l'administrateur ne verra pas le nœud ou ne pourra pas configurer les paramètres des serveurs TACACS+ auxquels les profils d'authentification font référence.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les profils de serveurs TACACS+, mais ne peut ni les ajouter ni les modifier. | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |
| LDAP | Indique si l'administrateur peut afficher et configurer les profils de serveur LDAP utilisés pour l'authentification des administrateurs Panorama.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les profils de serveur LDAP, mais ne peut pas les gérer.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les profils de serveur LDAP. | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |
| Kerberos | Indique si l'administrateur peut afficher et configurer les profils de serveur Kerberos utilisés pour l'authentification des administrateurs Panorama.<br>Si vous définissez ce privilège sur Lecture seule, | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | l'administrateur peut afficher les profils de serveur Kerberos, mais ne peut pas les gérer.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les profils de serveur Kerberos. | | | | |
| Fournisseur d'identité SAML | Indique si l'administrateur peut afficher et configurer les profils de serveurs de Fournisseurs d'identité SAML utilisés pour l'authentification des administrateurs Panorama.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les profils de serveurs de fournisseurs d'identité SAML, mais ne peut pas les gérer.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les profils de serveurs de fournisseurs d'identité SAML. | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |
| Exportation planifiée des configurations | Indique si l'administrateur peut afficher, ajouter, modifier, supprimer ou cloner des exportations planifiées des configurations Panorama.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les exportations planifiées, mais ne peut pas les gérer.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni gérer les exportations planifiées. | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Non | Oui |
| Logiciels | Indique si l'administrateur peut afficher des informations sur des mises à jour logicielles installées | Panorama : Oui | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | sur le serveur de gestion de Panorama, s'il peut télécharger, charger ou installer les mises à jour, et afficher les notes de version associées.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations sur les mises à jour logicielles Panorama ainsi que les notes de version associées, mais ne peut effectuer aucune opération associée.<br><br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher les mises à jour logicielles Panorama, ni afficher les notes de version associées, ni effectuer d'opération associée.<br><br>***Le privilège* Panorama > Déploiement de périphériques > Logiciels *contrôle l'accès aux logiciels PAN-OS déployés sur les pare-feux et aux logiciels Panorama déployés sur les collecteurs de journaux dédiés.*** | Modèle/Groupe de périphériques : Non | | | |
| Mises à jour dynamiques | Indique si l'administrateur peut afficher des informations sur des mises à jour de contenu installées sur le serveur de gestion de Panorama (par exemple, les mises à jour WildFire), s'il peut télécharger, charger, installer ou rétablir les mises à jour, et | Panorama : Oui<br><br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | afficher les notes de version associées.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations sur les mises à jour du contenu Panorama ainsi que les notes de version associées, mais ne peut effectuer aucune opération associée.<br><br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher les mises à jour du contenu Panorama, ni afficher les notes de version associées, ni effectuer d'opération associée.<br><br>*Le privilège **Panorama** > Déploiement de périphériques > Mises à jour dynamiques contrôle l'accès aux mises à jour du contenu déployées sur les pare-feux et les collecteurs de journaux dédiés.* | | | | |
| Assistance | Indique si l'administrateur peut afficher les informations de licence Panorama, les alertes produit et de sécurité, activer une licence de support et gérer des dossiers. Seul un administrateur super utilisateur peut générer des fichiers de support technique.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations de | Panorama : Oui<br><br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | support Panorama, les alertes produit et de sécurité, mais ne peut pas activer de licence de support, générer de fichier de support technique ni gérer de dossier.<br><br>Si vous désactivez ce privilège, l'administrateur ne peut pas afficher les informations de support Panorama, les alertes produit et de sécurité, activer de licence de support, générer de fichier de support technique ni gérer de dossier. | | | | |
| Déploiement de périphériques | Définit l'état par défaut, activé ou désactivé, de tous les privilèges associés au déploiement de licences et de logiciels ou de mises à jour de contenu pour des pare-feux et des collecteurs de journaux.<br><br>*Les privilèges **Panorama >** Logiciels **et Panorama >** Mises à jour dynamiques **contrôlent les mises à jour logicielles et du contenu installées sur un serveur de gestion de Panorama.*** | Panorama : Oui<br><br>Modèle/Groupe de périphériques : Oui | Oui | Non | Oui |
| Logiciels | Indique si l'administrateur peut afficher des informations sur les mises à jour logicielles installées sur les pare-feu et les collecteurs de journaux, télécharger, charger ou installer les mises à jour, et afficher les notes de version associées. | Panorama : Oui<br><br>Modèle/Groupe de périphériques : Oui | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| | Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations sur les mises à jour logicielles ainsi que les notes de version associées, mais ne peut pas déployer les mises à jour sur les pare-feux ou les collecteurs de journaux dédiés.<br><br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher les informations sur les mises à jour logicielles et les notes de version associées, ni déployer les mises à jour sur les pare-feu ou les collecteurs de journaux dédiés. | | | | |
| Client GlobalProtect | Indique si l'administrateur peut afficher des informations sur les mises à jour logicielles d'application GlobalProtect sur les pare-feu, s'il peut télécharger, charger ou activer les mises à jour, et afficher les notes de version associées.<br><br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations sur les mises à jour logicielles d'application GlobalProtect ainsi que les notes de version associées, mais ne peut pas activer les mises à jour sur les pare-feu.<br><br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher les informations sur les mises à jour logicielles d'application GlobalProtect et les notes de version associées, ni activer les mises à jour sur les pare-feu. | Panorama : Oui<br><br>Modèle/Groupe de périphériques : Oui | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| Mises à jour dynamiques | Indique si l'administrateur peut afficher des informations sur les mises à jour du contenu (par exemple, les mises à jour d'application) installées sur les pare-feu et les collecteurs de journaux dédiés, télécharger, charger ou installer les mises à jour, et afficher les notes de version associées.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les informations sur les mises à jour du contenu ainsi que les notes de version associées, mais ne peut pas déployer les mises à jour sur les pare-feu ou les collecteurs de journaux dédiés.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher les informations sur les mises à jour du contenu et les notes de version associées, ni déployer les mises à jour sur les pare-feu ou les collecteurs de journaux dédiés. | Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Oui | Oui |
| Licences | Indique si l'administrateur peut afficher, actualiser et activer des licences de pare-feux.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher les licences de pare-feux, mais ne peut pas les actualiser ni les activer.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher, ni actualiser, ni activer de licence de pare-feux. | Panorama : Oui<br>Modèle/Groupe de périphériques : Oui | Oui | Oui | Oui |

| Niveau d'accès | Description | Disponibilité du rôle administrateur | Activer | Lectu seule | Désact |
|---|---|---|---|---|---|
| Clé principale et diagnostics | Indique si l'administrateur peut afficher et configurer une clé principale avec laquelle crypter les clés privées sur Panorama.<br>Si vous définissez ce privilège sur Lecture seule, l'administrateur peut afficher la configuration de clé principale Panorama, mais ne peut pas la modifier.<br>Si vous désactivez ce privilège, l'administrateur ne peut ni afficher ni modifier la configuration de clé principale. | Panorama : Oui<br>Modèle/Groupe de périphériques : Non | Oui | Oui | Oui |

## Fournir un Accès granulaire aux paramètres des opérations

Pour définir les paramètres d'opération auxquels un administrateur a accès, lors de la création ou de la modification d'un profil de rôle d'administrateur pour un pare-feu (**Device (Périphérique)** > **Admin Roles (Rôles d'administrateur)**), faites défiler jusqu'à l'option **Operations (Opération** sous l'onglet **Web UI (Interface utilisateur Web)**.

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| Redémarrer | Redémarrez le pare-feu. Le pare-feu déconnecte tous les utilisateurs, recharge le logiciel PAN-OS et la configuration active, ferme et consigne les sessions existantes et crée une entrée de journal système qui affiche le nom de l'administrateur qui a initié le redémarrage. | Oui | S. O. | Oui |
| Créer un fichier d'assistance technique | Générez un fichier système d'assistance technique que l'équipe d'assistance de Palo Alto Networks peut utiliser pour résoudre les problèmes que vous pouvez rencontrer avec le pare-feu. | Oui | S. O. | Oui |
| Générer un fichier de vidage de statistiques | Générez et téléchargez un ensemble de rapports XML qui résument le trafic réseau au cours des sept derniers jours pour le pare-feu. | Oui | S. O. | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| Télécharger les fichiers de base | Si le pare-feu subit une défaillance du processus système, un fichier principal contenant des détails sur le processus et les raisons de son échec est généré automatiquement. Vous pouvez télécharger ce fichier de base pour le télécharger dans votre dossier d'assistance Palo Alto Networks afin d'obtenir de l'aide supplémentaire pour résoudre le problème. | Oui | S. O. | Oui |

## Privilèges d'accès à l'interface Web de Panorama

Les rôles administrateur Panorama personnalisés vous permettent de définir l'accès aux options sur Panorama et offrent la possibilité d'autoriser l'accès uniquement aux groupes de périphériques et aux modèles (onglets **Policies (Politiques)**, **Objects (Objets)**, **Network (Réseau)**, **Device (Périphérique)**).

Les rôles administrateur que vous pouvez créer sont **Panorama** et **Modèle et groupe de périphériques**. Vous ne pouvez affecter aucun privilège d'accès à la CLI à un profil de rôle administrateur **Modèle et groupe de périphériques**. Si vous affectez des privilèges d'accès super utilisateur à la CLI au profil de rôle administrateur **Panorama**, les administrateurs disposant de ce rôle peuvent accéder à toutes les fonctions, quels que soient les privilèges d'interface Web affectés.

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| Tableau de bord | Contrôle l'accès à l'onglet **Dashboard (Tableau de bord)**. Si vous désactivez ce privilège, l'administrateur ne verra pas l'onglet et ne pourra pas accéder aux widgets du Tableau de bord. | Oui | Non | Oui |
| ACC | Contrôle l'accès à l'Application Command Center (centre de commande des applications - ACC) Si vous désactivez ce privilège, l'onglet **ACC** ne sera pas affiché dans l'interface Web. N'oubliez pas que, si vous souhaitez protéger la vie privée de vos utilisateurs tout en fournissant toujours un accès à l'ACC, vous pouvez désactiver l'option **Privacy (Vie privée)** > **Show Full IP Addresses (Afficher les adresses IP en intégralité)** et/ou l'option **Show User Names In Logs And Reports (Afficher les noms des utilisateurs dans les journaux et les rapports)**. | Oui | Non | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| surveiller | Contrôle l'accès à l'onglet **Monitor (Surveillance)**. Si vous désactivez ce privilège, l'administrateur ne verra pas l'onglet **Monitor (Surveillance)** et ne pourra pas accéder aux journaux, captures de paquets, informations de session, rapports ou à Appscope. Pour un contrôle plus granulaire des informations de surveillance que l'administrateur peut afficher, laissez l'option Surveillance activée, puis activez ou désactivez des nœuds spécifiques dans l'onglet comme décrit dans la section Octroi d'un accès granulaire à l'onglet Surveillance. | Oui | Non | Oui |
| Politiques | Contrôle l'accès à l'onglet **Policies (Politiques)**. Si vous désactivez ce privilège, l'administrateur ne verra pas l'onglet **Policies (Politiques)** et n'aura accès à aucune information sur les politiques. Pour un contrôle plus granulaire des informations de politiques que l'administrateur peut afficher, par exemple pour activer l'accès à un type de politique spécifique ou pour activer l'accès en lecture seule aux informations de politiques, laissez l'option **Policies (Politiques)** activée, puis activez ou désactivez des nœuds spécifiques dans l'onglet comme décrit dans la section Octroi d'un accès granulaire à l'onglet Politiques. | Oui | Non | Oui |
| Objets | Contrôle l'accès à l'onglet **Objects (Objets)**. Si vous désactivez ce privilège, l'administrateur ne verra pas l'onglet **Objects (Objets)** et ne pourra pas accéder aux objets, profils de sécurité, profils de transfert de journal, profils de décryptage, ou calendriers. Pour un contrôle plus granulaire des objets que l'administrateur peut afficher, laissez l'option **Objects (Objets)** activée, puis activez ou désactivez des nœuds spécifiques dans l'onglet comme décrit dans la section Octroi d'un accès granulaire à l'onglet Objets. | Oui | Non | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| Réseau | Contrôle l'accès à l'onglet **Network (Réseau)**. Si vous désactivez ce privilège, l'administrateur ne verra pas l'onglet **Network (Réseau)** et ne pourra pas accéder aux informations de configuration des éléments tels que : interface, zone, VLAN, câble virtuel, routeur virtuel, tunnel IPsec, DHCP, serveur proxy DNS, GlobalProtect, ni aux informations de configuration QoS ou aux profils réseau. Pour un contrôle plus granulaire des objets que l'administrateur peut afficher, laissez l'option **Network (Réseau)** activée, puis activez ou désactivez des nœuds spécifiques dans l'onglet comme décrit dans la section Octroi d'un accès granulaire à l'onglet Réseau. | Oui | Non | Oui |
| Périphérique | Contrôle l'accès à l'onglet **Device (Périphérique)**. Si vous désactivez ce privilège, l'administrateur ne verra pas l'onglet **Périphérique** et ne pourra pas accéder aux informations de configuration au niveau du pare-feu, telles que User-ID, haute disponibilité, et aux informations de configuration des profils ou des certificats de serveur. Pour un contrôle plus granulaire des objets que l'administrateur peut afficher, laissez l'option **Device (Périphérique)** activée, puis activez ou désactivez des nœuds spécifiques dans l'onglet comme décrit dans la section Octroi d'un accès granulaire à l'onglet Périphérique.<br><br>*Vous ne pouvez pas activer l'accès aux nœuds **Admin Roles (Rôles administrateur)** ou **Administrators (Administrateurs)** pour un administrateur basé sur les rôles, même si vous activez un accès complet à l'onglet **Device (Périphérique)**.* | Oui | Non | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| Panorama | Contrôle l'accès à l'onglet **Panorama**. Si vous désactivez ce privilège, l'administrateur ne verra pas l'onglet **Panorama** et ne pourra pas accéder aux informations de configuration au niveau de Panorama, notamment celles des périphériques gérés, des collecteurs gérés ou des groupes de collecteurs.<br>Pour un contrôle plus granulaire des objets que l'administrateur peut afficher, laissez l'option **Panorama (Panorama)** activée, puis activez ou désactivez des nœuds spécifiques dans l'onglet comme décrit dans la section Fournir un Accès Granulaire à l'Onglet Panorama. | Oui | Non | Oui |
| Vie privée | Contrôle l'accès aux paramètres de la vie privée décrits dans la section Définition des paramètres de la vie privée des utilisateurs dans le profil de rôle administrateur. | Oui | Non | Oui |
| Appliquer | Lorsque l'option est désactivée, un administrateur ne peut pas confirmer une configuration. | Oui | Non | Oui |
| Save (Enregistrer) | Définit l'état par défaut (activé ou désactivé) de tous les privilèges d'enregistrement décrits ci-dessous (Enregistrement partiel et Enregistrement pour d'autres administrateurs). | Oui | Non | Oui |
| • Enregistrement partiel | Lorsque l'option est désactivée, un administrateur ne peut pas enregistrer les modifications faites par n'importe quel administrateur à la configuration Panorama. | Oui | Non | Oui |
| • Enregistrer pour les autres administrateurs. | Lorsque l'option est désactivée, un administrateur ne peut pas enregistrer les modifications faites par d'autres administrateurs à la configuration Panorama. | Oui | Non | Oui |
| Valider | Définit l'état par défaut (activé ou désactivé) de tous les privilèges de commit (valider), push (pousser) et revert (annuler) décrits ci-dessous (Panorama, Groupes | Oui | Non | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | d'Équipements, Modèles, Valeurs des Modèles Forcés, Groupes de Collecteurs, Clusters d'Équipements WildFire). | | | |
| • Panorama | Lorsque l'option est désactivée, un administrateur ne peut pas valider ou annuler les modifications de configuration effectuées par d'autres administrateurs, y compris ses propres modifications. | Oui | Non | Oui |
| • Valider pour les autres administrateurs | Lorsque l'option est désactivée, un administrateur ne peut pas valider ou annuler les modifications de configuration effectuées par d'autres administrateurs. | Oui | Non | Oui |
| Groupes de périphériques | Lorsque l'option est désactivée, un administrateur ne peut pas modifier les groupes d'équipements. | Oui | Non | Oui |
| Modèles | Lorsque l'option est désactivée, un administrateur ne peut pas modifier les modèles. | Oui | Non | Oui |
| Forcer les valeurs du modèle | Ce privilège contrôle l'accès à l'option **Force Template Values (Forcer les valeurs de modèle)** dans la boîte de dialogue de sélection de la portée de Push (l'opération Push).<br>Lorsque l'option est désactivée, un administrateur ne peut pas remplacer les paramètres substitués dans les configurations de pare-feu locales par les paramètres que Panorama pousse à partir d'un modèle. | Oui | Non | Oui |

| Niveau d'accès | Description | Activer | Lecture seule | Désactiva |
|---|---|---|---|---|
| | *Si vous transmettez un configuration avec l'option **Force Template Values (Forcer les valeurs du modèle)** activée, toutes les valeurs forcées du pare-feu sont remplacées par les valeurs du modèle. Avant d'utiliser cette option, vérifiez les valeurs forcées des pare-feu pour garantir que votre validation ne donne pas lieu à des pannes réseau imprévus ou à des problèmes causés par le remplacement de ces valeurs forcées.* | | | |
| Groupes de collecteurs | Lorsque l'option est désactivée, un administrateur ne peut pas modifier les groupes de collecteurs. | Oui | Non | Oui |
| Clusters d'appareils WildFire | Lorsque l'option est désactivée, un administrateur ne peut pas appliquer les modifications aux clusters d'appareils WildFire. | Oui | Non | Oui |
| Tâches | Lorsque l'option est désactivée, un administrateur ne peut pas accéder au Gestionnaire des tâches. | Oui | Non | Oui |
| Globale | Contrôle l'accès aux paramètres globaux (alarmes système) décrits dans la section Fournir un Accès Granulaire aux Paramètres Globaux<. | Oui | Non | Oui |

# Référence : Utilisation du numéro de port

Les tableaux suivants répertorient les ports utilisés par les pare-feux et par Panorama pour communiquer entre eux ou avec d'autres services sur le réseau.



## Ports utilisés pour les fonctions de gestion

Le pare-feu et Panorama utilisent les ports suivants pour les fonctions de gestion.

| Port de destination | Protocole | Description |
|---|---|---|
| 22 | TCP | Utilisé pour la communication entre un système client et l'interface de la CLI du pare-feu. |
| 80 | TCP | Port d'écoute du pare-feu pour les mises à jour du Protocole de vérification de statut de certificat en ligne ; OCSP lorsque le pare-feu agit en tant que répondeur OCSP. |
| 123 | UDP | Port utilisé par le pare-feu pour les mises à jour NTP. |
| 443 | TCP | Utilisé pour la communication entre un système client et l'interface Web du pare-feu. Il s'agit également du port d'écoute du pare-feu et de l'agent User-ID lorsque vous procédez à l'Activation de la surveillance des machines virtuelles pour suivre les modifications sur le réseau virtuel.<br>Pour surveiller l'environnement AWS, c'est le seul port utilisé.<br>Pour surveiller un environnement VMware vCenter/ESXi, le port d'écoute par défaut est 443, mais il est configurable. |
| 4443 | TCP | Utilisé comme port SSL alternatif pour HTTPS. |
| 162 | UDP | Port utilisé par le pare-feu, Panorama ou le collecteur de journaux pour Transférer les traps (pièges) vers un gestionnaire SNMP. |

| Port de destination | Protocole | Description |
|---|---|---|
| | | *Ce port n'a pas besoin d'être ouvert sur le pare-feu Palo Alto Networks. Vous devez configurer le gestionnaire Simple Network Management Protocol (protocole simple de gestion réseau - SNMP) pour écouter sur ce port. Pour plus d'informations, reportez-vous à la documentation de votre logiciel de gestion SNMP.* |
| 161 | UDP | Port du pare-feu à l'écoute des demandes d'interrogation (messages GET) du gestionnaire SNMP. |
| 514<br>514<br>6514 | TCP<br>UDP<br>SSL | Port que le pare-feu, Panorama ou un collecteur de journaux utilise pour envoyer des journaux à un serveur syslog si vous effectuez la Configuration de la surveillance Syslog, et les ports sur lesquels l'agent User-ID intégré à PAN-OS ou l'agent User-ID basé sur Windows écoute les messages syslog d'authentification. |
| 2055 | UDP | Port par défaut que le pare-feu utilise pour envoyer des enregistrements NetFlow à un collecteur NetFlow si vous effectuez la Configuration des exportations NetFlow, mais ceci est configurable. |
| 5008 | TCP | Port d'écoute de GlobalProtect Mobile Security Manager pour les demandes HIP des passerelles GlobalProtect.<br>Si vous utilisez un système MDM tiers, vous pouvez configurer la passerelle pour qu'elle utilise un port différent tel que requis par le fournisseur MDM. |
| 6080<br>6081<br>6082 | TCP<br>TLS 1.2<br>TCP | Ports utilisés pour le portail d'authentification User-ID™ :<br>• 6080 pour l'authentification NT LAN Manager (NTLM)<br>• 6081 pour le portail d'authentification sans profil de serveur SSL/TLS<br>• 6082 pour le portail d'authentification avec un profil de serveur SSL/TLS |
| 10443 | SSL | Port que le pare-feu et Panorama utilisent pour fournir des informations contextuelles sur une menace ou pour transférer votre enquête de menace de manière transparente à l'Archivage sécurisé des menaces et à AutoFocus. |

## Ports utilisés pour la HD

Les pare-feu configurés en tant qu'homologues HA (Haute disponibilité) doivent pouvoir communiquer entre eux afin de gérer les informations d'état (liaison de contrôle HA1) et de synchroniser les données (liaison de données HA2). Dans les déploiements HA active/active, les

pare-feu homologues doivent transférer les paquets à l'homologue HA auquel appartient la session. La liaison HA3 est une liaison de Couche 2 (MAC-in-MAC) qui ne prend pas en charge l'adressage ou le cryptage de Couche 3.

| Port de destination | Protocole | Description |
|---|---|---|
| 28769<br>28260 | TCP<br>TCP | Utilisé par la liaison de contrôle HA1 pour les communications en texte clair entre les pare-feu homologues HA. La liaison HA1 est une liaison de Couche 3 et exige une adresse IP. |
| 28 | TCP | Utilisé par la liaison de contrôle HA1 pour les communications cryptées (SSH sur TCP) entre les pare-feu homologues HA. |
| 28770 | TCP | Port d'écoute des liaisons de secours HA1. |
| 28771 | TCP | Port utilisé pour les sauvegardes de pulsations. Palo Alto Networks recommande d'activer la sauvegarde des pulsations sur l'interface MGT si vous utilisez un port sur bande pour les liaisons HA1 ou HA1 de secours. |
| 99<br>29281 | Adresse IP<br>UDP | Utilisé par la liaison HA2 pour la synchronisation des sessions, des tables de transfert, des associations de sécurité IPSec et des tables ARP entre les pare-feu d'une paire HA. Le flux de données de la liaison HA2 est toujours unidirectionnel (sauf pour la persistance HA2), du pare-feu actif (HA active/passive) ou actif-principal (HA active/active) vers le pare-feu passif (HA active/passive) ou actif-secondaire (HA active/active). La liaison HA2 est une liaison de Couche 2 et utilise l'EtherType 0x7261 par défaut.<br>La liaison de données HA peut également être configurée pour utiliser soit IP (numéro de protocole 99) ou UDP (port 29281) comme protocole de transport et permet donc à la liaison de données HA d'étendre les sous-réseaux. |

## Ports utilisés pour Panorama

Panorama utilise les ports suivants.

| Port de destination | Protocole | Description |
|---|---|---|
| 22 | TCP | Utilisé pour la communication entre un système client et l'interface de la CLI de Panorama. |
| 443 | TCP | Utilisé pour la communication entre un système client et l'interface Web de Panorama. |

| Port de destination | Protocole | Description |
|---|---|---|
| 444 | TCP | Utilisé pour la communication entre Panorama et le lac de données Cortex. |
| 3978 | TCP | Utilisé pour la communication entre Panorama et les pare-feu gérés ou les collecteurs gérés, ainsi que pour la communication entre les collecteurs gérés d'un groupe de collecteur :<br>• Pour la communication entre Panorama et les pare-feux. Cette connexion est initiée à partir du pare-feu géré vers Panorama et facilite un échange de données bidirectionnel sur lequel les pare-feu transmettent les journaux à Panorama et Panorama envoie les modifications de configuration aux pare-feux. Les commandes de commutation de contexte sont envoyées via la même connexion.<br>• Les collecteurs de journaux utilisent ce port de destination pour transférer les journaux à Panorama.<br>• Pour la communication avec le collecteur de journaux par défaut sur un appareil M-Series Panorama et avec les collecteurs de journaux dédiés. |
| 28443 | TCP | Utilisé pour les périphériques gérés (pare-feu et collecteurs de journaux) pour récupérer les mises à jour de logiciels et de contenu de Panorama.<br>***Seuls les périphériques qui utilisent PAN-OS 8.x et des versions ultérieures peuvent récupérer les mises à jour de Panorama en utilisant ce port. Pour les périphériques qui utilisent des versions antérieures, Panorama transmet les packages de mise à jour sur le port 3978.*** |
| 28769 (5.1 et versions ultérieures)<br>28260 (5.0 et versions ultérieures)<br>49160 (5.0 et versions antérieures) | TCP<br>TCP<br>TCP | Utilisé pour la connexion et la synchronisation HA entre les homologues HA Panorama utilisant les communications en texte clair. La communication peut être initiée par chaque homologue. |

| Port de destination | Protocole | Description |
|---|---|---|
| 28 | TCP | Utilisé pour la connexion et la synchronisation HA entre les homologues HA Panorama utilisant les communications cryptées (SSH sur TCP). La communication peut être initiée par chaque homologue.<br>Utilisé pour la communication entre les collecteurs de journaux d'un groupe de collecteurs pour la distribution des journaux. |
| 28270 (6.0 et versions ultérieures)<br>49190 (5.1 et versions antérieures) | TCP | Utilisé pour la communication entre les collecteurs de journaux d'un groupe de collecteurs pour la distribution des journaux. |
| 2049 | TCP | Utilisé par l'équipement virtuel Panorama pour la rédaction de journaux dans la banque de données NFS. |
| 10443 | SSL | Port que Panorama utilise pour fournir des informations contextuelles sur une menace ou pour transférer votre enquête de menace de manière transparente à l'Archivage sécurisé des menaces et à AutoFocus. |
| 23000 à 23999 | TCP, UDP ou SSL | Utilisé pour la communication Syslog entre Panorama et les composants ESM Traps (pièges). |

## Ports utilisés pour GlobalProtect

GlobalProtect utilise les ports suivants.

| Port de destination | Protocole | Description |
|---|---|---|
| 443 | TCP | Utilisé pour la communication entre les applications et les portails GlobalProtect ou les applications et les passerelles GlobalProtect et pour les connexions de tunnel SSL.<br>Les passerelles GlobalProtect utilisent également ce port pour collecter des informations d'hôte à partir des applications GlobalProtect et effectuer des vérifications du Host Information Profile (Profil des informations hôtes ; HIP). |
| 4501 | UDP | Utilisé pour les connexions de tunnel IPSec entre les applications et les passerelles GlobalProtect. |

Pour des astuces concernant l'utilisation d'une interface avec retour de boucle pour permettre l'accès à GlobalProtect sur différents ports et adresses, consultez le document Can GlobalProtect Portal Page be Configured to be Accessed on any Port ? (La page du portail GlobalProtect peut-elle être configurée pour être accessible sur n'importe quel port ?).

## Ports utilisés pour User-ID

User-ID est une fonction de mappage des adresses IP d'utilisateur aux noms d'utilisateurs et aux appartenances aux groupes, qui permet l'activation d'une politique en fonction d'un utilisateur ou d'un groupe et la visibilité de l'activité des utilisateurs sur votre réseau (par exemple, la localisation d'un utilisateur victime d'une menace). Pour effectuer ce mappage, le pare-feu, l'agent User-ID (installé sur un système Windows ou l'agent intégré à PAN-OS exécuté sur le pare-feu) et/ou l'agent Terminal Server doivent pouvoir se connecter aux services d'annuaire sur votre réseau afin de procéder au Mappage de groupe et au Mappage d'utilisateur. De plus, si les agents sont exécutés sur des systèmes externes au pare-feu, ils doivent pouvoir se connecter au pare-feu afin de communiquer l'adresse IP aux mappages de noms d'utilisateurs au pare-feu. Le tableau suivant répertorie les exigences de communication de User-ID ainsi que les numéros de ports nécessaires pour établir des connexions.

| Port de destination | Protocole | Description |
|---|---|---|
| 389 | TCP | Port utilisé par le pare-feu pour se connecter à un serveur LDAP (texte brut ou Start Transport Layer Security (Démarrer la sécurité de couche de transport ; Start TLS) pour Mapper les utilisateurs aux groupes. |
| 3268 | TCP | Port utilisé par le pare-feu pour se connecter à un serveur de catalogue global Active Directory (texte brut ou Démarrer TLS) pour Mapper les utilisateurs aux groupes. |
| 636 | TCP | Port utilisé par le pare-feu pour les connexions LDAP sur SSL avec un serveur LDAP pour Mapper les utilisateurs aux groupes. |
| 3269 | TCP | Port utilisé par le pare-feu pour les connexions LDAP sur SSL à un serveur de catalogues global Active Directory en vue de Mapper les utilisateurs aux groupes. |
| 514<br>6514 | TCP<br>UDP<br>SSL | Port d'écoute de l'agent User-ID pour les messages syslog d'authentification si vous effectuez la Configuration de User-ID pour surveiller les expéditeurs Syslog pour le mappage d'utilisateur. Le port dépend du type d'agent et du protocole :<br>• Agent User-ID intégré à PAN-OS - Port 6514 pour SSL et port 514 pour UDP.<br>• Agent User-ID Windows-Port 514 pour TCP et UDP. |
| 5007 | TCP | Port d'écoute du pare-feu pour l'obtention des informations de mappage auprès de l'agent User-ID ou Terminal Server. L'agent |

| Port de destination | Protocole | Description |
|---|---|---|
| | | envoie le mappage d'adresse IP/nom d'utilisateur ainsi que horodatage associé, à chaque fois qu'il apprend un mappage nouveau ou mis à jour. En outre, il se connecte au pare-feu à intervalles réguliers pour actualiser les mappages connus. |
| 5006 | TCP | Port d'écoute de l'agent User-ID pour les demandes de l'API XML. La source de cette communication est généralement le système exécutant un script qui appelle l'API. |
| 88 | UDP/TCP | Port utilisé par l'agent User-ID pour l'authentification d'un serveur Kerberos. Le pare-feu essaie d'abord UDP, puis a recours à TCP. |
| 1812 | UDP | Port utilisé par l'agent User-ID pour l'authentification d'un serveur RADIUS. |
| 49 | TCP | Port utilisé par l'agent User-ID pour l'authentification d'un serveur TACACS+. |
| 135 | TCP | Port utilisé par l'agent User-ID pour l'établissement de connexions WMI TCP avec le mappeur de terminal Microsoft Remote Procedure Call (appel de procédure distant - RPC). Le mappeur de terminale affecte ensuite l'agent à un port aléatoire de la plage de ports 49152-65535. L'agent utilise cette connexion pour effectuer des requêtes RPC de journaux de sécurité ou tables de session auprès du serveur AD ou Exchange. Il s'agit également du port utilisé pour l'accès aux Terminal Servers.<br><br>L'agent User-ID utilise également ce port pour la connexion aux systèmes clients afin d'effectuer le sondage Windows Management Instrumentation (WMI). |
| 139 | TCP | Port utilisé par l'agent User-ID pour l'établissement de connexions NetBIOS TCP avec le serveur AD afin de pouvoir envoyer des requêtes RPC de journaux de sécurité et d'informations de session.<br><br>L'agent User-ID utilise également ce port pour la connexion aux systèmes clients afin d'effectuer des sondages NetBIOS (fonction prise en charge par l'agent User-ID Windows uniquement). |
| 445 | TCP | Port utilisé par l'agent User-ID pour se connecter à Active Directory (AD) à l'aide de connexions SMB TCP au serveur AD afin d'accéder aux informations de connexion utilisateur (spouleur d'impression et Net Logon). |

| Port de destination | Protocole | Description |
|---|---|---|
| 5985 | HTTP | Port que l'agent User-ID utilise pour surveiller les journaux de sécurité et les informations de session avec le protocole WinRM sur HTTP. |
| 5986 | HTTPS | Port que l'agent User-ID utilise pour surveiller les journaux de sécurité et les informations de session avec le protocole WinRM sur HTTPS. |
| 5009 | TCP | Port que le pare-feu utilise pour se connecter à l'agent Terminal Services. |

## Ports utilisés pour IPSec

Le pare-feu et Panorama utilisent les ports suivants pour les fonctions IPSec.

| Port de destination | Protocole | Description |
|---|---|---|
| 500 | UDP | Port utilisé par IKE sur le plan de gestion pour se connecter aux homologues IKE distants. |
| 4500 | UDP | Port utilisé par IKE sur le plan de gestion pour se connecter aux homologues IKE distants. |
| 4510 | UDP | Port utilisé par le plan de données pour envoyer des requêtes à IKE. |
| 4511 | UDP | Port utilisé par le plan de données pour envoyer des requêtes à `keymgr`. |

## Ports utilisés pour le routage

Le pare-feu et Panorama utilisent les ports suivants pour les fonctions de routage.

| Port de destination | Protocole | Description |
|---|---|---|
| 179 | TCP | Port utilisé par BGP pour se connecter aux homologues. |
| 3784<br>3785<br>4784 | UDP | Ports utilisés par BGP pour se connecter aux homologues. |

| Port de destination | Protocole | Description |
|---|---|---|
| 520 | UDP | Port utilisé pour RIPv2. |
| 89 | Adresse IP | Port utilisé pour OSPF. |
| 103 | Adresse IP | Port utilisé pour la multidiffusion indépendante du protocole (PIM). |

## Ports utilisés pour DHCP

Le pare-feu et Panorama utilisent les ports suivants pour les fonctions DHCP.

| Port de destination | Protocole | Description |
|---|---|---|
| 67<br>68<br>546<br>547 | UDP | Ports utilisés comme ports d'écoute du serveur DHCP. |

## Ports utilisés pour l'infrastructure

Le pare-feu et Panorama utilisent les ports suivants pour les fonctions de gestion.

| Port de destination | Protocole | Description |
|---|---|---|
| 111 | TCP/UDP | Port utilisé comme mappeur de port. |
| 23 | TCP/UDP | Port utilisé pour le protocole d'application Telnet. |
| 69 | TCP/UDP | Port utilisé pour TFTP. |
| 2049 | TCP/UDP | Port utilisé pour le système de fichiers réseau (NFS). |
| 28260 | TCP | Port utilisé par la communication IPC sysd interne pour les processus internes. |
| 28261 | TCP | Port utilisé par les applications mastered (maitrisées) internes pour gérer les processus internes. |

# Rétablissement des paramètres d'usine du pare-feu

Le rétablissement des paramètres d'usine du pare-feu entraînera la perte de tous les journaux et paramètres de configuration.

**STEP 1 |** Configurez une connexion de console au pare-feu.

1. Connectez un câble série de votre ordinateur au port de console et connectez-vous au pare-feu à l'aide d'un logiciel d'émulation de terminal (9600-8-N-1).

   *Si votre ordinateur ne dispose d'aucun port série 9 broches, utilisez un connecteur de port USB/série.*

2. Saisissez vos informations d'identification de connexion.
3. Saisissez la commande CLI suivante :

   **debug system maintenance-mode**

   Le pare-feu redémarre en mode maintenance.

**STEP 2 |** Rétablissez les paramètres d'usine du système.

1. Lorsque le pare-feu redémarre, appuyez sur **Entrée** pour continuer vers le menu du mode maintenance.
2. Sélectionnez **Rétablir les paramètres d'usine** et appuyez sur **Entrée**.
3. Sélectionnez à nouveau **Rétablir les paramètres d'usine** et appuyez sur **Entrée**.

   Le pare-feu redémarre sans aucun paramètre de configuration. Le nom d'utilisateur et le mot de passe par défaut pour se connecter au pare-feu sont admin/admin.

   Pour effectuer la configuration initiale sur le pare-feu et configurer la connexion réseau, reportez-vous à la section Intégration du pare-feu dans votre réseau de gestion.

# Autoamorçage du pare-feu

L'autoamorçage accélère le processus de configuration et de mise sous licence du pare-feu afin que celui-ci soit fonctionnel sur le réseau avec ou sans accès Internet. L'autoamorçage vous permet de choisir de configurer le pare-feu à l'aide d'un fichier de configuration de base (init-cfg.txt) pour qu'il puisse se connecter à Panorama et obtenir la configuration complète ou d'installer la configuration de base sur le pare-feu en ajoutant le fichier facultatif bootstrap.xml.

- Prise en charge des lecteurs USB Flash
- Fichiers init-cfg.txt modèles
- Préparation d'un lecteur USB pour l'amorçage automatique d'un pare-feu
- Autoamorçage d'un pare-feu à l'aide d'une clé USB à mémoire flash

## Prise en charge des lecteurs USB Flash

Le lecteur USB Flash qui amorce un pare-feu matériel Palo Alto Networks doit prendre en charge un des formats suivants :

- File Allocation Table 32 (FAT32)
- Third Extended File System (ext3)

Le pare-feu peut amorcer à partir des lecteurs Flash suivants avec une connectivité USB2.0 ou USB3.0 :

| Lecteurs USB Flash pris en charge |
| --- |
| Kingston<br>• Kingston SE9 8 Go (2.0)<br>• Kingston SE9 16 Go (3.0)<br>• Kingston SE9 32 Go (3.0) |
| SanDisk<br>• SanDisk Cruzer Fit CZ33 8 Go (2.0)<br>• SanDisk Cruzer Fit CZ33 16 Go (2.0)<br>• SanDisk Cruzer CZ36 16 Go (2.0)<br>• SanDisk Cruzer CZ36 32 Go (2.0)<br>• SanDisk Cruzer CZ80 32 Go (3.0) |
| Silicon Power<br>• Silicon Power Jewel 32 Go (3.0)<br>• Silicon Power Blaze 16 Go (3.0) |
| PNY |

| Lecteurs USB Flash pris en charge |
| --- |
| • PNY Attache 16 Go (2.0)<br>• PNY Turbo 32 Go (3.0) |

## Fichiers init-cfg.txt modèles

Un fichier init-cfx.txt est nécessaire pour le processus d'autoamorçage ; ce fichier est un fichier de configuration de base que vous pouvez créer à l'aide d'un éditeur de texte. Pour créer ce fichier, consultez 5 Les exemples suivants de fichiers init-cfg.txt montrent tous les paramètres qui sont pris en charge dans le fichier ; les paramètres obligatoires sont en gras.

| Exemple de fichier init-cfg.txt (adresse IP fixe) | Exemple de fichier init-cfg.txt (client DHCP) |
| --- | --- |
| **type=static**<br>**ip-address=10.5.107.19**<br>**default-gateway=10.5.107.1**<br>**netmask=255.255.255.0**<br>**ipv6-address=2001:400:f00::1/64**<br>**ipv6-default-gateway=2001:400:f00::2**<br>hostname=Ca-FW-DC1<br>panorama-server=10.5.107.20<br>panorama-server-2=10.5.107.21<br>tplname=FINANCE_TG4<br>dgname=finance_dg<br>dns-primary=10.5.6.6<br>dns-secondary=10.5.6.7<br>op-command-modes=multi-vsys,jumbo-frame<br>dhcp-send-hostname=no<br>dhcp-send-client-id=no<br>dhcp-accept-server-hostname=no<br>dhcp-accept-server-domain=no | **type=dhcp-client**<br>ip-address=<br>default-gateway=<br>netmask=<br>ipv6-address=<br>ipv6-default-gateway=<br>hostname=Ca-FW-DC1<br>panorama-server=10.5.107.20<br>panorama-server-2=10.5.107.21<br>tplname=FINANCE_TG4<br>dgname=finance_dg<br>dns-primary=10.5.6.6<br>dns-secondary=10.5.6.7<br>op-command-modes=multi-vsys,jumbo-frame<br>dhcp-send-hostname=yes<br>dhcp-send-client-id=yes<br>dhcp-accept-server-hostname=yes<br>dhcp-accept-server-domain=yes |

Le tableau suivant décrit les champs dans le fichier init-cfg.txt. Le type doit être renseigné ; si le type est statique, l'adresse IP, la passerelle par défaut et le masque réseau doivent être renseignés ou l'adresse IPv6 et la passerelle IPv6 pas défaut doivent être renseignées.

| Champ | Description |
| --- | --- |
| type | (Obligatoire) Type d'adresse IP de gestion : statique ou client dhcp. |
| adresse-ip | (Obligatoire pour une adresse IPv4 de gestion statique) Adresse IPv4. Le pare-feu ignore ce champ si le type est défini sur client dhcp. |

| Champ | Description |
|---|---|
| default-gateway | (Obligatoire pour une adresse IPv4 de gestion statique) Passerelle IPv4 par défaut de l'interface de gestion. Le pare-feu ignore ce champ si le type est défini sur client dhcp. |
| netmask | (Obligatoire pour une adresse IPv4 de gestion statique) Masque réseau IPv4. Le pare-feu ignore ce champ si le type est défini sur client dhcp. |
| ipv6-address | (Obligatoire pour une adresse IPv6 de gestion statique) Adresse IPv6/Longueur de préfixe de l'interface de gestion. Le pare-feu ignore ce champ si le type est défini sur client dhcp. |
| ipv6-default-gateway | (Obligatoire pour une adresse IPv6 de gestion statique) Passerelle IPv6 par défaut de l'interface de gestion. Le pare-feu ignore ce champ si le type est défini sur client dhcp. |
| Nom d'hôte | (Facultatif) Nom d'hôte du pare-feu. |
| panorama-server | (Recommandé) Adresse IPv4 ou IPv6 du serveur Panorama principal. |
| panorama-server-2 | (Facultatif) Adresse IPv4 ou IPv6 du serveur Panorama secondaire. |
| tplname | (Recommandé) Nom du modèle Panorama. |
| DgName | (Recommandé) Nom du groupe de périphériques Panorama. |
| dns-primary | (Facultatif) Adresse IPv4 ou IPv6 du serveur DNS principal. |
| dns-secondary | (Facultatif) Adresse IPv4 ou IPv6 du serveur DNS secondaire. |
| vm-auth-key | (Pare-feu VM-Series uniquement) Clé d'authentification de la machine virtuelle. |
| op-command-modes | (Facultatif) Saisissez multi-vsys, jumbo-frame ou les deux séparés par une virgule uniquement. Autorise les systèmes virtuels multiples et les trames Jumbo lors de l'auto-amorçage. |
| dhcp-send-hostname | (Client DHCP uniquement) Le serveur DHCP détermine si la valeur est oui ou non. Si la valeur est oui, le pare-feu envoie son nom d'hôte au serveur DHCP. |
| dhcp-send-client-id | (Client DHCP uniquement) Le serveur DHCP détermine si la valeur est oui ou non. Si la valeur est oui, le pare-feu envoie son id client au serveur DHCP. |

| Champ | Description |
|---|---|
| dhcp-accept-server-hostname | (Client DHCP uniquement) Le serveur DHCP détermine si la valeur est oui ou non. Si la valeur est oui, le pare-feu accepte son nom d'hôte du serveur DHCP. |
| dhcp-accept-server-domain | (Client DHCP uniquement) Le serveur DHCP détermine si la valeur est oui ou non. Si la valeur est oui, le pare-feu accepte son serveur DNS du serveur DHCP. |

# Préparation d'un lecteur USB pour l'amorçage automatique d'un pare-feu

Vous pouvez utiliser un lecteur USB pour autoamorcer un pare-feu physique. Cependant, pour ce faire, vous devez utiliser PAN-OS 7.1, ou toute version ultérieure, et procéder au Rétablissement des paramètres d'usine du pare-feu. Pour des raisons de sécurité, vous ne pouvez autoamorcer un pare-feu que lorsqu'il se trouve à son état d'usine par défaut ou que lorsque l'ensemble de ses données privées ont été supprimées.

**STEP 1 |** Obtenez des numéros de série (S/N) et les codes d'autorisation pour les abonnements de support à partir de votre e-mail de traitement des commandes.

**STEP 2 |** Enregistrez les numéros de série des nouveaux pare-feu sur le portail du support client.

1. Accédez à support.paloaltonetworks.com, connectez-vous et sélectionnez **Assets (Ressources)** > **Devices (Périphériques)** > **Register New Device (Enregistrer un nouveau périphérique)** > **Register device using Serial Number or Authorization Code (Enregistrer l'appareil à l'aide du numéro de série ou du code d'autorisation)**.
2. Suivez les étapes pour Enregistrer le pare-feu.
3. Cliquez sur **Submit (Envoyer)**.

**STEP 3 |** Activez les codes d'autorisation sur le portail du Support client, qui crée les clés de licence.

1. Allez à support.paloaltonetworks.com, connectez-vous et sélectionnez **Assets (Ressources)** > **Devices (Périphériques)** sur le panneau de navigation de gauche.
2. Pour chaque numéro de série de périphérique que vous venez d'enregistrer, cliquez sur le lien **Action (Action)** (icône de crayon).
3. Sous Activate Licenses (Activer les licences), sélectionnez **Activate Auth-Code (Activer le code d'authentification)**.
4. Saisissez le **Authorization Code (code d'autorisation)**, cliquez sur **Agree (Accepter)** et **Submit (Envoyer)**.

**STEP 4 |** Ajoutez les numéros de série dans Panorama.

Terminez l'étape 1 dans Ajouter un pare-feu en tant que périphérique géré dans le Guide de l'administrateur Panorama.

**STEP 5 |** Création du fichier init-cfg.txt.

Créez le fichier init-cfg.txt, un fichier obligatoire qui fournit les paramètres d'autoamorçage. Les champs sont décrits à la section Fichiers init-cfg.txt modèles.

*Si le fichier init-cfg.txt est manquant, le processus d'amorçage échouera et le pare-feu démarrera avec la configuration par défaut dans la séquence de démarrage normale.*

Il n'y a pas d'espace entre la clé et la valeur dans chaque champ ; N'ajoutez pas d'espaces car ils provoquent des erreurs lors de l'analyse du serveur de gestion.

Vous pouvez disposer de plusieurs fichiers init-cfg.text, chacun se rapportant à un site distant différent, en ajoutant le numéro de série devant le nom de fichier. Par exemple :

0008C200105-init-cfg.txt

0008C200107-init-cfg.txt

Si aucun nom de fichier ajouté au début n'est présent, le pare-feu utilise le fichier init-cfg.txt et procède à l'amorçage.

**STEP 6 |** (Facultatif) Création du fichier bootstrap.xml.

Le fichier bootstrap.xml facultatif est une configuration de pare-feu complète que vous pouvez exporter à partir d'un pare-feu de production existant.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)** > **Export named configuration snapshot (Exporter l'instantané de configuration nommé)**.
2. Sélectionnez le **Name (nom)** de la configuration enregistrée ou en cours d'exécution.
3. Cliquez sur **OK**.
4. Renommez le fichier **`bootstrap.xml`**.

**STEP 7 |** Créez et téléchargez le kit d'amorçage à partir du portail du support client.

Pour un pare-feu physique, le kit d'amorçage requiert uniquement les répertoires /license et /config.

Utilisez l'une des méthodes suivantes pour créer et télécharger le kit d'amorçage :

- Utilisez la **Méthode 1** pour créer un kit d'amorçage spécifique à un site distant (vous n'avez qu'un seul fichier init-cfg.txt).
- Utilisez la **Méthode 2** pour créer un kit d'amorçage pour plusieurs sites.

**Méthode 1**

1. Sur votre système local, accédez à support.paloaltonetworks.com et connectez-vous.
2. Sélectionnez **Assets (ressources)**.
3. Sélectionnez le numéro de série du pare-feu que vous voulez amorcer.
4. Sélectionnez **Bootstrap Container (Conteneur d'amorçage)**.
5. Cliquez **Select (Sélectionnez)**.
6. Téléchargez et **Open (Ouvrez)** le fichier init-cfg.txt que vous avez créé.
7. (Facultatif) Sélectionnez le fichier bootstrap.xml que vous avez créé et **Upload Files (Télécharger des fichiers**.

   *Vous devez utiliser un fichier bootstrap.xml provenant d'un pare-feu du même modèle et de la même version PAN-OS.*
8. Sélectionnez **Bootstrap Container Download (Télécharger le conteneur d'autoamorçage)** pour télécharger un fichier tar.gz nommé **`bootstrap_<S/N>_<date>.tar.gz`** vers votre système local. Ce conteneur d'autoamorçage contient les clés de licence associées au numéro de série du pare-feu.

**Méthode 2**

Créez un fichier tar.gz sur votre système local, lequel doit contenir deux répertoires de premier niveau : /license et /config. Ajoutez toutes les licences et fichiers init-cfg.txt auxquels le numéro de série a été ajouté aux noms de fichier.

Les fichiers de clé de licence que vous téléchargez du portail de support client comportent le numéro de série dans le nom de fichier de la licence. PAN-OS vérifie que le numéro de série qui figure dans le nom de fichier correspond au numéro de série du pare-feu tout en exécutant le processus d'autoamorçage.

**STEP 8 |** Importez le fichier tar.gz que vous avez créé (vers un pare-feu utilisant PAN-OS 7.1 ou toute version ultérieure) en utilisant Secure Copy (copie sécurisée ; SCP) ou TFTP.

Accédez à la CLI et entrez l'une des commandes suivantes :

- **tftp import bootstrap-bundle file <path and filename> from <host IP address>**

  Par exemple :

  **tftp import bootstrap-bundle file /home/userx/bootstrap/devices/pa5000.tar.gz from 10.1.2.3**

- **scp import bootstrap-bundle from <<user>@<host>:<path to file>>**

  Par exemple :

  **scp import bootstrap-bundle from userx@10.1.2.3:/home/userx/bootstrap/devices/pa200_bootstrap_bundle.tar.gz**

**STEP 9 |** Préparez le lecteur flash USB.

1. Insérez le lecteur flash USB dans le pare-feu que vous avez utilisé à l'étape précédente.
2. Saisissez la commande opérationnelle CLI suivante, en utilisant le nom de votre fichier tar.gz à la place de « **pa5000.tar.gz** ». Cette commande formate la clé USB, décompresse le fichier et valide la clé USB :

   **request system bootstrap-usb prepare from pa5000.tar.gz**
3. Appuyez sur **y** pour continuer. Le message suivant s'affiche lorsque la clé USB est prête :

   ```
   USB prepare completed successfully. (Préparation USB terminée avec succès.)
   ```
4. Retirez le lecteur flash USB du pare-feu.
5. Vous pouvez préparer autant de lecteurs flash USB que nécessaire.

**STEP 10 |** Livrez le lecteur flash USB à votre site distant.

Si vous avez utilisé la méthode 2 pour créer le module d'autoamorçage, vous pouvez utiliser le contenu de la même clé USB pour autoamorcer les pare-feu sur de multiples sites distants. Vous pouvez traduire le contenu en de multiples clés USB ou en une seule clé USB utilisée de multiples fois.

## Autoamorçage d'un pare-feu à l'aide d'une clé USB à mémoire flash

Après avoir reçu un nouveau pare-feu Palo Alto Networks et une clé USB chargée de fichiers d'autoamorçage, vous pouvez autoamorcer le pare-feu.

*Les systèmes d'exploitation Microsoft Windows et Apple Mac ne sont pas capables de lire la clé USB parce qu'elle est formatée à l'aide d'un système de fichiers ext4. Vous devez installer un logiciel tiers ou utiliser le système Linux pour lire la clé USB.*

**STEP 1 |** Le pare-feu doit se trouver à son état d'usine par défaut ou que lorsque l'ensemble de ses données privées ont été supprimées.

**STEP 2 |** Pour garantir la connectivité de vos sièges sociaux, câblez le pare-feu en connectant l'interface de gestion (MGT) à l'aide d'un câble Ethernet à l'un ou l'autre des éléments suivants :

- Un modem en amont
- Un port sur le commutateur ou sur le routeur
- Une prise Ethernet dans le mur

**STEP 3 |** Insérez la clé USB dans le port USB du pare-feu et allumez le pare-feu. Le pare-feu ayant les paramètres d'usine par défaut s'autoamorce à partir de la clé USB.

Le témoin d'état du pare-feu passe du jaune au vert lorsque le pare-feu est configuré ; l'autovalidation a réussi.

**STEP 4 |** Vérifiez que l'autoamorçage est terminé. Vous pouvez voir les journaux d'état de base sur la console durant l'amorçage et vous pouvez vérifier que l'opération est terminée.

1. Si vous avez inclus les valeurs de Panorama (panorama-server, tplname et dgname) dans votre fichier init-cfg.txt, vérifiez les périphériques gérés, les groupes de périphériques et le nom de modèle Panorama.
2. Vérifiez la configuration et les paramètres système généraux en accédant à l'interface Web et en sélectionnant **Dashboard (Tableau de bord)** > **Widgets (Widgets)** > **System (Système)** ou en utilisant les commandes opérationnelles de la CLI **`show system info`** et **`show config running`**.
3. Vérifiez l'installation de la licence en sélectionnant **Device (Périphérique)** > **Licenses (Licences)** ou en utilisant la commande opérationnelle de la CLI **`request license info`**.
4. Si Panorama est configuré, gérez les versions de contenu et les versions de logiciel depuis Panorama. Si Panorama n'est pas configuré, utilisez l'interface Web pour gérer les versions de contenu et les versions de logiciel.

# Télémétrie du périphérique

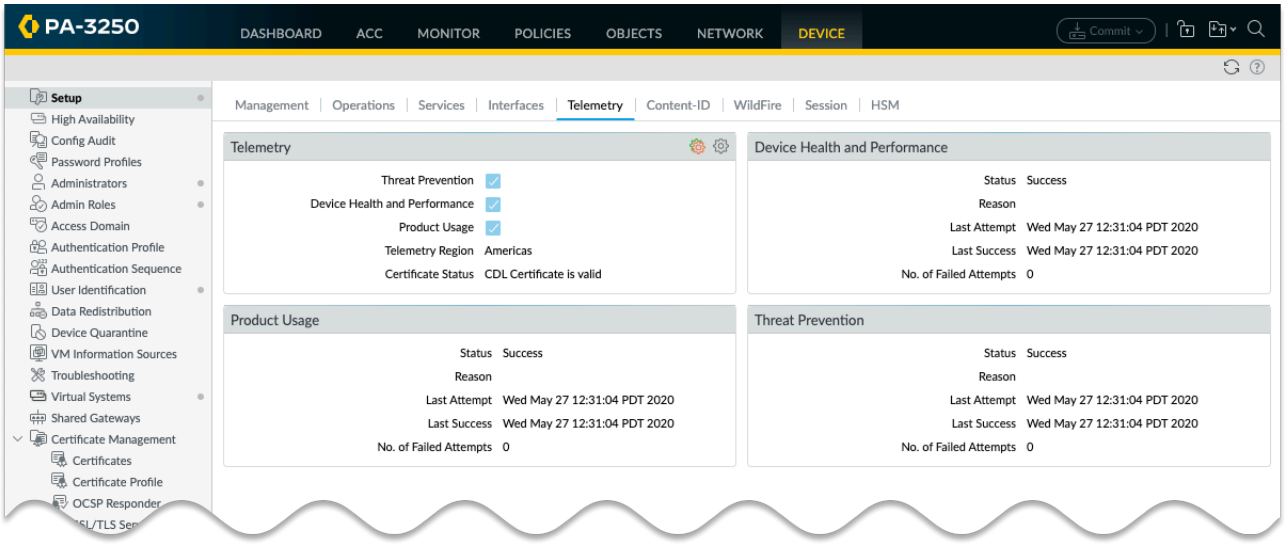
La télémétrie du périphérique recueille des données sur votre pare-feu nouvelle génération ou Panorama, et les partage avec Palo Alto Networks en les chargeant dans le lac de données Cortex. Ces données sont utilisées pour alimenter des applications de télémétrie et pour partager des renseignements sur les menaces.



# Présentation de la télémétrie du périphérique

La télémétrie du périphérique recueille des données sur votre pare-feu nouvelle génération ou Panorama, et les partage avec Palo Alto Networks en les chargeant dans le lac de données Cortex. Ces données sont utilisées pour alimenter les applications de télémétrie, qui sont des applications basées sur le cloud qui facilitent la surveillance et la gestion de vos pare-feu nouvelle génération et Panoramas. Ces applications améliorent votre visibilité sur la santé, les performances, la planification des capacités et la configuration des périphériques. Grâce à ces applications, vous pouvez maximiser les avantages que vous tirez des produits et services fournis par Palo Alto Networks.

Les données télémétriques sont également utilisées pour le partage des renseignements sur les menaces, ce qui permet d'améliorer la prévention des intrusions, l'évaluation des signatures de menaces, ainsi que la détection des logiciels malveillants grâce au filtrage des URL PAN-DB, aux signatures de commande et de contrôle (C2) basées sur le DNS et à WildFire.




Les données télémétriques sont collectées et stockées localement sur votre périphérique pendant une période limitée. Ces données ne sont partagées avec Palo Alto Networks que si vous configurez une région de destination pour les données. Si votre organisation possède une licence de lac de données Cortex, vous ne pouvez envoyer les données que dans la même région que celle où réside votre instance de lac de données Cortex. Si votre organisation ne dispose pas d'une licence de lac de données Cortex, vous devez installer un certificat de périphérique afin de partager ces données. Dans ce cas, vous pouvez choisir n'importe quelle région disponible, mais vous devez vous conformer à toutes les lois locales applicables en matière de vie privée et de stockage des données.

Les données télémétriques sont collectées et partagées avec Palo Alto Networks selon des intervalles de collecte prédéfinis. Vous pouvez contrôler si les données sont collectées et partagées en activant/désactivant des catégories de données. Vous pouvez également surveiller l'état actuel de la collecte et de la transmission des données.

Enfin, vous pouvez obtenir un échantillon en direct des données que votre pare-feu collecte à des fins de télémétrie. Pour une description complète de toutes les mesures de télémétrie qui peuvent être partagées avec Palo Alto Networks, y compris les implications en matière de confidentialité pour chaque mesure, consultez le Guide de référence des mesures de télémétrie du périphérique PAN-OS.

# Intervalles de collecte et de transmission de télémétrie du périphérique

PAN-OS collecte et envoie des données de télémétrie à intervalles fixes. La collecte est définie sur une base métrique par métrique, et peut être l'une des suivantes :

- Toutes les 20 minutes
- Toutes les 4 heures.
- Une fois par semaine.

La télémétrie est collectée en lots de données. Chaque lot est une agrégation de toutes les données collectées jusqu'au moment de la transmission des données. Ces paquets sont stockés sur le périphérique jusqu'à un événement de transmission, qui se produit une fois toutes les 4 heures. Lorsqu'un lot a été envoyé avec succès à Palo Alto Networks, il est supprimé du périphérique.

Si une erreur se produit lors de l'envoi d'un lot à Palo Alto Networks, le pare-feu attend 10 minutes puis réessaye. Le pare-feu continuera à essayer d'envoyer le lot jusqu'à ce qu'il réussisse ou qu'il ait besoin de l'espace de stockage nécessaire pour collecter de nouvelles données télémétriques.

À chaque intervalle de transmission régulier, le pare-feu commence par envoyer les lots prévus pour cet événement. Après un transfert réussi de ces lots, le pare-feu envoie tous les lots défectueux qu'il a pu stocker lors des transmissions précédentes.

# Gestion de la télémétrie du périphérique

Pour gérer la télémétrie du périphérique, vous pouvez effectuer les actions suivantes :

- Activation de la télémétrie du périphérique
- Désactivation de la télémétrie du périphérique
- Gestion des données que la télémétrie du périphérique collecte
- Gestion de l'historique de la télémétrie du périphérique

## Activation de la télémétrie du périphérique

Par défaut, votre périphérique ne partage pas les données avec Palo Alto Networks. Si le partage est activé, vous pouvez arrêter le partage de toute télémétrie du périphérique comme suit : **Device (Périphérique)** > **Setup (Configuration)** > **Telemetry (Télémétrie)**, décochez la case **Enable Telemetry (Activer la télémétrie)**, puis validez votre modification.

Pour activer la télémétrie du périphérique afin que les données soient partagées avec Palo Alto Networks :

**STEP 1 |** Activez le lac de données Cortex.

1. Si votre organisation ne dispose pas d'une licence de lac de données Cortex, installez un certificat de périphérique si celui-ci n'est pas déjà installé sur votre périphérique.

   Si votre organisation possède une licence de lac de données Cortex, assurez-vous qu'elle est activée.
2. Assurez-vous que votre réseau est correctement configuré pour que le pare-feu puisse envoyer des données au lac de données Cortex.

**STEP 2 |** Accédez à **Device (Périphérique)** > **Setup (Configuration)** > **Telemetry (Télémétrie)**

**STEP 3 |** Modifiez le widget **Telemetry (Télémétrie)**.

**STEP 4 |** Dans **Telemetry Destination (Destination de télémétrie)**, sélectionnez votre région. Si votre organisation utilise le lac de données Cortex, vous devez utiliser la région pour laquelle votre lac de données Cortex est configuré.

**STEP 5 |** Cliquez sur **OK**, puis validez vos modifications.

## Désactivation de la télémétrie du périphérique

Si votre pare-feu nouvelle génération est configuré pour partager des données avec Palo Alto Networks, vous pouvez désactiver ce partage comme suit :

**STEP 1 |** Accédez à **Device (Périphérique)** > **Setup (Configuration)** > **Telemetry (Télémétrie)**

**STEP 2 |** Modifiez le widget **Telemetry (Télémétrie)**.

**STEP 3 |** Décochez la case **Enable Telemetry (Activer la télémétrie)**.

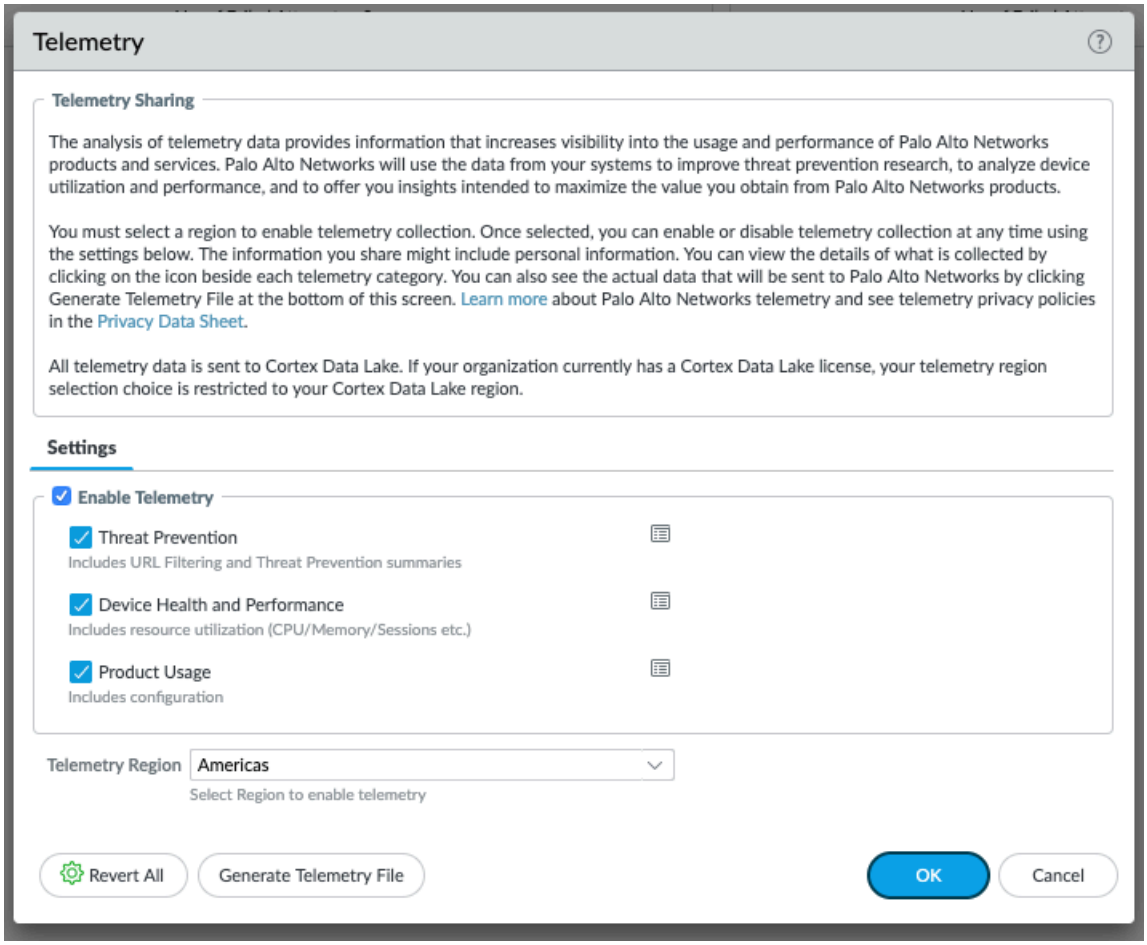
**STEP 4 |** Cliquez sur **OK**, puis validez vos modifications.

**STEP 5 |** Toutes les données télémétriques actuellement stockées dans le lac de données Cortex sont automatiquement purgées un an après que votre pare-feu les ait chargées. En option, si vous ne souhaitez pas que les données résident dans le lac de données Cortex pendant cette période après avoir désactivé la télémétrie, ouvrez un ticket de support et demandez à Palo Alto Networks de purger vos données de télémétrie.

## Gestion des données que la télémétrie du périphérique collecte

Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Telemetry (Télémétrie)** pour voir les catégories de télémétrie actuellement collectées. Pour changer ces catégories, éditez le widget Télémétrie. Désélectionnez les catégories que vous ne voulez pas que le pare-feu collecte, **OK**, puis validez la modification.




*Pour cesser de partager toute la télémétrie du périphérique, décochez la case **Enable Telemetry (Activer la télémétrie)**, puis validez votre modification.*

## Gestion de l'historique de la télémétrie du périphérique

La télémétrie du périphérique a considérablement changé pour la version PAN-OS 10.1. Avant la version 10.0, les données télémétriques étaient surtout intéressantes à des fins de renseignement sur les menaces. À partir de 10.0, les mesures de renseignements sur les menaces représentent toujours une grande partie des données recueillies par le périphérique, mais beaucoup plus de

données concernant la santé, les performances et la configuration du périphérique sont également recueillies.

En d'autres termes, la télémétrie du périphérique de PAN-OS 10.1 étend les données qui ont été collectées pour les versions précédentes. PAN-OS 10.1 envoie également les données de télémétrie vers un emplacement du cloud différent de celui des versions précédentes. Mais la prise en charge de la télémétrie historique existe toujours pour les pare-feux nouvelle génération fonctionnant sous PAN-OS 10.0. La seule différence est que l'interface utilisateur de télémétrie du périphérique 10.1 n'est pas capable de gérer cette collecte de données historiques.

Si vous disposez d'un pare-feu nouvelle génération et que vous avez activé l'une des catégories de données télémétriques historiques, votre pare-feu continuera à collecter et à partager ces informations lorsque vous passerez à PAN-OS 10.1. Si vous souhaitez désactiver ce partage de données télémétriques, utilisez les commandes CLI suivantes :

```
set deviceconfig system update-schedule statistics-service
 application-reports no
set deviceconfig system update-schedule statistics-service threat-
prevention-reports no
set deviceconfig system update-schedule statistics-service threat-
prevention-information no
set deviceconfig system update-schedule statistics-service threat-
prevention-pcap no
set deviceconfig system update-schedule statistics-service passive-
dns-monitoring no
set deviceconfig system update-schedule statistics-service url-
reports no
set deviceconfig system update-schedule statistics-service health-
performance-reports no
set deviceconfig system update-schedule statistics-service file-
identification-reports no
```

Si vous avez un pare-feu 10.1 et que ce partage de télémétrie est désactivé, mais que vous voulez partager ces données avec Palo Alto Networks, alors vous pouvez l'activer en utilisant :

```
set deviceconfig system update-schedule statistics-service
 application-reports yes
set deviceconfig system update-schedule statistics-service threat-
prevention-reports yes
set deviceconfig system update-schedule statistics-service threat-
prevention-information yes
set deviceconfig system update-schedule statistics-service threat-
prevention-pcap yes
set deviceconfig system update-schedule statistics-service passive-
dns-monitoring yes
set deviceconfig system update-schedule statistics-service url-
reports yes
set deviceconfig system update-schedule statistics-service health-
performance-reports yes
set deviceconfig system update-schedule statistics-service file-
identification-reports yes
```

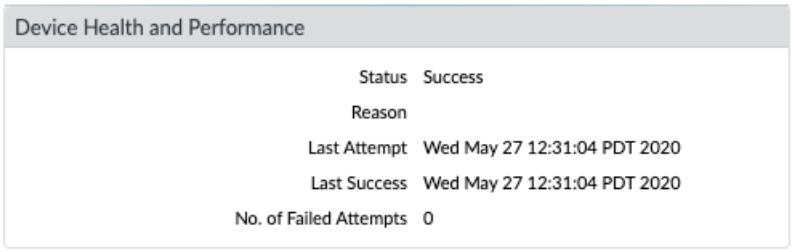
Vous pouvez voir si votre périphérique collecte et partage ces données télémétriques historiques en utilisant la commande CLI suivante :

```
show deviceconfig system update-schedule statistics-service
```

# Surveillance de la télémétrie du périphérique

PAN-OS vous montre l'état de partage pour chaque catégorie de télémétrie. Les widgets pour chaque catégorie de mesure sont disponibles sous **Device (Périphérique)** > **Setup (Configuration)** > **Telemetry (Télémétrie)**.



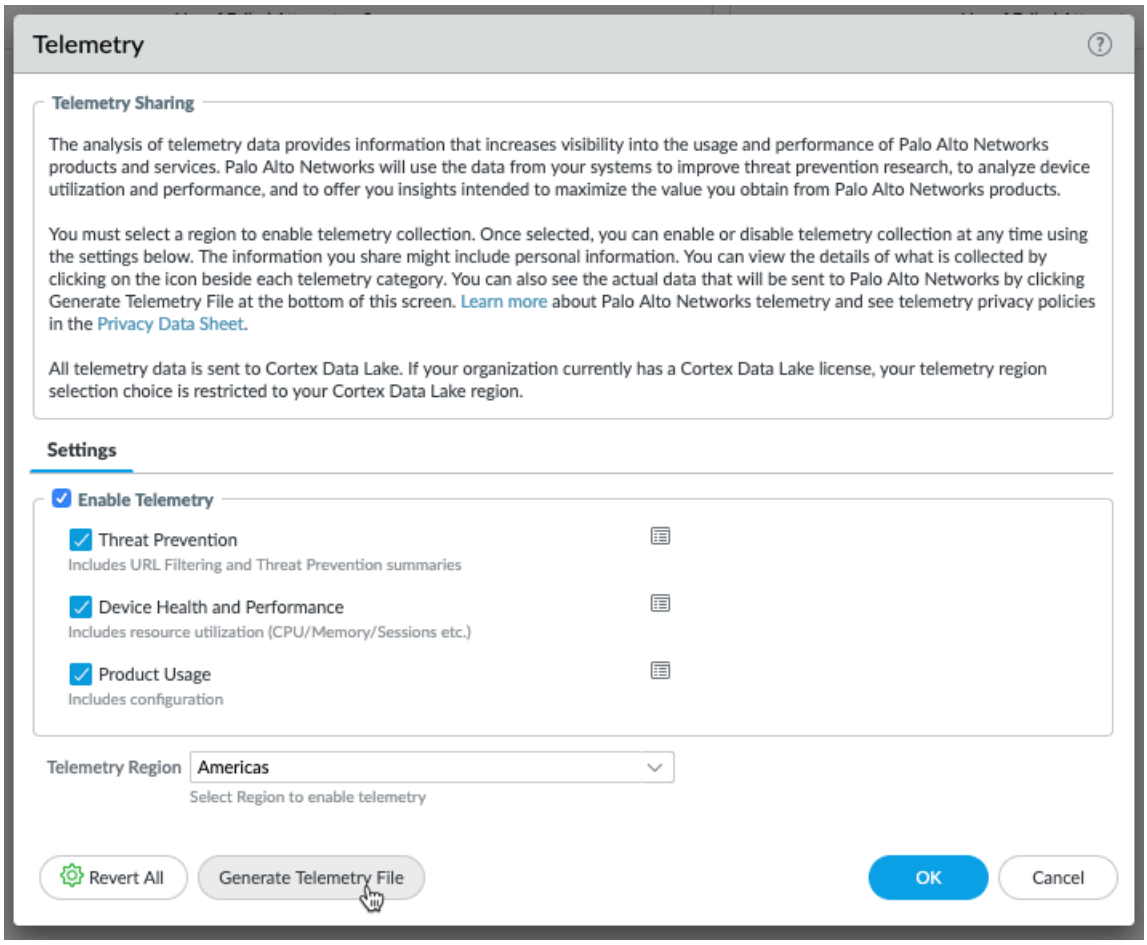

En cas d'échec, votre périphérique tentera à nouveau l'envoi à l'heure de transmission suivante. Si le problème persiste, vérifiez que vos périphériques sont correctement configurés pour envoyer des données au lac de données Cortex :

- Si votre organisation possède une licence de lac de données Cortex, assurez-vous que votre licence de lac de données Cortex a été activée et que votre pare-feu est configuré pour utiliser le lac de données Cortex.
- Si votre organisation ne dispose pas d'une licence de lac de données Cortex, assurez-vous que vous avez installé un certificat de périphérique et que votre réseau est configuré pour autoriser le trafic vers le lac de données Cortex.

# Exemple de données que la télémétrie du périphérique collecte

Vous pouvez télécharger un exemple en direct des données que la télémétrie du périphérique collecte et partage avec Palo Alto Networks. Pour ce faire, accéder à **Device (Périphérique)** > **Setup (Configuration)** > **Telemetry (Télémétrie)** et modifiez le widget **Telemetry (Télémétrie)**. Cliquez ensuite sur **Generate Telemetry File (Générer le fichier de télémétrie)**.




La collecte des données prendra quelques minutes, en fonction de la vitesse de votre pare-feu. Lorsque le processus est terminé, cliquez sur **Download Device Telemetry Data (Télécharger les données de télémétrie du périphérique)**. Le lot de télémétrie est une archive tar compressée, et elle est placée dans le répertoire de téléchargement par défaut de votre navigateur.

Pour une description de chaque mesure que la télémétrie du périphérique collecte et partage avec Palo Alto Networks, consultez le Guide de référence des mesures de télémétrie du périphérique PAN-OS.

# Authentification

L'authentification est une méthode de protection des services et des applications par la vérification de l'identité des utilisateurs afin de s'assurer que seuls les utilisateurs légitimes ont accès. Plusieurs fonctions du pare-feu et de Panorama exigent une authentification. Les administrateurs s'authentifient pour accéder à l'interface Web, à la CLI ou à l'API XML du pare-feu et de Panorama. Les utilisateurs finaux s'authentifient via le portail d'authentification ou GlobalProtect pour accéder aux divers services et applications. Un éventail de services d'authentification s'offrent à vous pour protéger votre réseau et pour supporter votre infrastructure réseau existante tout en garantissant une expérience utilisateur harmonieuse.

Si vous disposez d'une infrastructure à clés publiques, vous pouvez déployer des certificats pour activer l'authentification sans que les utilisateurs aient à répondre manuellement aux demandes de connexion (reportez-vous à la section Gestion des certificats). En plus des certificats, vous pouvez éventuellement mettre en œuvre une authentification interactive, qui force les utilisateurs à s'authentifier au moyen d'au moins une méthode. Les rubriques suivantes décrivent comment mettre en œuvre, tester et dépanner les divers types d'authentification interactive :

# Types d'authentification

- Services d'authentification externes
- Authentification multifacteur
- SAML
- Kerberos
- TACACS+
- RADIUS
- LDAP
- Authentification locale

## Services d'authentification externes

Le pare-feu et Panorama peuvent se servir de serveurs externes pour contrôler l'accès administratif à l'interface Web et l'accès des utilisateurs finaux aux services et aux applications via le portail d'authentification et GlobalProtect. Dans ce contexte, tout service d'authentification qui ne se trouve pas localement sur le pare-feu ou sur Panorama est considéré externe, peu importe si le serveur est interne (comme c'est le cas de Kerberos) ou externe (comme c'est le cas d'un fournisseur d'identités SAML) à votre réseau. Voici certains types de serveurs auxquels le pare-feu et Panorama peuvent s'intégrer : authentification multifactorielle, SAML, Kerberos, TACACS+, RADIUS et LDAP. Bien qu'il soit également possible d'utiliser les services d'authentification locale que le pare-feu et Panorama prennent en charge, il convient généralement de privilégier les services externes, car ils offrent :

- une gestion centralisée de tous les comptes utilisateur dans un annuaire d'identités externe. Tous les services externes pris en charge offrent cette option pour les utilisateurs finaux et les administrateurs.
- une gestion centralisée de l'autorisation des comptes (affectation des rôles et des domaines d'accès). SAML, TACACS+ et RADIUS prennent en charge cette option pour les administrateurs.
- la Single sign-on (ouverture de session unique ; SSO), qui permet aux utilisateurs de s'authentifier une seule fois pour accéder aux services et aux applications. SAML et Kerberos prennent en charge la SSO.
- plusieurs demandes d'authentification de divers types (facteurs) pour protéger vos services et applications les plus sensibles. Les services MFA prennent en charge cette option.

L'authentification via un serveur externe exige la présence d'un profil de serveur qui définit comment le pare-feu se connecte au service. Vous affectez le profil de serveur aux profils d'authentification, qui définissent les paramètres que vous personnalisez pour chaque application et ensemble d'utilisateurs. Par exemple, vous pouvez configurer un profil d'authentification pour les administrateurs qui accèdent à l'interface Web et un autre profil pour les utilisateurs finaux qui accèdent à un portail GlobalProtect. Pour plus d'informations, consultez la section Configuration d'un profil et d'une séquence d'authentification.

## Authentification multifacteur

Vous pouvez configurer l'authentification multifacteur (MFA) pour vous assurer que chaque utilisateur puisse d'identifier à l'aide de plusieurs méthodes (facteurs) lors de l'accès à des services

et applications hautement sensibles. Par exemple, vous pouvez forcer les utilisateurs à entrer un mot de passe de connexion, puis entrer un code de vérification qu'ils reçoivent par téléphone avant de permettre l'accès à des documents financiers importants. Cette approche permet d'empêcher les pirates d'accéder à tous les services et applications de votre réseau en usurpant des mots de passe. Bien sûr, tous les services et applications ne requièrent pas le même degré de protection, et le MFA n'est peut-être pas nécessaire pour les services et applications moins sensibles auxquels les utilisateurs accèdent fréquemment. Pour répondre à une variété de besoins de sécurité, vous pouvez configurer les règles de stratégie d'authentification qui déclenchent MFA ou un seul facteur d'authentification (tels que les informations de connexion ou les certificats) en fonction de services, applications et utilisateurs finaux spécifiques.

Lors du choix du nombre et du type de facteurs d'authentification à appliquer, il est important de comprendre comment l'évaluation des stratégies affecte l'expérience de l'utilisateur. Lorsqu'un utilisateur demande un service ou une application, le pare-feu évalue d'abord la stratégie d'authentification. Si la demande correspond à une règle de stratégie d'authentification avec MFA activée, le pare-feu affiche un formulaire Web de portail d'authentification afin que les utilisateurs puissent s'authentifier pour le premier facteur. En cas de réussite, le pare-feu affiche ensuite une page de connexion MFA pour chaque facteur additionnel. Certains services AMF invitent l'utilisateur à choisir un facteur sur deux à quatre, ce qui est utile lorsque certains facteurs ne sont pas disponibles. Si l'authentification réussit pour tous les facteurs, le pare-feu évalue la stratégie de sécurité pour le service ou l'application demandé.

***Pour réduire la fréquence des problèmes d'authentification qui interrompent le flux de travail utilisateur, configurez le premier facteur pour utiliser l'authentification unique (SSO) de Kerberos ou SAML.***

***Pour implémenter la MFA pour GlobalProtect, reportez-vous à la section configurer GlobalProtect pour faciliter des notifications de l'authentification multifactorielle.***

***Vous ne pouvez utiliser profils d'authentification MFA dans les séquences d'authentification.***

Pour l'authentification de l'utilisateur final via la politique d'authentification, le pare-feu s'intègre directement à plusieurs plateformes MFA (Duo v2, Okta Adaptive, PingID et RSA SecurID), et s'intègre via RADIUS ou SAML pour toutes les autres plateformes MFA. Pour l'authentification des utilisateurs distants sur les portails et les passerelles GlobalProtect et pour l'authentification de l'administrateur sur l'interface Web Panorama et PAN-OS, le pare-feu s'intègre aux fournisseurs MFA en utilisant seulement RADIUS et SAML.

Le pare-feu prend en charge les facteurs MFA suivants :

| Facteur | Description |
|---|---|
| Pousser (Push) | Un périphérique terminal (tel qu'un téléphone ou une tablette) invite l'utilisateur à autoriser ou à refuser l'authentification. |
| Short Message Service (service de | Un message SMS sur le périphérique d'extrémité invite l'utilisateur à autoriser ou à refuser l'authentification. Dans certains cas, le |

| Facteur | Description |
| --- | --- |
| messages courts ; SMS) | périphérique de point de terminaison fournit un code que l'utilisateur doit entrer dans la page de connexion MFA. |
| Voix | Un appel téléphonique automatisé invite l'utilisateur à s'authentifier en appuyant sur une touche du téléphone ou en entrant un code dans la page de connexion MFA. |
| One-Time Password (mot de passe à usage unique ; OTP) | Un dispositif terminal fournit une chaîne alphanumérique générée automatiquement, que l'utilisateur saisit dans la page de connexion MFA pour activer l'authentification pour une seule transaction ou session. |

## SAML

Vous pouvez utiliser SAML 2.0 (Security Assertion Markup Language) pour authentifier les administrateurs qui accèdent au pare-feu ou à l'interface Web Panorama et aux utilisateurs finaux qui accèdent aux applications web externes ou internes à votre organisation. Dans des environnements où chaque utilisateur accède à de nombreuses applications et où l'authentification au coup par coup pourrait être un frein à sa productivité, vous pouvez configurer une ouverture de session unique (SSO) en SAML pour autoriser l'accès à plusieurs applications après avoir ouvert une session. Dans le même ordre idée, le service de déconnexion unique (SLO) en SAML permet de fermer une session accédant à plusieurs applications en se déconnectant d'une seule session. Le SSO est accessible aux administrateurs ayant accès à l'interface web et aux utilisateurs ayant accès aux applications via GlobalProtect ou le portail d'authentification. Le SLO est accessible aux administrateurs et aux utilisateurs finaux de GlobalProtect, mais pas aux utilisateurs finaux du portail d'authentification. Quand vous configurez une authentification SAML dans le pare-feu ou dans Panorama, vous pouvez définir les attributs SAML des autorisations administrateur. Les attributs SAML vous permettent de changer les rôles rapidement, d'accéder aux domaines et aux groupes d'utilisateurs à travers votre service annuaire au lieu de reconfigurer les réglages dans le pare-feu ou dans Panorama.

***Les administrateurs ne peuvent pas utiliser SAML pour s'authentifier à la CLI sur le pare-feu ou sur Panorama.***

***Vous ne pouvez pas utiliser les profils d'authentification SAML pour des séquences d'authentification.***

Une authentification SAML nécessite un ***fournisseur de services*** (le pare-feu ou Panorama) qui contrôle l'accès aux applications, et un ***fournisseur d'identité*** (IdP), qui authentifie les utilisateurs. Quand un utilisateur nécessite un service ou une application, le pare-feu ou Panorama intercepte la requête et redirige l'utilisateur vers l'IdP pour authentification. L'IdP procède à l'authentification de l'utilisateur et renvoie une ***assertion SAML*** indiquant si l'authentification a réussi ou échoué. L'authentification SAML pour les utilisateurs finaux du portail d'authentification illustre l'authentification SAML pour un utilisateur final accédant aux applications via le portail d'authentification.

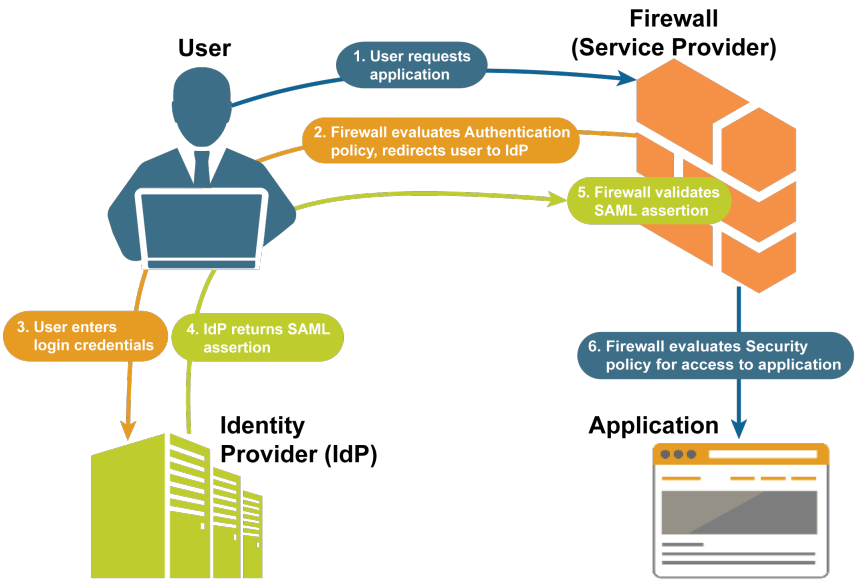



**Figure 1: Authentification SAML pour les utilisateurs finaux du portail d'authentification**

## Kerberos

Kerberos est un protocole d'authentification qui permet un échange sécurisé d'informations entre les parties sur un réseau non sécurisé en utilisant des clés uniques (appelées tickets) pour identifier les parties. Le pare-feu et Panorama prennent en charge deux types d'authentification Kerberos pour les administrateurs et les utilisateurs finaux :

- **Authentification du serveur Kerberos**Un profil de serveur Kerberos permet aux utilisateurs de s'authentifier de façon native auprès du contrôleur de domaine Active Directory ou d'un serveur d'authentification compatible avec Kerberos V5. Cette méthode d'authentification est interactive ; les utilisateurs doivent entrer leurs noms d'utilisateur et leurs mots de passe. Pour les étapes de configuration, reportez-vous à la section Configurer Authentification du serveur Kerberos.
- **Authentification unique Kerberos (SSO)**Un réseau prenant en charge SSO Kerberos va inviter un utilisateur à se connecter uniquement pour un premier accès au réseau (par exemple, une connexion à Microsoft Windows). Ensuite, l'utilisateur pourra accéder à tout service basé sur un navigateur dans le réseau (par exemple, l'interface Web du pare-feu) sans avoir à se reconnecter et jusqu'à l'expiration de la session SSO. (la durée des sessions SSO étant définie par votre administrateur Kerberos). Si vous activez Kerberos SSO et un autre service d'authentification externe (tel qu'un serveur TACACS +), le pare-feu essaie d'abord l'authentification unique et uniquement en cas d'échec, revient vers le service externe pour authentification. Pour prendre en charge SSO Kerberos, votre réseau doit contenir les éléments suivants :
  - Une infrastructure Kerberos, notamment un Key Distribution Center (centre de distribution de clé ; KDC) avec un Authentication Server (serveur d'authentification ; AS) et un Ticket-Granting Service (service d'émission de tickets ; TGS).
  - Un compte Kerberos pour le pare-feu ou Panorama qui permettra d'authentifier les utilisateurs. Un compte permet de créer un keytab Kerberos qui est un fichier contenant le nom principal

et le mot de passe haché du pare-feu ou de Panorama. Un keytab est indispensable au processus SSO.

Pour les étapes de configuration, reportez-vous à la section Configurer l'authentification unique de Kerberos.

***Kerberos SSO est disponible uniquement pour les services et les applications internes à votre environnement Kerberos. Pour activer l'authentification unique pour les services et applications externes, utilisez*** SAML.

## TACACS+

Terminal Access Controller Access-Control System Plus (TACACS+) est une famille de protocoles permettant une authentification et une autorisation à partir d'un serveur centralisé. TACACS+ crypte les noms d'utilisateurs et mots de passe, assurant ainsi une meilleure sécurité que RADIUS, qui crypte uniquement les mots de passe. TACACS+ est aussi plus fiable car il utilise le protocole TCP, alors que RADIUS utilise le protocole UDP. Vous pouvez configurer l'authentification TACACS + pour les utilisateurs finaux ou les administrateurs dans le pare-feu et pour les administrateurs dans Panorama. Vous pouvez également utilisez les VSA de TACACS+ pour gérer les autorisations administrateur. Les VSA de TACACS+ vous permettent de changer les rôles rapidement, d'accéder aux domaines et aux groupes d'utilisateurs à travers votre service annuaire au lieu de configurer à nouveau les réglages dans le pare-feu ou dans Panorama.

Le pare-feu et Panorama sont compatibles avec les VSA de TACACS+ suivants. Reportez-vous à la documentation de votre serveur TACACS+ pour les étapes à suivre pour définir ces VSA sur le serveur TACACS+.

| Name (Nom) | Valeur |
|---|---|
| service | Cet attribut est requis pour identifier le VSA comme spécifique à Palo Alto Networks. Vous devez définir la valeur sur **`PaloAlto`**. |
| protocol | Cet attribut est requis pour identifier le VSA comme spécifique aux périphériques Palo Alto Networks. Vous devez définir la valeur sur **`firewall`**. |
| PaloAlto-Admin-Role | Nom d'un rôle d'administration (dynamique) par défaut ou nom d'un rôle d'administration personnalisé sur le pare-feu. |
| PaloAlto-Admin-Access-Domain | Nom d'un domaine d'accès réservé aux administrateurs du pare-feu (configuré à la page **Device (Périphérique)** > **Access Domains (Domaines d'accès)**). Définissez ce VSA si le pare-feu comporte plusieurs systèmes virtuels. |
| PaloAlto-Panorama-Admin-Role | Nom d'un rôle d'administration (dynamique) par défaut ou nom d'un rôle d'administration personnalisé sur Panorama. |

| Name (Nom) | Valeur |
|---|---|
| PaloAlto-Panorama-Admin-Access-Domain | Nom d'un domaine d'accès réservé aux administrateurs de modèles et de groupes de périphériques (configuré à la page **Panorama** > **Access Domains (Domaines d'accès)**). |
| PaloAlto-User-Group | Le nom d'un groupe utilisateurs dans la liste d'autorisation d'un profil d'authentification. |

# RADIUS

Radius (Remote Authentication Dial-In User Service) est un protocole réseau bénéficiant d'un large support et fournissant une authentification et une autorisation centralisées. Vous pouvez configurer l'authentification RADIUS pour les utilisateurs finaux ou les administrateurs dans le pare-feu et pour les administrateurs dans Panorama. Vous pouvez également utiliser les attributs spécifiques d'un fournisseur ou VSA (Vendor Specific Attributes) pour gérer les autorisations administrateur. Les VSA de RADIUS vous permettent de changer les rôles rapidement et d'accéder aux domaines et aux groupes d'utilisateurs à travers votre service annuaire au lieu de reconfigurer les réglages dans le pare-feu ou dans Panorama. Vous pouvez aussi configurer le pare-feu pour qu'il utilise un serveur RADIUS pour :

- Recueillir des VSA de points de terminaison GlobalProtect.
- Établir une Authentification multifacteur.

Lors de l'envoi de requêtes d'authentification à un serveur RADIUS, le pare-feu et Panorama utilisent le nom du profil d'authentification comme identifiant du Network Access Server (serveur d'accès au réseau ; NAS), même si le profil est associé à une séquence d'authentification pour le service (comme un accès administratif à l'interface web) ayant lancé le processus d'authentification.

Le pare-feu et Panorama sont compatibles avec les VSA RADIUS suivants. Pour définir les VSA sur un serveur RADIUS, vous devez spécifier le code fournisseur (25461 pour les pare-feu Palo Alto Networks ou pour Panorama), ainsi que le nom du VSA et son numéro. Vous devez également indiquer une valeur pour certains VSA. Reportez-vous à la documentation de votre serveur RADIUS pour les étapes à suivre pour définir ces VSA.

Vous pouvez également télécharger le dictionnaire RADIUS de Palo Alto Networks, qui définit les attributs d'authentification que le pare-feu Palo Alto Networks et un serveur RADIUS utilisent pour communiquer entre eux, et l'installer sur votre serveur RADIUS pour mapper les attributs aux données RADIUS binaires.

*Lorsque vous définissez des rôles administrateur dynamiques pour les utilisateurs sur le serveur, utilisez des lettres minuscules pour préciser le rôle (par exemple, saisissez* ***superuser****, et non pas* ***SuperUser****).*

*Quand vous configurez les options de fournisseurs avancées sur un serveur de contrôle d'accès (ACS) Cisco sécurisé, vous devez régler aussi bien la* ***Vendor Length Field Size (Longueur de Champ Fournisseur)*** *et le* ***Vendor Type Field Size (Type de Champ Fournisseur)*** *sur* ***1****. Sinon, l'authentification échouera.*

| Name (Nom) | Numéro | Valeur |
|---|---|---|
| VSA pour la gestion et l'authentification des comptes administrateur | | |
| PaloAlto-Admin-Role | 1 | Nom d'un rôle d'administration (dynamique) par défaut ou nom d'un rôle d'administration personnalisé sur le pare-feu. |
| PaloAlto-Admin-Access-Domain | 2 | Nom d'un domaine d'accès réservé aux administrateurs du pare-feu (configuré à la page **Device (Périphérique)** > **Access Domains (Domaines d'accès)**). Définissez ce VSA si le pare-feu comporte plusieurs systèmes virtuels. |
| PaloAlto-Panorama-Admin-Role | 3 | Nom d'un rôle d'administration (dynamique) par défaut ou nom d'un rôle d'administration personnalisé sur Panorama. |
| PaloAlto-Panorama-Admin-Access-Domain | 4 | Nom d'un domaine d'accès réservé aux administrateurs de modèles et de groupes de périphériques (configuré à la page **Panorama** > **Access Domains (Domaines d'accès)**). |
| PaloAlto-User-Group | 5 | Nom d'un groupe d'utilisateurs référencé par un profil d'authentification. |
| VSA transférés entre des points de terminaison GlobalProtect et le serveur RADIUS | | |
| PaloAlto-User-Domain | 6 | N'indiquez aucune valeur lors de la définition de ces VSA. |
| PaloAlto-Client-Source-IP | 7 | |
| PaloAlto-Client-OS | 8 | |
| PaloAlto-Client-Hostname | 9 | |
| PaloAlto-GlobalProtect-Client-Version | 10 | |

# LDAP

LDAP (Lightweight Directory Access Protocol) est un protocole standard d'accès aux répertoires d'informations. Vous pouvez configurer l'authentification LDAP pour les utilisateurs finaux, ainsi que pour les pare-feu et les administrateurs Panorama.

La configuration du pare-feu pour la connexion à un serveur LDAP vous permet également de définir des règles de stratégie basées sur les utilisateurs et les groupes d'utilisateurs au lieu de simplement les adresses IP. Pour les étapes, consultez Mapper les utilisateurs en groupes et Activer la stratégie basée sur les utilisateurs et les groupes.

# Authentification locale

Bien que le pare-feu et Panorama fournissent une authentification locale pour les administrateurs et les utilisateurs finaux, les services d'authentification externes sont préférables dans la plupart des cas, car ils fournissent une gestion centralisée des comptes. Toutefois, vous pouvez avoir besoin de comptes d'utilisateurs spéciaux que vous ne gérez pas via les serveurs d'annuaire que votre organisation réserve aux comptes habituels. Par exemple, vous pourriez définir un compte de super utilisateur qui est local sur le pare-feu, lequel vous permettra d'accéder au pare-feu même si le serveur d'annuaire ne fonctionne pas. Dans ce cas, vous pouvez utiliser les méthodes d'authentification locales suivantes :

- **(Pour le pare-feu uniquement) Authentification de base de données locale** : Pour configurer l'authentification de base de données locale, vous créez une base de données qui s'exécute localement sur le pare-feu et contient des comptes utilisateur (noms d'utilisateur et mots de passe). Ce type d'authentification est utile pour créer des comptes d'utilisateurs qui réutilisent les informations d'identification des comptes Unix existants dans les cas où vous connaissez uniquement les mots de passe hachés, pas les mots de passe en texte brut. Étant donné que l'authentification de base de données locale est associée à des profils d'authentification, vous pouvez prendre en charge des déploiements où différents groupes d'utilisateurs nécessitent des paramètres d'authentification différents, tels que l'authentification unique Kerberos (SSO) ou l'authentification multifacteur (MFA). Pour plus d'informations, consultez la section Configuration d'un profil et d'une séquence d'authentification. Pour les comptes d'administrateur qui utilisent un profil d'authentification, les password complexity and expiration settings (paramètres de complexité et d'expiration du mot de passe) ne sont pas appliqués. Cette méthode d'authentification est disponible pour les administrateurs qui accèdent au pare-feu (mais pas à Panorama) et aux utilisateurs finaux qui accèdent aux services et applications via le portail d'authentification ou GlobalProtect.
- **Authentification locale sans base de données** : vous pouvez configurer des comptes d'administration de pare-feu ou des comptes d'administration Panorama sans créer de base de données d'utilisateurs et de groupes d'utilisateurs s'exécutant localement sur le pare-feu ou Panorama. Cette méthode n'étant pas associée aux profils d'authentification, vous ne pouvez pas la combiner avec Kerberos SSO ou MFA. Toutefois, il s'agit de la seule méthode d'authentification qui autorise les profils de mot de passe, qui vous permettent d'associer des comptes individuels à des paramètres d'expiration de mot de passe différents des paramètres globaux. (Pour plus de détails, voir Définir la complexité du mot de passe et les paramètres d'expiration.

# Planification de votre déploiement d'authentification

Voici les questions clés à prendre en compte avant d'implémenter une solution d'authentification pour les administrateurs qui accèdent au pare-feu et pour les utilisateurs finaux qui accèdent aux services et applications via le portail d'authentification.

Pour les utilisateurs finaux et les administrateurs, considérez :

- Comment exploiter votre infrastructure de sécurité existante ? Normalement, il est plus rapide et moins coûteux d'intégrer le pare-feu à une infrastructure existante que d'établir une solution nouvelle et distincte destinée uniquement aux services du pare-feu. Le pare-feu peut s'intégrer à l'authentification multifactorielle, à SAML, à Kerberos, à TACACS+, à RADIUS et à LDAP. Si vos utilisateurs accèdent à des services et à des applications qui se trouvent à l'extérieur de votre réseau, vous pouvez utiliser SAML pour intégrer le pare-feu à un Identify Provider (Fournisseur d'identité ; IdP) qui contrôle l'accès aux services et aux applications internes et externes.
- Comment optimiser l'expérience utilisateur ? Si vous ne voulez pas que les utilisateurs s'authentifient manuellement et que vous possédez une infrastructure à clé publique, vous pouvez mettre en œuvre l'authentification à l'aide de certificats. Une autre option consiste à mettre en œuvre une Single Sign-On (Ouverture de session unique ; SSO) Kerberos ou SAML pour que les utilisateurs puissent accéder aux multiples services et applications après s'être connectés à un seul d'entre eux. Si vous réseau exige une sécurité supplémentaire, vous pouvez combiner l'authentification du certificat à une authentification interactive (mécanisme de demande/réponse).
- Avez-vous besoin de comptes d'utilisateur spéciaux que vous ne gérez pas via les serveurs d'annuaire que votre organisation réserve aux comptes ordinaires ? Par exemple, vous pourriez définir un compte de super utilisateur qui est local sur le pare-feu, lequel vous permettra d'accéder au pare-feu même si le serveur d'annuaire ne fonctionne pas. Vous pouvez configurer la Local Authentication (Authentification locale) pour ces comptes à but spécial.

  ***Il faut généralement préférer les** services d'authentification externe **aux services d'authentification locale puisqu'ils offrent l'avantage d'une gestion centrale des comptes, des services d'authentifications fiables et, généralement, des fonctions de journalisation et de dépannage.***

- Les noms d'utilisateur de vos comptes d'utilisateurs sont-ils correctement formatés ? L'exploitation de l'authentification SAML, Kerberos,, TACACS+,, RADIUS, et LDAP nécessite que tous les noms d'utilisateur adhèrent à la règle de nom de connexion Linux de l'expression régulière. Les noms d'utilisateur doivent avoir le format **`[a-zA-Z0-9_.] [a-zA-Z0-9_.-] {0,30} [a-zA-Z0-9_.$-]`**.

  Cela signifie que :

  - Le premier caractère du nom d'utilisateur doit être une lettre alphabétique majuscule ou minuscule, un chiffre (0-9) ou **_** (trait de soulignement) ou **.** (point).
  - Outre le premier et le dernier caractère, le nom d'utilisateur peut contenir des caractères alphabétiques majuscules ou minuscules, des nombres (0-9) et **_** (trait de soulignement), **.** (point) ou **-** (tiret). La longueur maximale est de 30 caractères, à l'exclusion du premier et du dernier caractère.

- Le dernier caractère du nom d'utilisateur peut être une lettre alphabétique majuscule ou minuscule, un nombre (0-9) ou **_** (trait de soulignement), **.** (point), **$**, ou **-** (tiret).

Le respect de la règle de nom de connexion Linux de l'expression régulière est requis pour les administrateurs PAN-OS uniquement. Il n'est pas requis pour les utilisateurs de GlobalProtect et du portail captif.

Pour les utilisateurs finaux uniquement, considérez :

- Quels services et applications sont plus sensibles que les autres ? Par exemple, vous pourriez souhaiter disposer d'une authentification plus forte pour les documents financiers clés que pour les moteurs de recherche. Pour protéger vos applications et services les plus sensibles, vous pouvez configurer l'Authentification multifacteur pour vous assurer que chaque utilisateur s'authentifie au moyen de méthodes (facteurs) lorsqu'il accède à ces services et à ces applications. Pour satisfaire une diversité de besoins en sécurité, procédez à la Configuration des règles de la politique d'authentification qui entraînent la MFA ou l'authentification à un seul facteur (comme les informations d'identification d'ouverture de session ou les certificats) selon des services, des applications et des utilisateurs finaux spécifiques. Parmi les autres façons qui s'offrent à vous de réduire votre surface d'attaque, notons la segmentation de réseau et les groupes d'utilisateurs pour les applications autorisées.

Pour les administrateurs uniquement, considérez :

- Utilisez-vous un serveur externe pour gérer l'autorisation de tous les comptes administratifs de manière centralisée ? En définissant des Vendor-Specific Attributes (attributs spécifiques au fournisseur ; VSA) sur le serveur externe, vous pouvez rapidement modifier les affectations de rôles d'administrateur via votre service d'annuaire plutôt que de devoir reconfigurer les paramètres sur le pare-feu. Les VSA vous permettent également de spécifier des domaines d'accès pour les administrateurs des pare-feu disposant de plusieurs systèmes virtuels. SAML, TACACS+ et RADIUS prennent en charge l'autorisation externe.

# Configuration de l'authentification multifacteur

Pour utiliser la Multi-Factor Authentication (authentification multifacteur ; MFA) pour protéger les services et applications sensibles, vous devez configurer le portail d'authentification pour qu'il affiche un formulaire Web pour le premier facteur d'authentification et consigne les horodatages d'authentification. Le pare-feu se sert des horodatages pour évaluer les délais d'expiration des règles de la politique d'authentification. Pour permettre l'existence d'autres facteurs d'authentification, vous pouvez intégrer le pare-feu aux fournisseurs MFA via RADIUS ou les API des fournisseurs. Après avoir évalué la politique d'authentification, le pare-feu évalue la politique de sécurité ; vous devez donc configurer les règles pour les deux types de politique.

*Palo Alto Networks fournit de l'assistance pour les fournisseurs MFA dans les mises à jour de contenu des applications. C'est-à-dire que si vous utilisez Panorama pour transmettre les configurations du groupe de périphériques aux pare-feu, vous devez installer les mêmes mises à jour d'applications sur les pare-feu et sur Panorama pour éviter qu'il n'existe de disparités dans l'assistance côté fournisseur.*

*Les intégrations des API des fournisseurs MFA sont prises en charge pour l'authentification des utilisateurs finaux via la Politique d'authentification uniquement. Pour l'authentification des utilisateurs distants aux portails et passerelles GlobalProtect ou pour l'authentification des administrateurs à l'interface Web de Panorama ou PAN-OS, vous ne pouvez utiliser que les fournisseurs MFA pris en charge par RADIUS ou SAML ; les services MFA via les API des fournisseurs ne sont pas pris en charge dans ces cas d'utilisation.*

**STEP 1 |** Effectuez la Configure Authentication Portal (Configuration du portail d'authentification) en mode **Redirect (Rediriger)** pour afficher un formulaire Web pour le premier facteur d'authentification, pour consigner les horodatages d'authentification et pour mettre à jour les mappages d'utilisateur.

**STEP 2 |** Configurez l'un des profils de serveur suivants pour définir la manière dont le pare-feu se connectera au service qui permet d'authentifier les utilisateurs pour le premier facteur d'authentification.

- Ajoutez un profil de serveur RADIUS. Cette étape est requise si le pare-feu s'intègre à un fournisseur MFA via RADIUS. Dans ce cas, le fournisseur MFA fournir le premier facteur d'authentification ainsi que les facteurs supplémentaires ; vous pouvez donc sauter l'étape suivante (configuration d'un profil de serveur MFA). Si le pare-feu s'intègre à un fournisseur MFA via une API, vous pouvez tout de même utiliser un profil de serveur RADIUS pour le premier facteur ; des profils de serveur MFA sont toutefois requis pour les facteurs supplémentaires.
- Ajoutez un profil de serveur d'IDP en SAML.
- Ajoutez un profil de serveur Kerberos.
- Ajoutez un profil de serveur TACACS+.

- Ajoutez un profil de serveur LDAP.

*Dans la plupart des cas, un service externe est recommandé pour le premier facteur d'authentification. Vous pouvez toutefois effectuer une* configuration de l'authentification à l'aide d'une base de données locale *comme option de rechange.*

**STEP 3 |** Ajoutez un profil de serveur MFA.

Le profil définit comment le pare-feu se connecte au serveur MFA. Ajoutez un profil distinct pour chaque facteur d'authentification qui suit le premier facteur. Le pare-feu s'intègre avec ces serveurs MFA au moyen des API des fournisseurs. Vous pouvez indiquer jusqu'à trois facteurs supplémentaires. Chaque fournisseur MFA fournit un facteur, bien que certains fournisseurs permettent aux utilisateurs de choisir un facteur parmi plusieurs options.

1. Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveur)** > **Multi Factor Authentication (Authentification multifacteur)** et **Add (Ajoutez)** un profil.
2. Saisissez un **Name (Nom)** pour identifier le serveur MFA.
3. Sélectionnez le **Certificate Profile (Profil du certificat)** que le pare-feu utilisera pour valider le certificat du serveur MFA lors de la configuration d'une connexion sécurisée au serveur MFA.
4. Sélectionnez le **MFA Vendor (Fournisseur MFA)** que vous avez déployé.
5. Configurez la **Value (Valeur)** de chaque attribut du fournisseur.

   Les attributs définissent la manière dont le pare-feu se connecte au serveur MFA. Chaque **Type (Type)** de fournisseur exige différents attributs et valeurs ; consultez votre documentation du fournisseur pour obtenir de plus amples renseignements.
6. Cliquez sur **OK** pour enregistrer le profil.

**STEP 4 |** Configurez un profil d'authentification.

Le profil définit l'ordre des facteurs d'authentification auxquels les utilisateurs doivent répondre.

1. Sélectionnez **Device (Périphérique)** > **Authentication Profile (Profil d'authentification)** et **Add (Ajoutez)** un profil.
2. Entrez un **Name (Nom)** pour identifier le profil d'authentification.
3. Sélectionnez le **Type (Type)** applicable au premier facteur d'authentification et sélectionnez le **Server Profile (Profil de serveur)** correspondant.
4. Sélectionnez **Factors (Facteurs)**, **Enable Additional Authentication Factors (Activer les facteurs d'authentification supplémentaires)** et **Add (Ajoutez)** les profils de serveur MFA que vous avez configurés.

   Le pare-feu appellera chaque service MFA dans l'ordre indiqué, de haut en bas.
5. Cliquez sur **OK** pour enregistrer le profil d'authentification.

**STEP 5 |** Configurez un objet de mise en œuvre de l'authentification.

L'objet associe chaque profil d'authentification à une méthode du portail d'authentification. La méthode détermine si la première demande d'authentification (facteur) est transparente ou si elle exige une réponse de l'utilisateur.

Sélectionnez le **Authentication Profile (Profil d'authentification)** que vous avez configuré et saisissez un **Message (Message)** qui indique aux utilisateurs la manière de s'authentifier au premier facteur. Le message s'affiche dans le formulaire Web du portail d'authentification.

*Si vous définissez la **Authentication Method (Méthode d'authentification)** sur **browser-challenge (Navigateur/demande)**, le formulaire Web du portail d'authentification n'apparaît que si l'authentification SSO Kerberos SSO échoue. Sinon, l'authentification au premier facteur est automatique ; les utilisateurs ne verront pas le formulaire Web.*

**STEP 6 |** Configurez une règle de politique d'authentification.

La règle doit correspondre aux services et aux applications que vous voulez protéger et aux utilisateurs qui doivent s'authentifier.

1. Sélectionnez **Policies (Stratégies)** > **Authentication (Authentification)**, puis **Add (Ajoutez)** une règle.
2. Donnez un **Name (Nom)** à la règle afin de l'identifier.
3. Sélectionnez **Source (Source)** et **Add (Ajoutez)** des zones ou des adresses IP précises ou sélectionnez **Any (Toute)** zone ou adresse IP.

   La règle ne s'applique qu'au trafic provenant des adresses IP indiquées ou des interfaces qui se trouvent dans les zones indiquées.
4. Sélectionnez **User (Utilisateur)**, puis sélectionnez ou **Add (Ajoutez)** les utilisateurs sources et les groupes d'utilisateurs auxquels les règles s'appliquent (par défaut **any (indifférent)**).
5. Sélectionnez **Destination (Destination)** et **Add (Ajoutez)** des zones ou des adresses IP précises ou sélectionnez **Any (Toute)** zone ou adresse IP.

   Les adresses IP peuvent être des ressources (comme des serveurs) auxquelles vous souhaitez contrôler l'accès.
6. Sélectionnez **Service/URL Category (Service/Catégorie d'URL)**, puis sélectionnez ou **Add (Ajoutez)** les services et groupes de services auxquels la règle contrôle l'accès (par défaut **service-http (service-http)**).
7. Sélectionnez ou **Add (Ajoutez)** les catégories d'URL auxquelles la règle contrôle l'accès (par défaut **any (indifférent)**). Par exemple, vous pouvez créer une catégorie d'URL personnalisée qui spécifie vos sites internes les plus sensibles.
8. Sélectionnez **Actions (Actions)**, puis sélectionnez l'objet de **Authentication Enforcement (Mise en œuvre de l'authentification)** que vous avez créé.
9. Indiquez la période de **Timeout (Temporisation)** en minutes (par défaut 60) au cours de laquelle le pare-feu invite l'utilisateur à s'authentifier une seule fois pour un accès récurrent aux services et aux applications.

   *Le **Délai d'expiration** est un compromis entre une sécurité plus stricte (période plus courte entre les invites d'authentification) et l'expérience utilisateur (période plus longue entre les invites d'authentification). Une authentification plus fréquente est souvent le choix le plus indiqué pour accéder aux systèmes critiques et aux zones sensibles, comme un centre de données. Une authentification moins fréquente est souvent indiquée au périmètre du réseau de même que pour les entreprises pour lesquelles l'expérience utilisateur est clé.*
10. Cliquez sur **OK** pour enregistrer la règle.

**STEP 7 |** Personnalisez la page de connexion MFA.

Le pare-feu affiche la page pour informer les utilisateurs de la manière dont ils doivent s'authentifier aux facteurs MFA et pour indiquer l'état de l'authentification (en cours, réussie ou échouée).

1. Sélectionnez **Device (Périphérique)** > **Response Pages (Pages de réponse)**, puis sélectionnez **MFA Login Page (Page de connexion MFA)**.
2. Sélectionnez la page de réponse **Predefined (Prédéfinie)**, puis **Export (Exportez)** la page vers votre système client.
3. Sur votre système client, utilisez un éditeur HTML pour personnaliser la page de réponse téléchargée et enregistrez-la en lui donnant un nom de fichier unique.
4. Revenez à la boîte de dialogue de la page de connexion MFA du pare-feu, **Import (Importez)** votre page personnalisée, **Browse (Parcourez)** pour sélectionnez le **Import File (Fichier d'importation)**, sélectionnez la **Destination (Destination)** (système virtuel ou emplacement **shared (partagé)**), cliquez sur **OK (OK)**, et cliquez sur **Close (Fermer)**.

**STEP 8 |** Configurez une règle de politique de sécurité qui autorise les utilisateurs à accéder aux services et aux applications qui exigent une authentification.

1. Création d'une règle de politique de sécurité.
2. **Commit (Validez)** vos modifications.

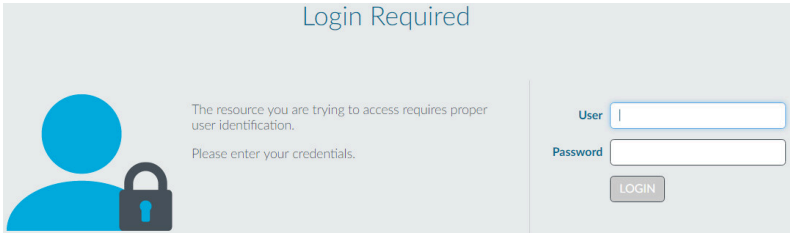
*Le moteur de corrélation automatique du pare-feu utilise plusieurs objets de corrélation pour détecter les événements sur votre réseau qui pourraient indiquer la présence d'un abus des informations d'identification lié à la MFA. Pour examiner les événements, sélectionnez **Monitor (Surveillance)** > **Automated Correlation Engine (Moteur de corrélation automatique)** > **Correlated Events (Événements corrélés)**.*

**STEP 9 |** Vérifiez que le pare-feu applique la MFA.

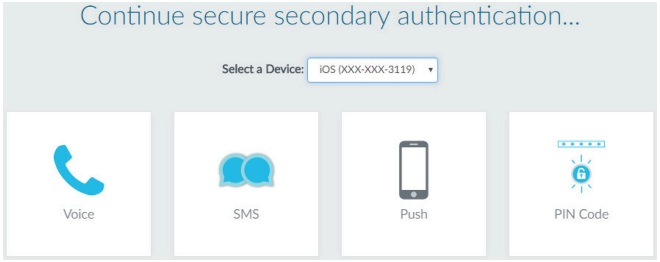
1. Connectez-vous à votre réseau en utilisant les informations d'identification de l'un des utilisateurs sources indiqués dans la règle d'authentification.
2. Demandez un service ou une application qui correspond à l'un des services ou à l'une des applications indiqués dans la règle.

   Le pare-feu affiche le formulaire Web du portail d'authentification correspondant au premier facteur d'authentification. La page contient le message que vous avez saisi dans l'objet de mise en œuvre de l'authentification. Par exemple :




3. Saisissez vos informations d'identification d'utilisateur pour répondre à la première demande d'authentification.

   Le pare-feu affiche ensuite la page de connexion MFA correspondant au facteur d'authentification suivant. Par exemple, le service MFA pourrait vous inviter à sélectionner la méthode d'authentification par voix, SMS, fonction push ou code PIN (OTP). Si vous sélectionnez la fonction push, votre téléphone vous invite à approuver l'authentification.




4. Authentifiez-vous au facteur suivant.

   Un message d'échec ou de réussite de l'authentification s'affiche sur le pare-feu. En cas de réussite, le pare-feu affiche ensuite une page de connexion MFA pour le facteur d'authentification suivant, le cas échéant.

   Répétez cette étape pour chaque facteur MFA. Une fois que vous vous êtes authentifié à tous les facteurs, le pare-feu évalue la politique de sécurité pour déterminer s'il autorise l'accès au service ou à l'application.
5. Mettez fin à la session du service ou de l'application auquel vous venez d'accéder.
6. Commencez une nouvelle session pour ce même service ou cette même application. Assurez-vous d'effectuer cette étape dans la période de **Timeout (Temporisation)** que vous avez configurée dans la règle d'authentification.

   Le pare-feu autorise l'accès sans que vous ayez à vous authentifier de nouveau.
7. Attendez que la période de **Timeout (Temporisation)** soit écoulée et demandez l'accès au même service ou à la même application.

   Le pare-feu vous invite à vous authentifier de nouveau.

# Configuration de la MFA entre RSA SecurID et le pare-feu

L'authentification multifacteur vous permet de protéger les ressources de l'entreprise en utilisant des facteurs multiples pour vérifier l'identité d'un utilisateur avant de l'autoriser à accéder aux ressources du réseau. Pour activer la Multi-Factor Authentication (authentification multifacteur ; MFA) entre le pare-feu et le Service d'authentification au cloud RSA SecurID Access, vous devez d'abord configurer le Service RSA SecurID afin de disposer des détails dont vous avez besoin pour configurer le pare-feu pour l'authentification des utilisateurs au moyen de plusieurs facteurs. Une fois que vous avez effectué la configuration requise sur la Console RSA SecurID Access, vous pouvez configurer le pare-feu pour qu'il s'intègre à RSA SecurID.

*Le pare-feu nouvelle génération Palo Alto Networks s'intègre au Service d'authentification au cloud RSA SecurID Access. L'intégration de l'API MFA à RSA SecurID est prise en charge pour les services cloud uniquement et ne prend pas en charge l'authentification à deux facteurs pour le gestionnaire d'authentification sur site lorsque le deuxième facteur utilise l'API propre au fournisseur. La version du contenu minimale requise pour cette intégration est 752 et PAN-OS 8.0.2.*

- Obtenir les détails auprès du Service d'authentification au cloud RSA SecurID Access
- Configurer le pare-feu pour la MFA avec RSA SecurID

## Obtenir les détails auprès du Service d'authentification au cloud RSA SecurID Access

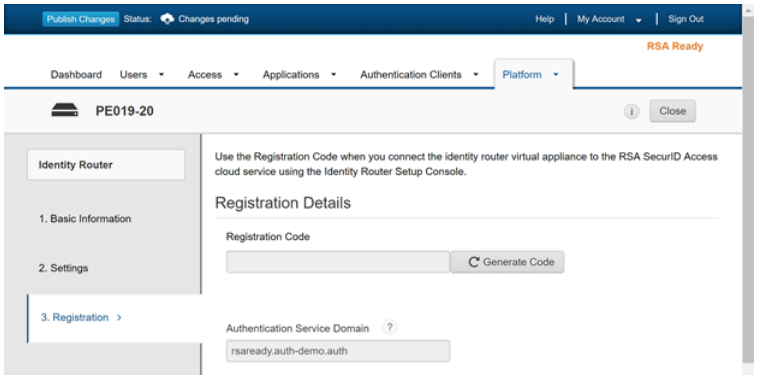
Afin de transmettre les requêtes d'authentification entre le pare-feu et le Service d'authentification au cloud RSA SecurID Access, vous devez d'abord vous rendre sur la Console RSA SecurID Access et configurer l'ID RSA Access, l'URL du service d'authentification et la clé API du client auquel le pare-feu doit s'authentifier et qui possède le service avec lequel le pare-feu doit interagir. Le pare-feu a également besoin de l'ID de la politique d'accès qui utilise la méthode d'authentification par code de jeton RSA ou RSA Approuve pour s'authentifier auprès de la source d'identité.

1. **Generate the RSA SecurID API key (Générer la clé API RSA SecurID)** : connectez-vous à la Console RSA SecurID, puis sélectionnez **My Account (Mon compte)** > **Company Settings (Paramètres d'entreprise)** > **Authentication API Keys (Clés API d'authentification)**. **Add (Ajoutez)** une nouvelle clé, puis **Save Settings (Enregistrez les paramètres)** et **Publish Changes (Publiez les modifications)**.

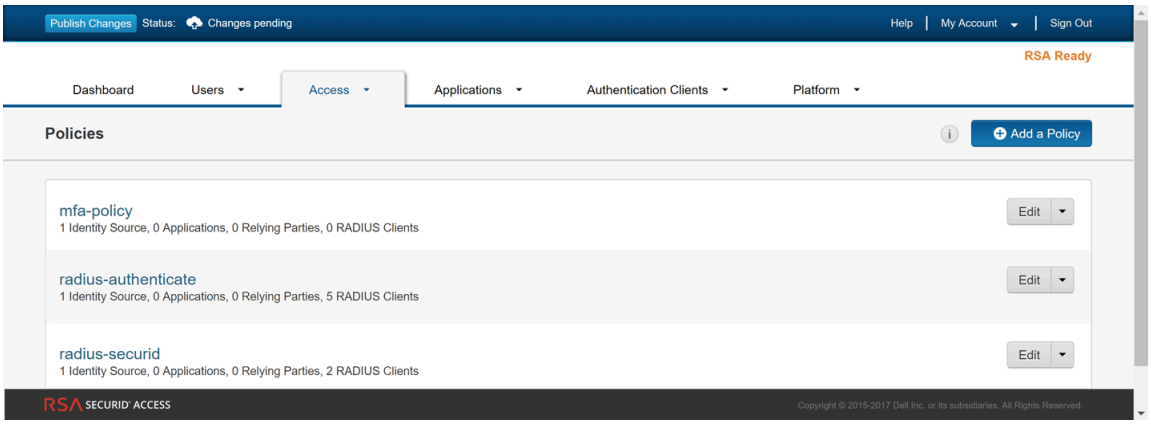

2. **Get the RSA SecurID Access endpoint API (Authentication Service Domain) to which the firewall must connect (Obtenir l'API des terminaux RSA SecurID Access)** : sélectionnez **Platform (Plateforme)** > **Identity Routers (Routeurs d'identité)**, sélectionnez un routeur

d'identité pour **Edit (Modifier)** et notez le **Authentication Service Domain (Domaine du service d'authentification)**. Dans cet exemple, il s'agit de https://rsaready.auth-demo.auth.




- **Get the Access Policy ID (Obtenir l'ID de la politique d'accès)** : sélectionnez **Access (Accès)** > **Policies (Politiques)**, puis notez le nom de la politique d'accès qui permettra au pare-feu de faire office de client d'authentification auprès du service RSA SecurID. Selon sa configuration, la politique doit soit utiliser les méthodes d'authentification RSA Approuve ou par code de jeton RSA uniquement.




## Configurer le pare-feu pour la MFA avec RSA SecurID

Une fois que vous avez réussi à Obtenir les détails auprès du Service d'authentification au cloud RSA SecurID Access, vous pouvez configurer le pare-feu pour qu'il invite les utilisateurs à saisir un jeton RSA SecurID lorsque la MFA est invoquée.

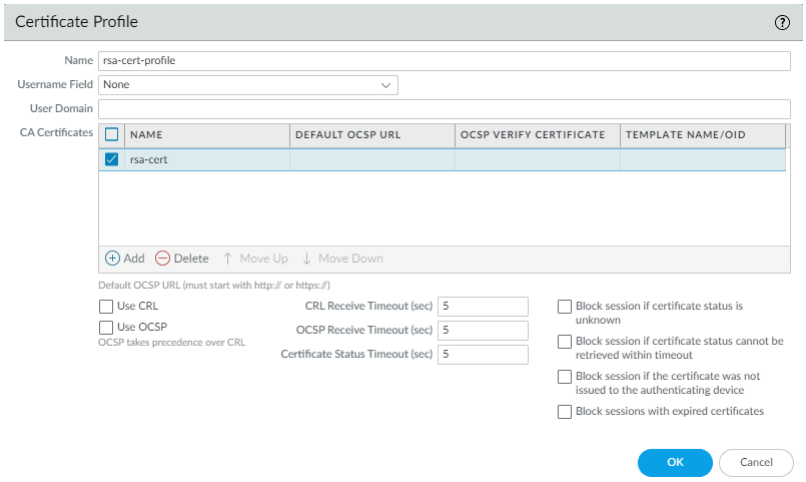
 

**STEP 1 |** Configurez le pare-feu pour qu'il se fie au certificat SSL fourni par l'API du terminal RSA SercurID Access.

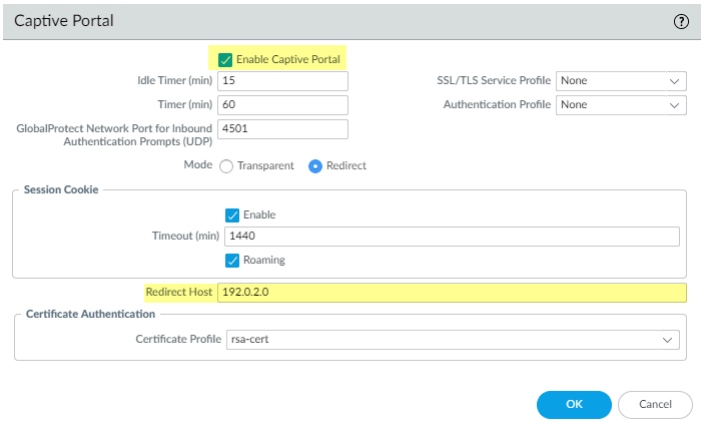
1. Exportez le certificat SSL du terminal RSA SecurID Access et importez-le sur le pare-feu.

   Pour activer la confiance entre le pare-feu et l'API du terminal RSA SecurID Access, vous devez importer un certificat auto-signé ou le certificat de l'autorité de certification utilisé pour signer le certificat.

2. Procédez à la Configuration d'un profil de certificat (**Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificat)**, puis cliquez sur **Add (Ajouter)**).




**STEP 2 |** Procédez à la Configure Authentication Portal (Configuration du portail d'authentification) (**Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Authentication Portal Settings (Paramètres du portail d'authentification)**) en mode Rediriger pour afficher un formulaire Web permettant l'authentification auprès de RSA SecurID. Assurez-vous d'indiquer l'Hôte de redirection sous forme d'adresse IP ou d'un nom d'hôte (un nom d'hôte sans point) qui résout en adresse IP l'interface de Couche 3 sur le pare-feu vers laquelle les requêtes Web sont redirigées.

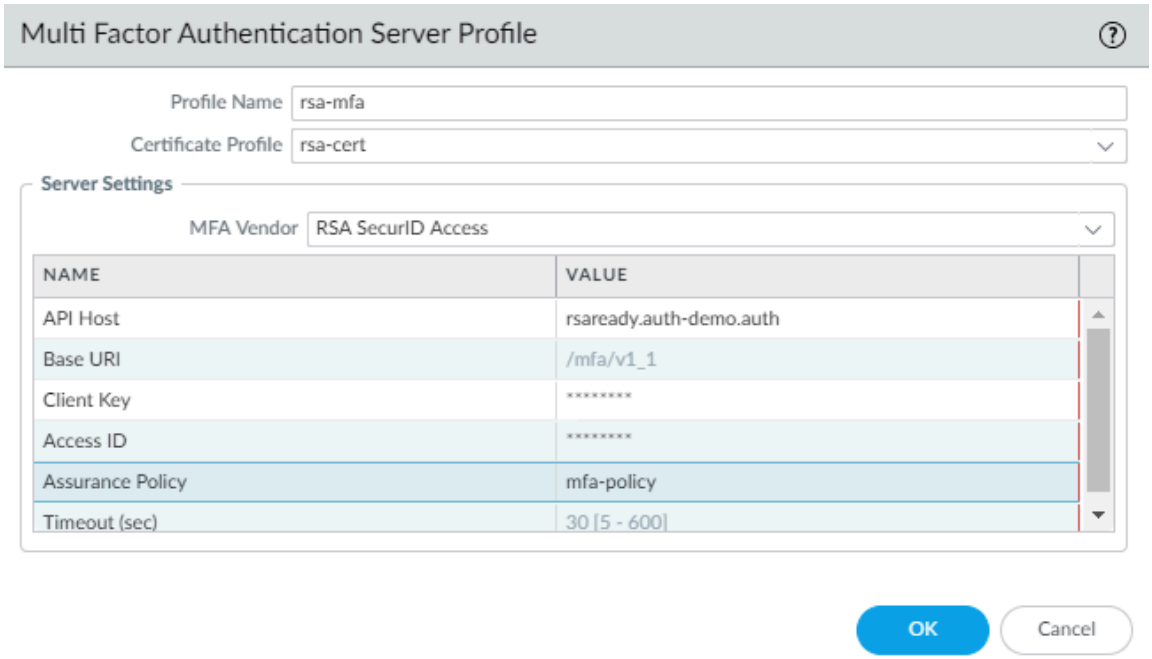



**STEP 3 |** Configurez un profils de serveur d'authentification multifacteur pour préciser la méthode de connexion entre le pare-feu et le service de cloud RSA SecurID **(Device (Périphérique)**

> **Server Profiles (Profils de serveur)** > **Multi Factor Authentication (Authentification multifacteur)**, puis cliquez sur **Add (Ajouter)**).

1. Saisissez un **Name (Nom)** pour identifier le profil de serveur MFA.
2. Sélectionnez le **Certificate Profile (Profil de certificat)** que vous avez créé précédemment, rsa-cert-profile dans le présent exemple. Le certificat utilisera ce certificat lorsqu'il établira une connexion sécurisée avec le service Cloud RSA SecurID.
3. Dans la liste déroulante **MFA Vendor (Fournisseur de MFA)** sélectionnez **RSA SecurID Access (Accès à RSA SecurID)**.
4. Configurez la **Value (Valeur)** de chaque attribut que vous avez noté à la section Obtenir les détails auprès du Service d'authentification au cloud RSA SecurID Access :
   - **API Host (Hôte API)** : saisissez le nom d'hôte ou l'adresse IP du terminal API de RSA SecurID auquel le pare-feu doit se connecter, rsaready.auth-demo.auth dans le présent exemple.
   - **Base URI (URI de base)** : ne modifiez pas la valeur par défaut (/mfa/v1_1).
   - **Client Key (Clé du client)** : saisissez la clé du client RSA SecurID.
   - **Access ID (ID Access)** : saisissez l'ID RSA SecurID Access.
   - **Assurance Policy (Politique d'assurance)** : entrez le nom de la politique RSA SecurID Access, mfa-policy dans le cas présent.
   - **Timeout (Délai d'expiration)** : la valeur par défaut est 30 secondes.



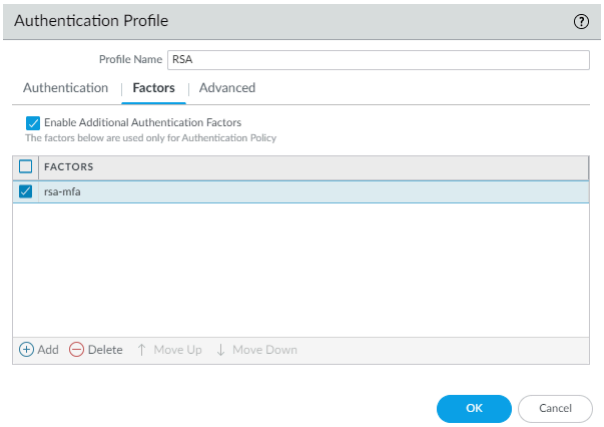

5. Enregistrez le profil.

**STEP 4 |** Procédez à la Configuration d'un Profil d'authentification (**Device (Périphérique)** > **Authentication Profile (Profil d'authentification)**, puis cliquez sur **Add (Ajouter)**).

Le profil définit l'ordre des facteurs d'authentification auxquels les utilisateurs doivent répondre.

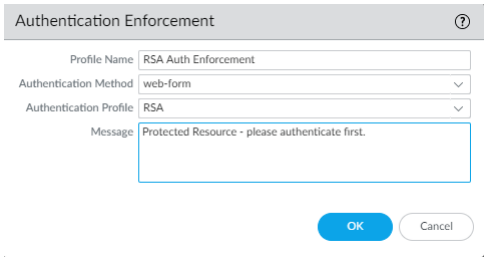
1. Sélectionnez le **Type (Type)** applicable au premier facteur d'authentification et sélectionnez le **Server Profile (Profil de serveur)** correspondant.
2. Sélectionnez **Factors (Facteurs)**, **Enable Additional Authentication Factors (Activer les facteurs d'authentification supplémentaires)** et **Add (Ajoutez)** le profil de serveur rsa-mfa que vous avez créé précédemment dans cet exemple.




3. Cliquez sur **OK** pour enregistrer le profil d'authentification.

**STEP 5 |** Configurez un objet de mise en œuvre de l'authentification. (**Objects (Objets)** > **Applications (Applications)** et cliquez sur **Add (Ajouter)**).

Assurez-vous de sélectionner le profil d'authentification que vous venez de définir, nommé RSA dans le présent exemple.

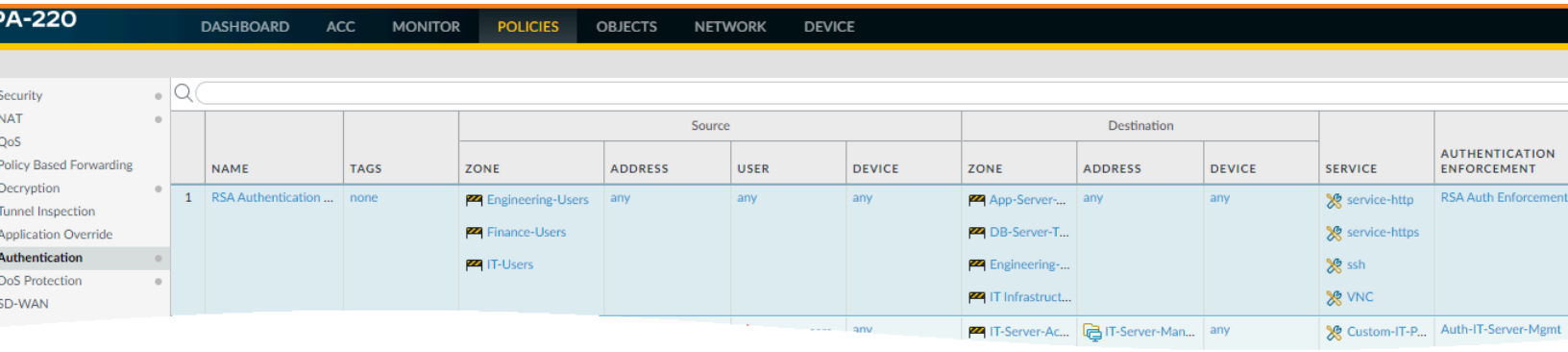



**STEP 6 |** Configurez une règle de politique d'authentification. (**Policies (Politiques)** > **Applications (Applications)** et cliquez sur **Add (Ajouter)**.)

Votre règle de politique d'authentification doit correspondre aux services et aux applications que vous souhaitez protéger, spécifier les utilisateurs qui doivent s'authentifier et inclure l'objet d'application de l'authentification qui lance le profil d'authentification. Dans le présent exemple, RSA SecurID Access authentifie tous les utilisateurs accédant par trafic HTTP, HTTPS, SSH et VNC au moyen de l'objet d'application de l'authentification nommé RSA Auth Enforcement

(Application de l'authentification RSA) (sous **Actions**, sélectionnez l'objet de **Authentication Enforcement (Application de l'authentification)**).

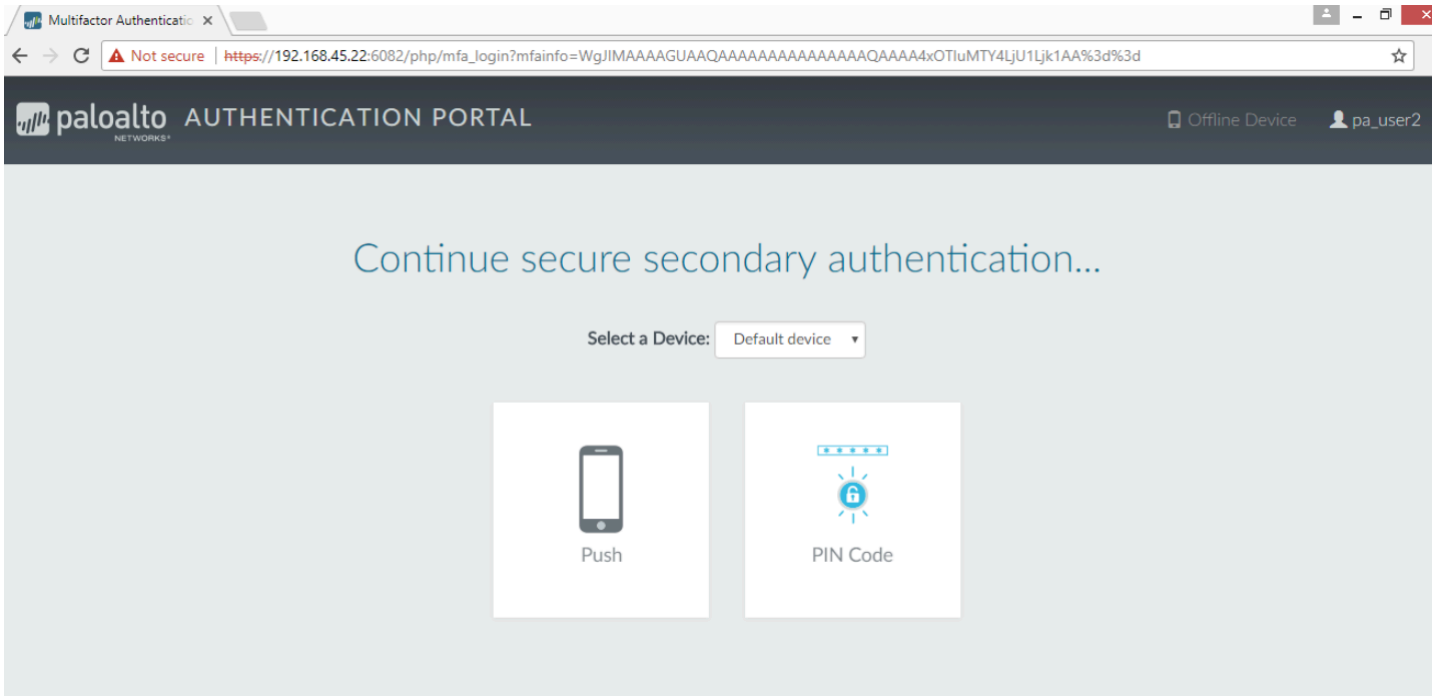



**STEP 7 |** Cliquez sur **Commit (Valider)** pour valider les modifications que vous avez apportées au pare-feu.

**STEP 8 |** Vérifiez que les utilisateurs de votre réseau sont sécurisés par RSA SecurID en utilisant la méthode d'authentification push ou par code PIN que vous avez activée.

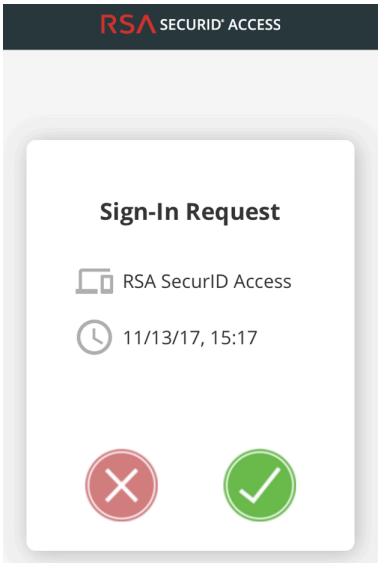
1. **Authentification push**

   1. Demandez à un utilisateur de votre réseau de lancer un navigateur Web d'accéder au site Web. La page du portail d'authentification qui possède l'adresse IP ou le nom d'hôte correspondant à la valeur Rediriger l'hôte que vous avez définie précédemment devrait s'afficher.
   2. Vérifiez que l'utilisateur saisit les informations d'identification du premier facteur d'authentification, puis qu'il passe au facteur d'authentification secondaire, et qu'il sélectionne **Push**.



3. Vérifiez la présence d'une **Sign-In request (Requête d'ouverture de session)** sur l'application RSA SecurID Access installée sur le périphérique mobile de l'utilisateur.
4. Demandez à l'utilisateur de **Accept (Accepter)** la requête d'ouverture de session sur le périphérique mobile et d'attendre quelques secondes pour donner le temps au pare-feu de recevoir la notification de réussite d'authentification. L'utilisateur devrait parvenir à accéder au site Web demandé.



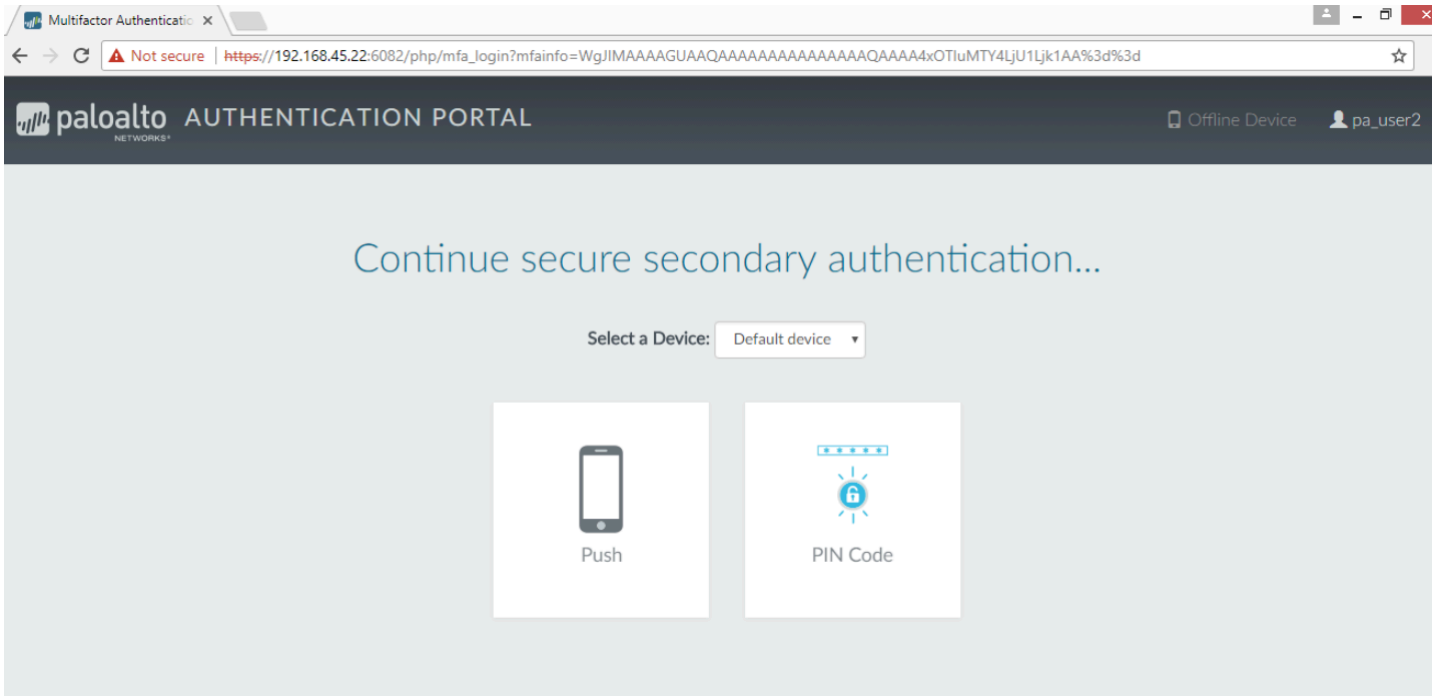

*Pour tester un échec d'authentification, **Decline (Refusez)** la requête d'ouverture de session sur le périphérique mobile.*

2. **Authentification par Code PIN**

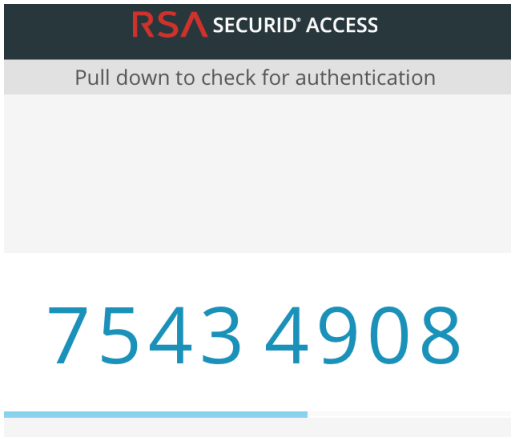
1. Demandez à un utilisateur de votre réseau de lancer un navigateur Web d'accéder au site Web. La page du portail d'authentification qui possède l'adresse IP ou le nom d'hôte correspondant à la valeur Rediriger l'hôte que vous avez définie précédemment devrait s'afficher.

2. Vérifiez que l'utilisateur saisit les informations d'identification du premier facteur d'authentification, puis qu'il passe au facteur d'authentification secondaire, et qu'il sélectionne **PIN Code**.




3. Vérifiez qu'un **PIN Code** s'affiche sur l'application RSA SecurID Access installée sur le périphérique mobile de l'utilisateur.




4. Demandez à l'utilisateur de copier le code PIN dans l'invite **Enter the PIN... (Saisir le PIN...)** du navigateur Web, puis de cliquer sur **Submit (Soumettre)**. Attendez quelques secondes pour donner le temps au pare-feu de recevoir la notification de réussite d'authentification. L'utilisateur devrait parvenir à accéder au site Web demandé.

## Configuration de la MFA entre Okta et le pare-feu

L'authentification multifacteur vous permet de protéger les ressources de l'entreprise en utilisant des facteurs multiples pour vérifier l'identité des utilisateurs avant de l'autoriser à accéder aux ressources du réseau.

Pour activer la Multi-Factor Authentication (authentification multifacteur ; MFA) entre le pare-feu et le service de gestion de l'identité d'Okta :

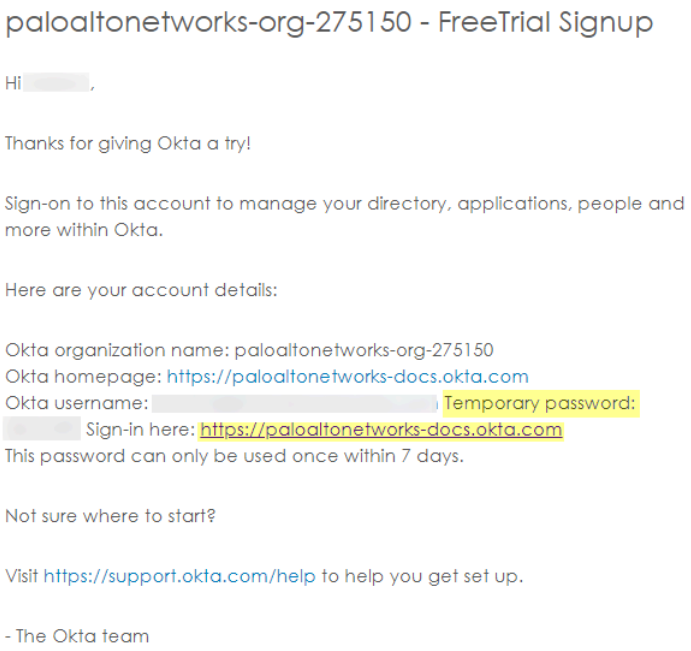
- Configurez Okta
- Configurez le pare-feu pour l'intégrer à Okta
- Vérifiez la MFA au moyen d'Okta

## Configurez Okta

Connectez-vous au portail d'administration d'Okta pour créer vos comptes utilisateurs, définir votre politique MFA d'Okta et obtenir les informations sur les jetons nécessaires à la configuration de la MFA au moyen d'Okta sur le pare-feu.

**STEP 1 |** Créez votre compte utilisateur administratif Okta.

1. Soumettez votre adresse électronique et votre nom, puis cliquez sur **Get Started (Commencer)**.
2. Cliquez sur le lien dans le courriel de confirmation et utilisez le mot de passe temporaire inclus pour vous connecter au portail d'administration d'Okta.



paloaltonetworks-org-275150 - FreeTrial Signup

Hi ,

Thanks for giving Okta a try!

Sign-on to this account to manage your directory, applications, people and more within Okta.

Here are your account details:

Okta organization name: paloaltonetworks-org-275150
Okta homepage: https://paloaltonetworks-docs.okta.com
Okta username: Temporary password:
Sign-in here: https://paloaltonetworks-docs.okta.com
This password can only be used once within 7 days.

Not sure where to start?

Visit https://support.okta.com/help to help you get set up.

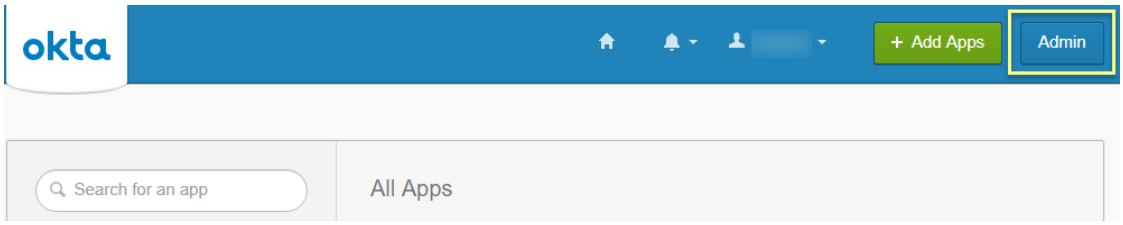
- The Okta team

3. Créez un nouveau mot de passe comprenant au moins huit caractères, une lettre minuscule, une lettre majuscule, un nombre qui n'inclut aucune partie de votre nom d'utilisateur.
4. Sélectionnez une question de rappel du mot de passe et saisissez la réponse.
5. Sélectionnez une image de sécurité, puis **Create My Account (Créez mon compte)**.

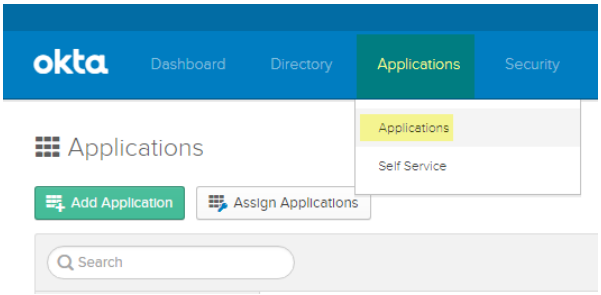
 

**STEP 2 |** Configurez votre service Okta.

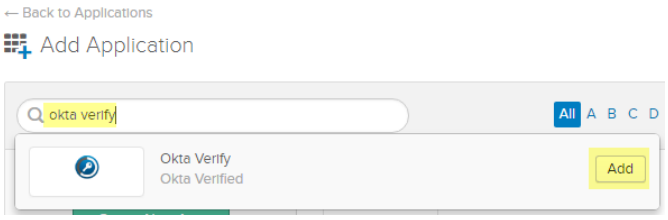
*Si vous vous connectez et n'êtes pas redirigé vers le portail d'administration d'Okta, sélectionnez **Admin** dans le coin supérieur droit.*




1. Dans le tableau de bord d'Okta, connectez-vous en utilisant vos informations d'identification d'administrateur d'Okta, puis sélectionnez **Applications** > **Applications**.



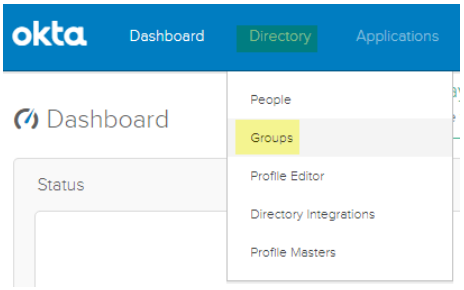

2. Sélectionnez **Add Application (Ajouter une application)**.
3. Cherchez **`Okta Verify`**.
4. Sélectionnez **Add (Ajouter)**, puis **Done (Terminé)**.



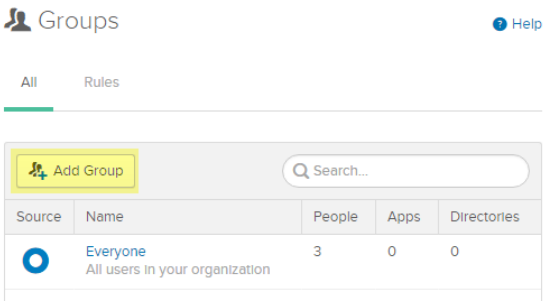

 

**STEP 3 |** Créez un ou plusieurs groupes d'utilisateurs pour classer vos utilisateurs (par exemple, par périphérique, par politique ou par service) et pour l'application Okta Verify.

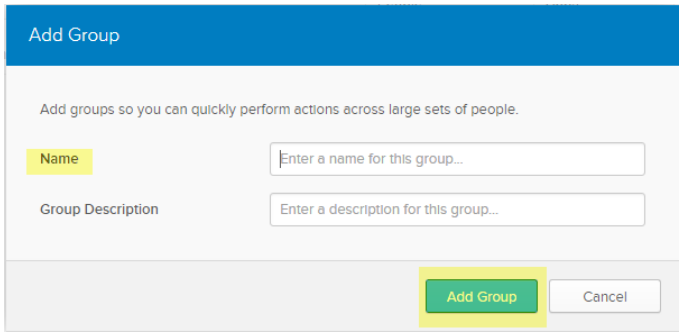
1. Sélectionnez **Directory (Répertoire)** > **Groups (Groupes)**.




2. Cliquez sur **Add Group (Ajouter le groupe)**.



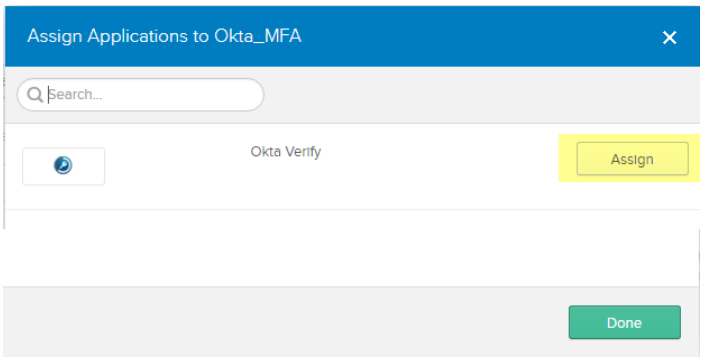

3. Saisissez un **Name (Nom)** de groupe et, éventuellement, une **Group Description (Description du groupe)**, puis **Add Group (Ajoutez le groupe)**.




*Le groupe **Everyone (Tout le monde)** par défaut comprend tous les utilisateurs configurés pour votre organisation lors de la première étape de* configuration d'Okta**.**

4. Sélectionnez le groupe que vous avez créé, puis sélectionnez **Manage Apps (Gérer les applications)**.
5. **Assign (Affectez)** l'application Okta Verify que vous avez ajoutée à l'étape 2.

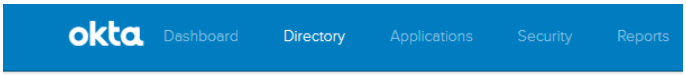
 

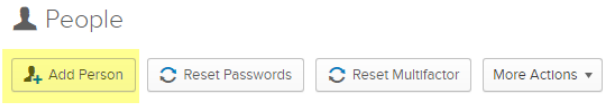



6. Une fois l'application **Assigned (Affectée)**, cliquez sur **Done (Terminé)**.
7. Reprenez ce processus pour tous les groupes qui utiliseront l'application Okta Verify pour la MFA.

**STEP 4 |** Ajoutez des utilisateurs et affectez-les à un groupe.

1. À partir du tableau de bord d'Okta, sélectionnez **Directory (Répertoire)** > **People (Personnes)** > **Add Person (Ajouter une personne)**.

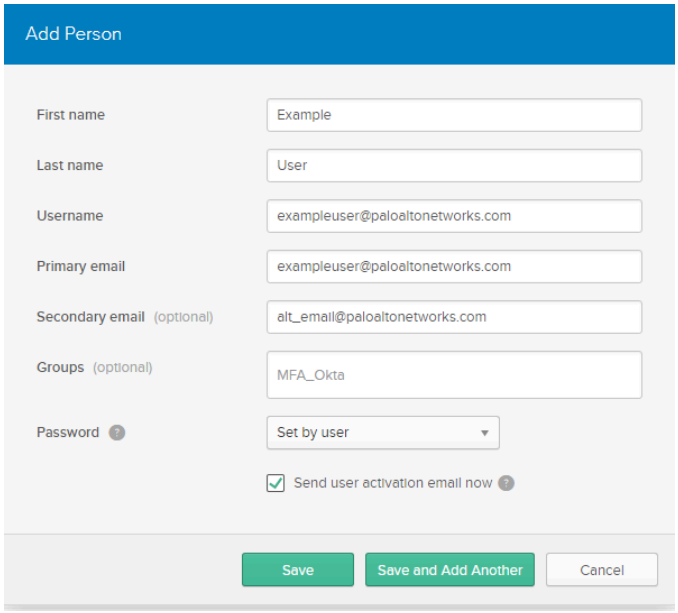



2. Saisissez le **First Name (Prénom)**, **Last Name (Nom)** et **Username (Nom d'utilisateur)** de l'utilisateur. Le nom d'utilisateur doit correspondre à la **Primary email (Adresse électronique principale)**, qui est indiquée automatiquement, ainsi qu'au nom d'utilisateur

saisi sur le pare-feu. Vous pouvez également saisir une adresse électronique de rechange en tant que **Secondary Email (Adresse électronique secondaire)**.




3. Saisissez le nom du groupe ou les **Groups (Groupes)** à associer à cet utilisateur. Lorsque vous commencez à taper, le nom du groupe s'inscrit automatiquement.
4. Cochez **Send user activation email now (Envoyer un message électronique d'activation à l'utilisateur immédiatement)**, puis **Save (Enregistrer)** pour ajouter un seul utilisateur ou **Save and Add Another (Enregistrer et ajouter un autre utilisateur)** pour poursuivre l'ajour d'utilisateurs.

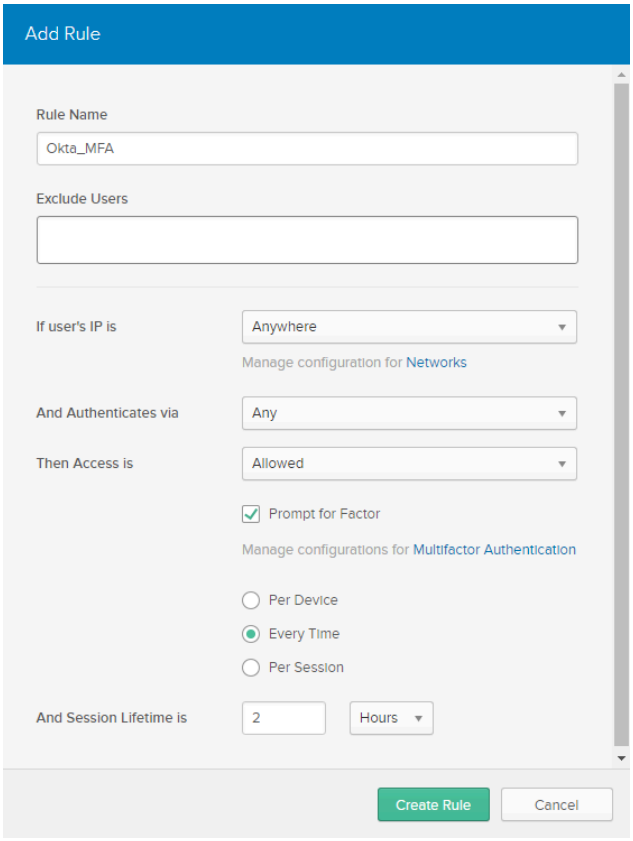
**STEP 5 |** Affectez une politique de test aux utilisateurs.

1. Sélectionnez **Security (Sécurité)** > **Authentication (Authentification)** > **Sign On (Ouverture de session)**.

   Il existe une **Default Policy (Politique par défaut)** avec une **Default Rule (Règle par défaut)** qui n'invite pas les utilisateurs à se connecter au moyen de la MFA.
2. Saisissez le **Rule Name (Nom de la règle)**, puis vérifiez le **Prompt for Factor (Facteur de présentation de l'invite)** pour appliquer l'invite MFA, puis sélectionnez le type d'invite (**Per**

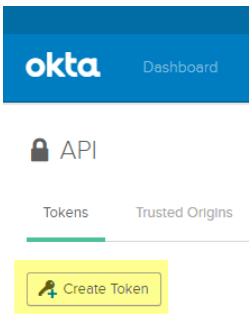
**Device (Par périphérique)**, **Every Time (Toutes les fois)** ou **Per Session (Par session)**), puis **Create Rule (Créez la règle)**.



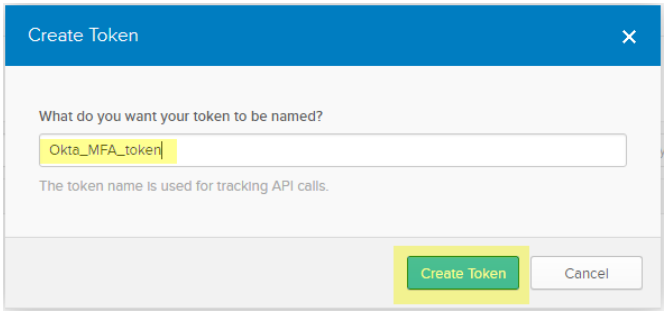

 

**STEP 6 |** Enregistrez les informations sur le jeton d'authentification Okta dans un endroit sûr, car elles ne s'affichent qu'une seule fois.

1. Sélectionnez **Security (Sécurité)** > **API** > **Tokens (Jetons)**.
2. Sélectionnez **Create Token (Créer un jeton)**.

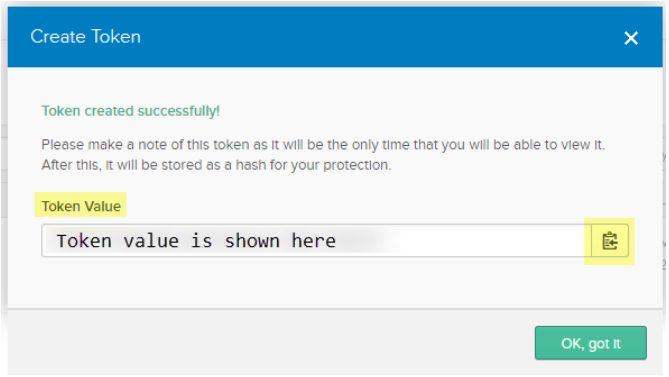



3. Donnez un nom au jeton, puis **Create Token (Créez le jeton)**.

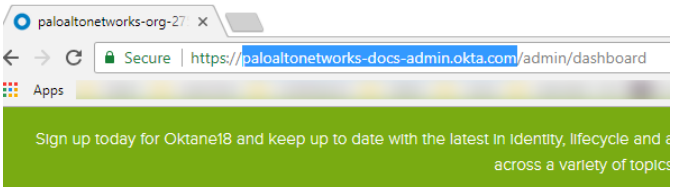



4. Copiez la **Token Value (Valeur du jeton)**.

   Vous pouvez cliquer sur le bouton **Copy to clipboard (Copier et coller dans le presse-papier)** pour copier et coller la valeur de votre jeton dans votre presse-papiers.

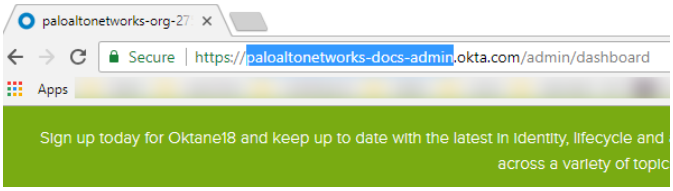



5. Dans l'URL du tableau de bord d'administration d'Okta, copiez la portion de l'URL après **`https://`** jusqu'à **`/admin`** que vous utiliserez en tant que **API host (hôte de l'API)**.




6. Omettez le domaine **`okta.com`** de cette URL pour l'utiliser en tant qu'**Organization (Organisation)**.




Par exemple, dans l'exemple d'URL du tableau de bord d'administration d'Okta ci-dessous, **`https://paloaltonetworks-doc-admin.okta.com/admin/dashboard`** :

- Le nom d'hôte de l'API est **`paloaltonetworks-doc-admin.okta.com`**.
- L'organisation est **`paloaltonetworks-doc-admin`**.

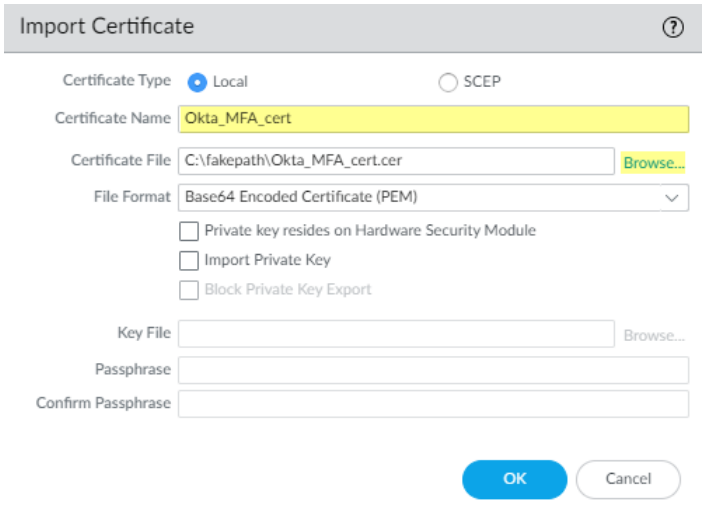
**STEP 7 |** Exportez tous les certificats de la chaîne de certificats au moyen de l'encodage en base 64 :

1. Selon le navigateur que vous utilisez, utilisez l'une des méthodes suivantes pour exporter tous les certificats de la chaîne.
   - **Chrome** : appuyez sur **F12**, puis sélectionnez **Security (Sécurité)** > **View Certificate (Afficher le certificat)** > **Details (Détails)** > **Copy to File (Copier vers le fichier)**.
   - **Firefox** : sélectionnez **Options** > **Privacy & Security (Confidentialité et Sécurité)** > **View Certificates (Afficher les certificats)** > **Export (Exporter)**.
   - **Internet Explorer** : sélectionnez **Settings (Paramètres)** > **Internet Options (Options Internet)** > **Content (Contenu)** > **Certificates (Certificats)** > **Export (Exporter)**.
2. Utilisez l'assistant d'exportation de certificat pour exporter tous les certificats de la chaîne et sélectionnez **Base-64 encoded X.509 (x.509 codé en base-64)** en tant que format.

## Configurez le pare-feu pour l'intégrer à Okta

Avant de commencer, confirmez que vous avez mappé tous les utilisateurs que vous souhaitez authentifier au moyen d'Okta.

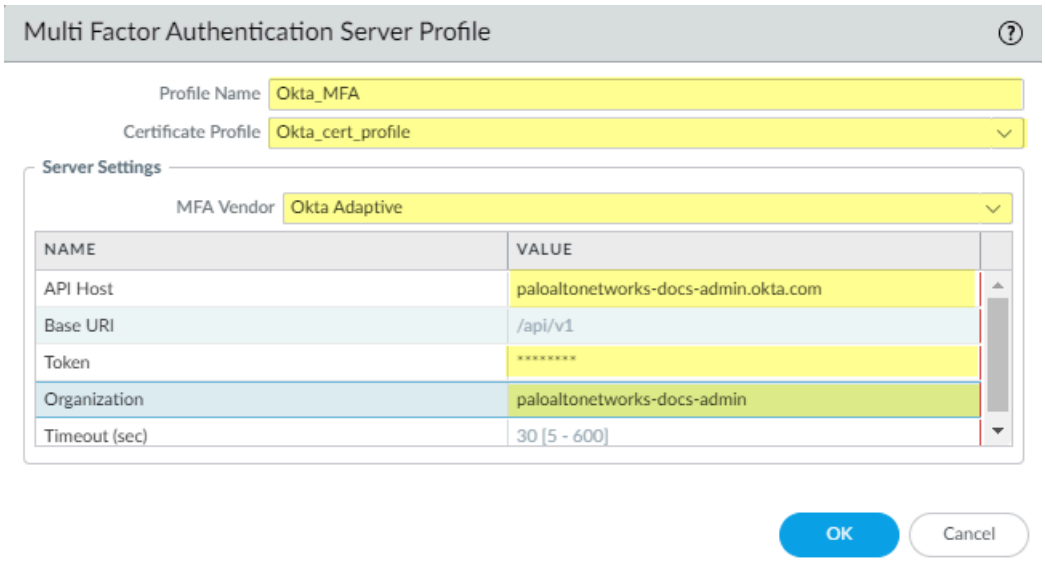
**STEP 1 |** Import (Importez) tous les certificats de la chaîne de certificat sur le pare-feu et ajoutez les certificats importés de l'autorité de certification (racine et intermédiaires) vers un Certificate Profile (Profil de certificat).



**STEP 2 |** Ajoutez un **Multi Factor Authentication Server Profile (Profil de serveur d'authentification multifacteur)** pour Okta.

1. Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveur)** > **Multi Factor Authentication (Authentification multifacteur)**.
2. **Add (Ajoutez)** un profil de serveur MFA.

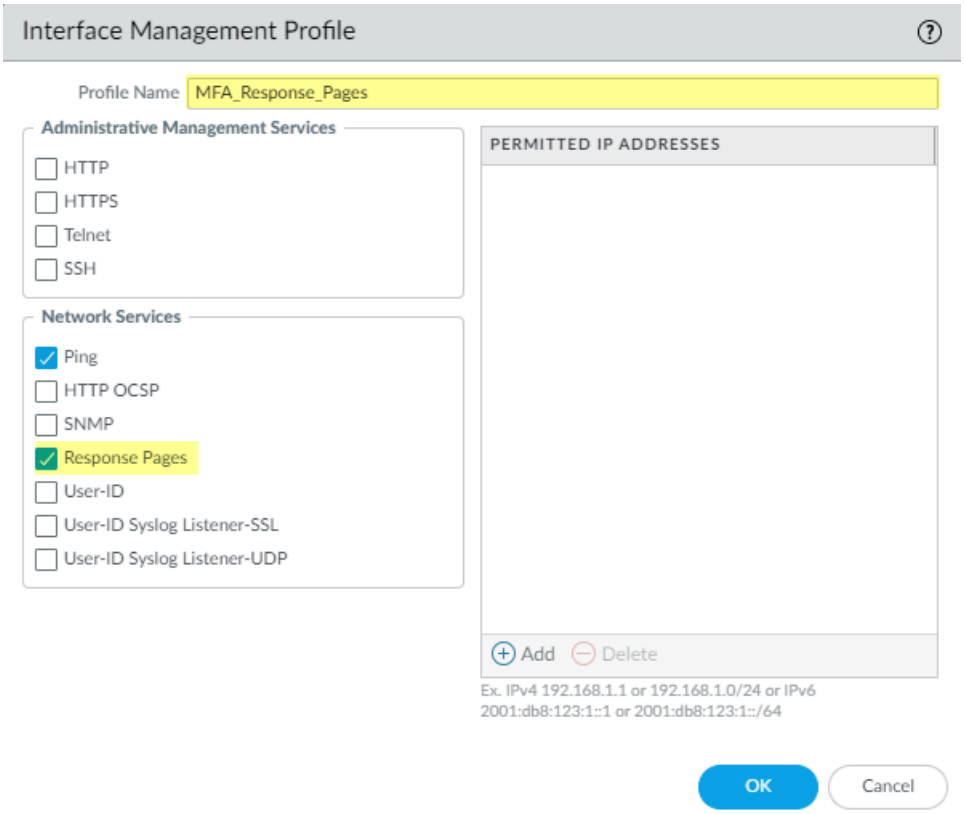



3. Saisissez un **Profile Name (Nom de profil)**.
4. Sélectionnez le **Certificate Profile (Profil de certificat)** que vous avez créé à l'étape 1 de la section Configurer le pare-feu pour l'intégrer à Okta.
5. Sélectionnez **Okta Adaptive** en tant que **MFA Vendor (Fournisseur MFA)**.
6. Saisissez le **API Host (Hôte de l'API)**, le **Token (Jeton)** et la **Organization (Organisation)** à l'étape 4 de la section Configurer le pare-feu pour l'intégrer à Okta.

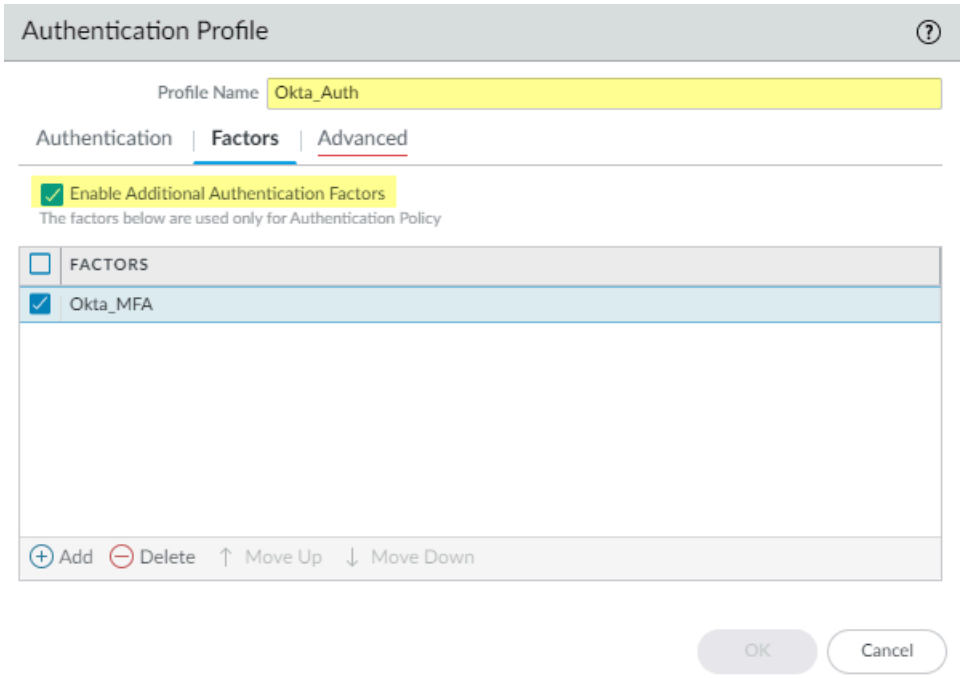
**STEP 3 |** Configurez le portail d'authentification au moyen d'un **Redirect Mode (Mode de redirection)** pour rediriger les utilisateurs vers la demande du fournisseur MFA.

**STEP 4 |** Activez les pages de réponse sur le profil de gestion de l'interface pour rediriger les utilisateurs vers la page de réponses au défi.




**STEP 5 |** Créez un profil d'authentification et ajoutez le fournisseur MFA en tant que **Factor (Facteur)** (voir Configurer l'authentification multifacteur, étape 3.)



**STEP 6 |** Activer User-ID sur la zone source pour demander aux utilisateurs pour répondre à la demande au moyen de votre fournisseur MFA.

**STEP 7 |** Créez un objet d'application de l'authentification pour utiliser le fournisseur MFA et créez une règle de politique d'authentification (reportez-vous à la section Configuration de la politique d'authentification, étapes 4 et 5).

**STEP 8 |** **Commit (Validez)** vos modifications.

### Vérifiez la MFA au moyen d'Okta

**STEP 1 |** Vérifiez que vos utilisateurs ont reçu leur message électronique d'inscription, ont activé leurs comptes et ont téléchargé l'application Okta Verify sur leurs périphériques.

**STEP 2 |** Allez à un site Web qui affiche la page de réponse à une demande d'authentification.

> ***Si vous utilisez un certificat auto-signé au lieu d'un certificat affecté à une PKI de votre organisation, un avertissement de sécurité s'affiche et invite l'utilisateur à cliquer pour accéder à la demande.***

**STEP 3 |** Connectez-vous à la page de réponse en utilisant vos informations d'identification d'Okta.

**STEP 4 |** Confirmez que le périphérique a reçu la notification poussée du défi.

**STEP 5 |** Confirmez que les utilisateurs peuvent accéder à la page après avoir authentifié la demande en acceptant la notification poussée sur leurs périphériques.

## Configuration de la MFA entre Duo et le pare-feu

L'authentification multifacteur vous permet de protéger les ressources de l'entreprise en utilisant des facteurs multiples pour vérifier l'identité des utilisateurs avant de l'autoriser à accéder aux ressources du réseau. Il existe plusieurs façons d'utiliser le service de gestion d'identité Duo pour s'authentifier auprès d'un pare-feu :

- L'authentification à deux facteurs pour les connexions VPN au moyen de la passerelle GlobalProtect et un profil RADIUS (pris en charge sur PAN-OS 7.0 et les versions ultérieures).
- L'intégration basée sur l'API au moyen du portail d'authentification et d'un profil de serveur MFA (aucun proxy d'authentification DUO ou IdP SAML requis - pris en charge sur PAN-OS 8.0 et toute version ultérieure).
- Intégration SAML pour les serveurs sur site (pris en charge sur PAN-OS 8.0 et toute version ultérieure).

Pour activer la SAML MFA entre le pare-feu et Duo pour sécuriser l'accès administratif au pare-feu :

- Configurer DUO pour la SAML MFA avec une passerelle d'accès Duo
- Configurer le pare-feu pour l'intégrer à Duo
- Vérifier la MFA au moyen de Duo

### Configurer DUO pour la SAML MFA avec une passerelle d'accès Duo

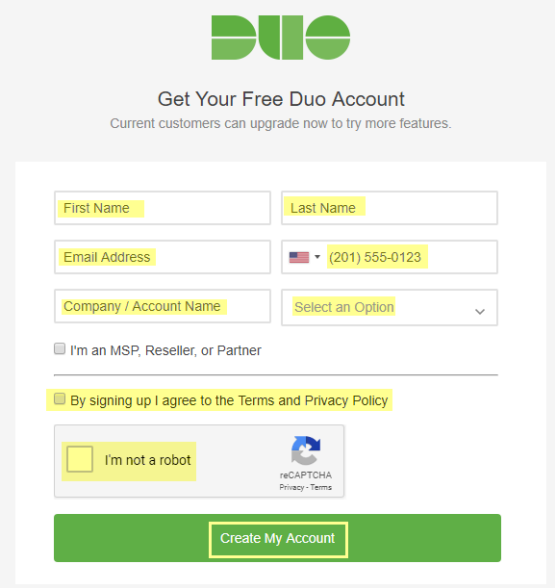
Avant de commencer, vérifiez que vous avez déployé la DuoAccessGateway (passerelle d'accès Duo ; DAG) sur un serveur sur site dans votre zone DMZ.

Créez votre compte administrateur Duo et configurez la passerelle d'accès Duo pour authentifier vos utilisateurs avant qu'ils ne puissent accéder aux ressources.

**STEP 1 |** Créez votre compte administrateur Duo.

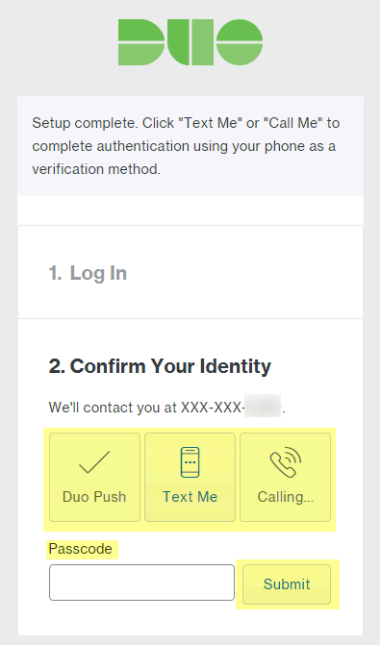
1. À la page de création de compte Duo, saisissez votre **First Name (Prénom)**, **Last Name (Nom)**, **Email Address (Adresse électronique)**, **Cell Phone Number (Numéro de téléphone cellulaire)**, **Company / Account Name (Nom de compte / de société)**, puis sélectionnez le nombre d'employés au sein de l'organisation.
2. Acceptez les Modalités et la politique de confidentialité et répondez à la demande reCAPTCHA pour la **Create My Account (Création de mon compte)**.



**STEP 2 |** Vérifiez votre compte administrateur Duo.

1. Sélectionnez la méthode de vérification de l'authentification (**Duo Push (Appliquée par Duo)**, **Text Me (Me Texter)** ou **Calling... (Appeler...)**).
2. Entrez le **Passcode (Code secret)** que vous recevez et **Submit (Soumettez)**-le pour vérifier votre compte.

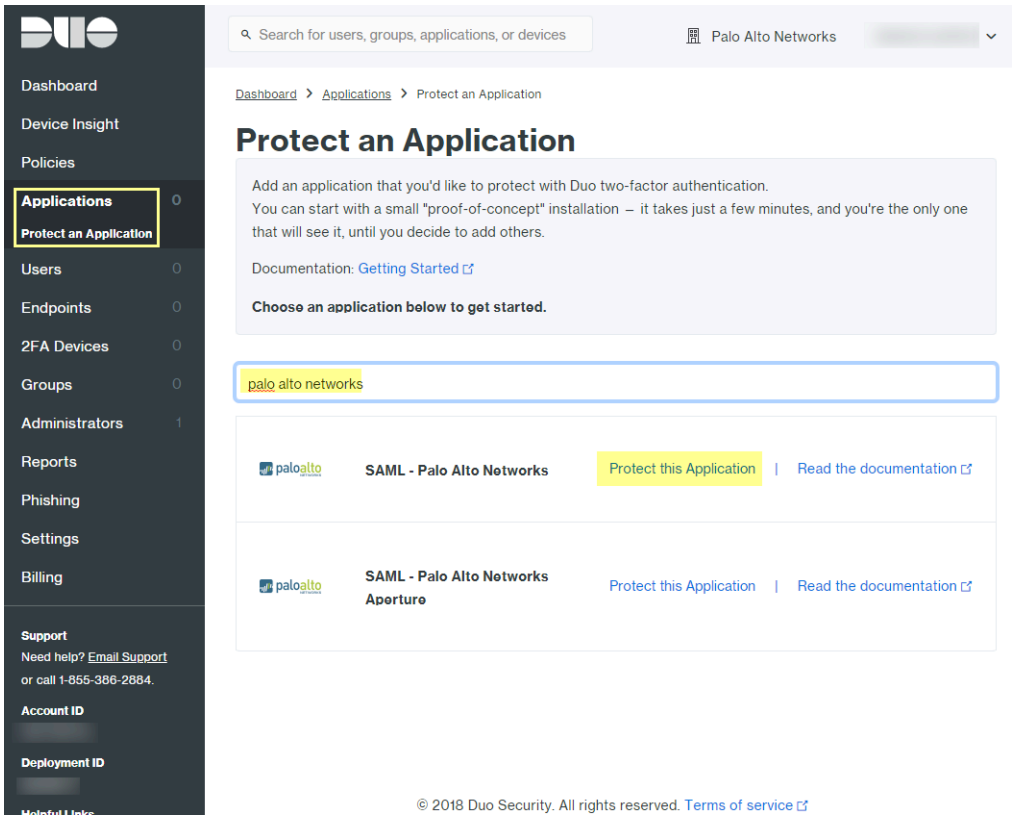


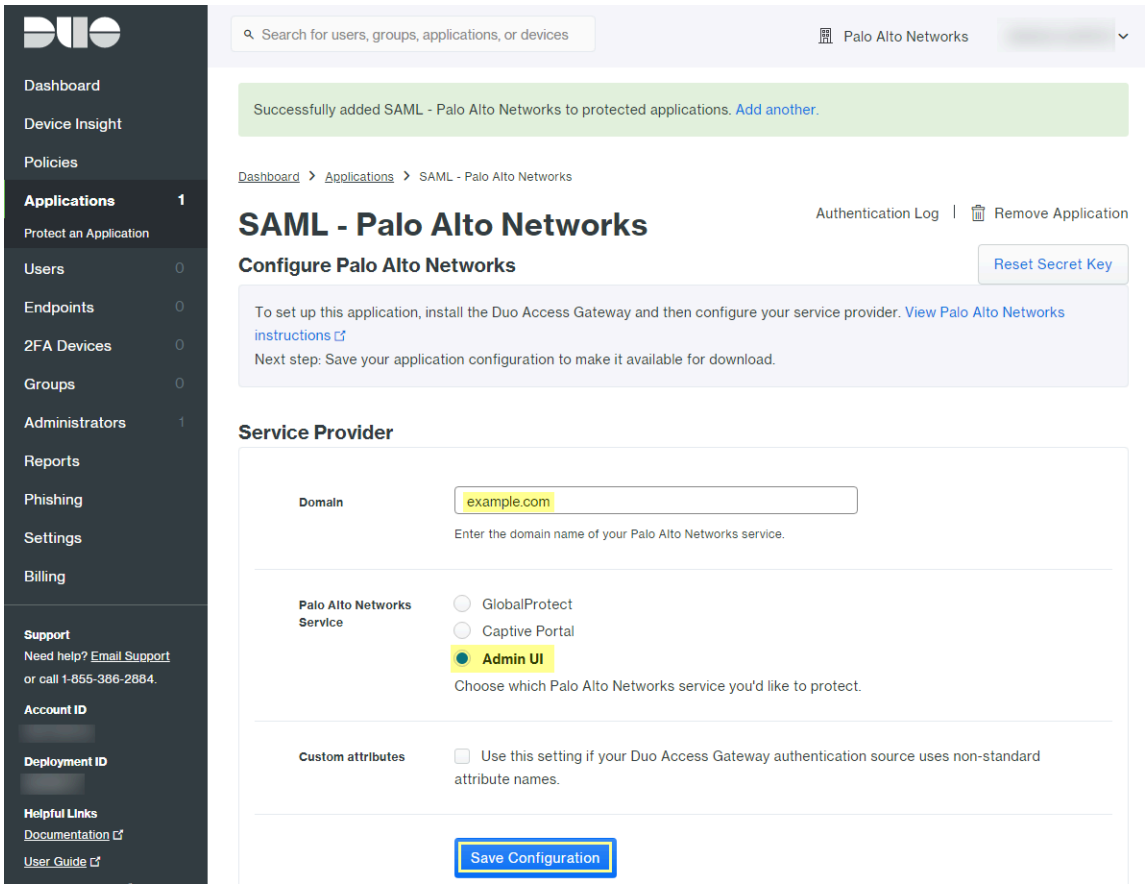
**STEP 3 |** Configurer votre service Duo pour SAML

Après avoir créé votre configuration, téléchargez le fichier de configuration au haut de la page.

1. Dans le panneau Duo Admin (Administration Duo), sélectionnez **Applications** > **Protect an Application (Protéger une application)**.
2. Saisissez **`Palo Alto Networks`** pour chercher les applications.
3. Trouvez **SAML - Palo Alto Networks** dans la liste des résultats, puis **Protect this Application (Protégez cette application)**.

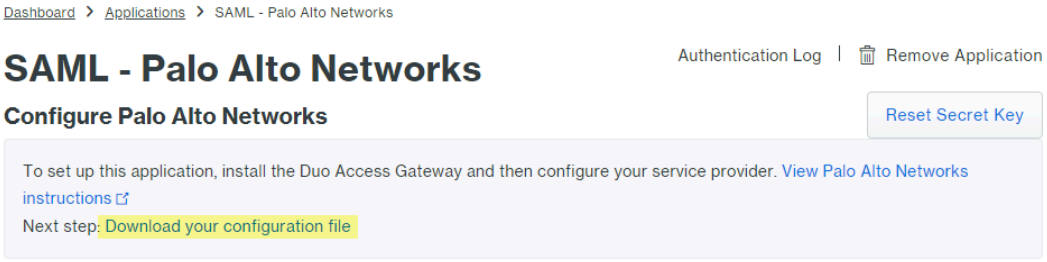



4. Saisissez le **Domain (Domaine)**.
5. Sélectionnez **Admin UI (IU Admin)** en tant que **Palo Alto Networks Service (Service Palo Alto Networks)**.
6. Configurez votre **Policy (Politique)** et vos autres **Settings (Paramètres)**, puis **Save Configuration (Enregistrez la configuration)**.




7. **Download your configuration file (Téléchargez votre fichier de configuration)**.

   Le lien vous permettant de télécharger le fichier se trouve au haut de la page.




**STEP 4 |** Chargez le fichier de configuration dans la Duo Access Gateway (Passerelle d'accès Duo ; DAG).

1. Dans la console d'administration de la DAG, sélectionnez **Applications**.
2. Cliquez sur **Choose File (Choisir le fichier)**, puis sélectionnez le fichier de configuration que vous avez téléchargé, puis **Upload (Chargez)**-le.
3. Sous **Settings (Paramètres)** > **Session Management (Gestion de sessions)**, désactivez la **User agent binding (liaison de l'agent Utilisateur)**, puis **Save Settings (Enregistrez les paramètres)**.

**STEP 5 |** Dans la console d'administration de la DAG, configurez votre serveur Active Directory ou OpenLDAP en tant que source d'authentification et téléchargez le fichier de métadonnées.

1. Connectez-vous à la console d'administration de la DAG.
2. Sous **Authentication Source (Source d'authentification)** > **Set Active Source (Définir la source active)**, sélectionnez votre **Source type (Type de source)** (Active Directory ou OpenLDAP), puis **Set Active Source (Définissez la source active)**.
3. Sous **Configure Sources (Configurez les sources)**, saisissez les **Attributes (Attributs)**.
   - Pour Active Directory, saisissez **`mail,sAMAccountName,userPrincipalName,objectGUID`**.
   - Pour OpenLDAP, saisissez **`mail,uid`**.
   - Ajoutez les attributs personnalisés à la fin de la liste et séparez chaque attribut au moyen d'une virgule. Ne supprimez pas les attributs existants.
4. Cliquez sur **Save Settings (Enregistrer les paramètres)** pour enregistrer la configuration.
5. Sélectionnez **Applications** > **Metadata (Métadonnées)**, puis cliquez sur **Download XML metadata (Télécharger le fichier XML contenant les métadonnées)** pour télécharger le fichier de métadonnées XML que vous devrez importer dans le pare-feu.

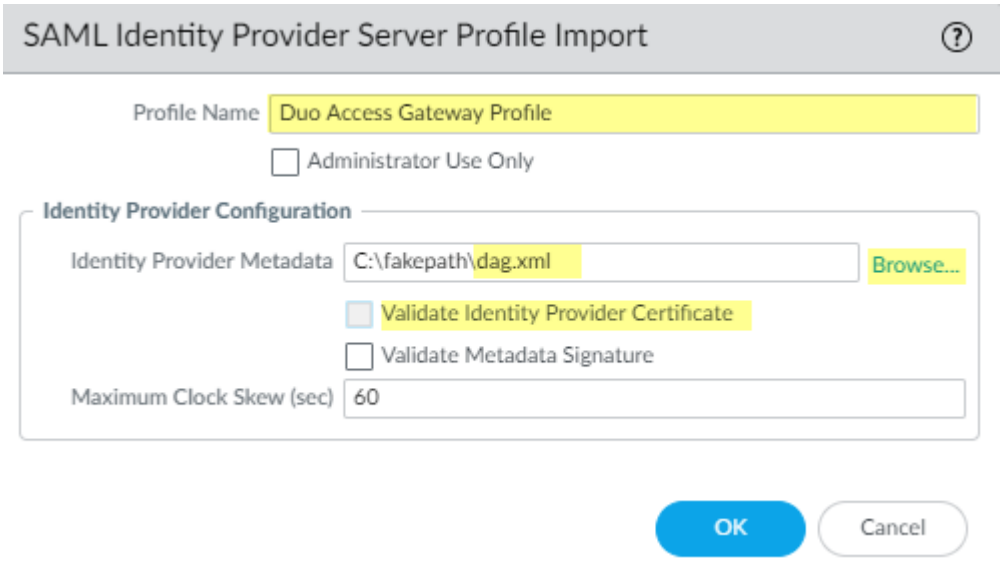
   Le nom du fichier sera named dag.xml. Puisque ce fichier contient des informations sensibles permettant d'authentifier votre compte Duo auprès du pare-feu, assurez-vous de conserver le fichier dans un emplacement sûr afin d'éviter le risque de compromettre ces informations.

## Configurer le pare-feu pour l'intégrer à Duo

**STEP 1 |** Importez les métadonnées de Duo.

1. Connectez-vous à l'interface Web du pare-feu.
2. Sur le pare-feu, sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveur)** > **SAML Identity Provider (Fournisseur d'identité SAML)** > **Import (Importer)**.
3. Saisissez le **Profile Name (Nom de profil)**.
4. **Browse (Accédez)** au fichier **Identity Provider Metadata (De métadonnées du fournisseur d'identité)** (**dag.xml**).
5. Si la passerelle d'accès Duo fournit un certificat auto-signé comme certificat de signature de l'IdP, vous ne pouvez **valider le certificat du fournisseur d'identité**. Dans ce cas, assurez-vous d'utiliser PAN-OS 10.1 pour éviter l'exposition au CVE-2020-2021.

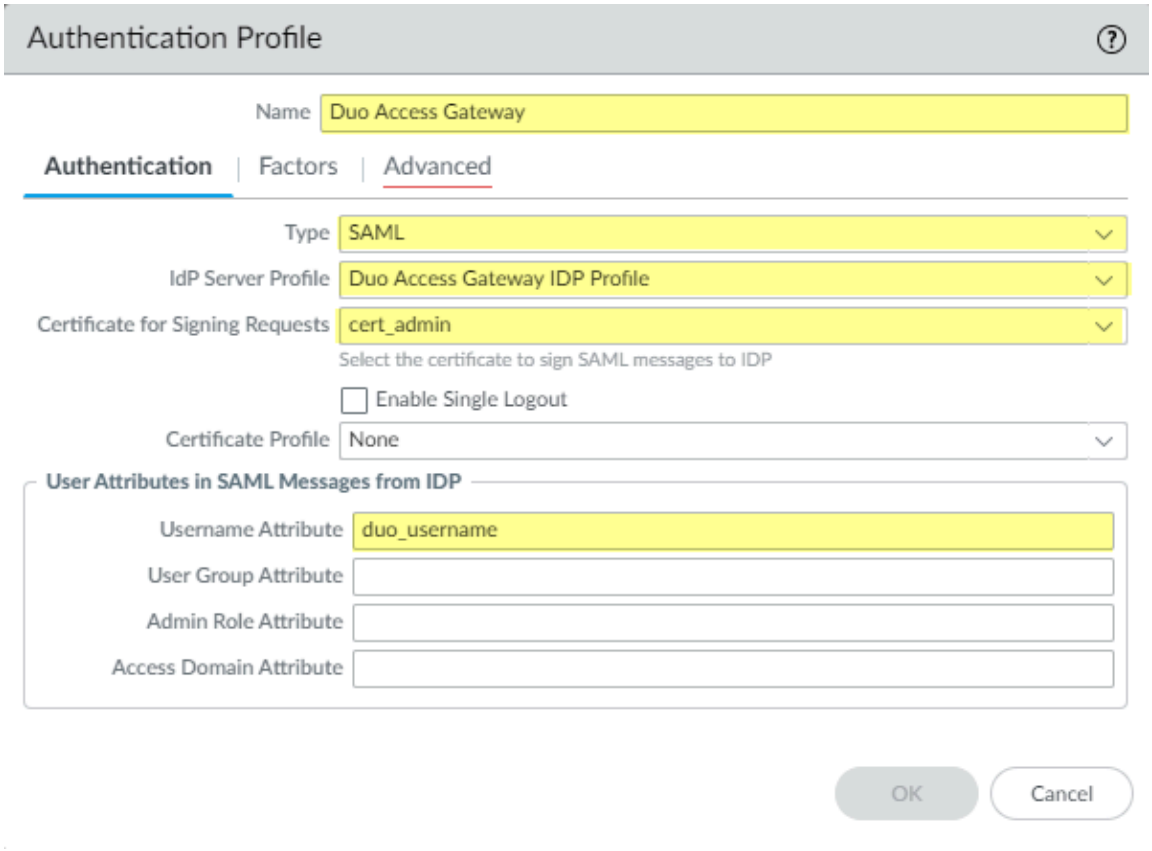


**STEP 2 |** Ajoutez un profil d'authentification.

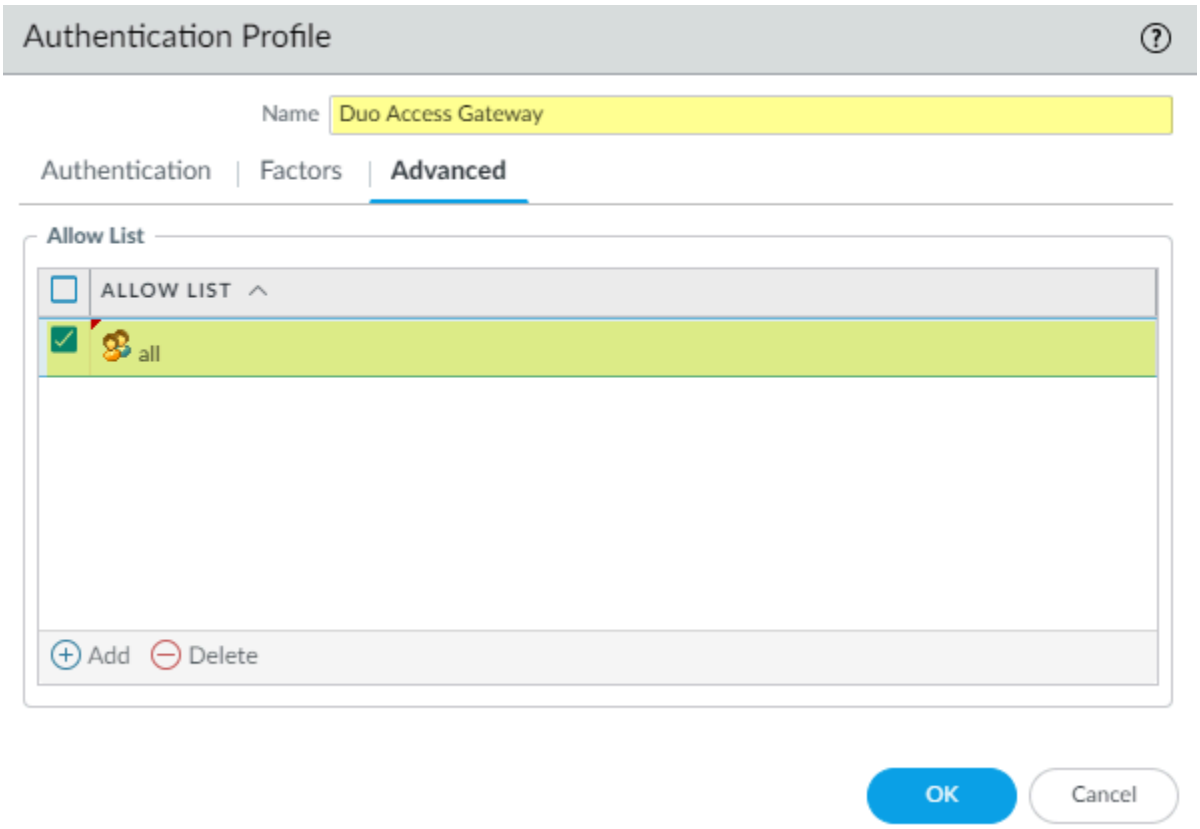
Le profil d'authentification permet à Duo de faire office de fournisseur d'identité pour valider les informations d'identification de l'administrateur.

1. **Add (Ajoutez)** un **Authentication Profile (Profil d'authentification)**.
2. Saisissez le **Name (Nom)** de profil.
3. Sélectionnez **SAML** en tant que **Type** d'authentification.
4. Sélectionnez le **Duo Access Gateway Profile (Profil de la passerelle d'accès Duo)** en tant que **IdP Server Profile (Profil de serveur IdP)**.
5. Sélectionnez le certificat que vous souhaitez utiliser pour la communication SAML avec la passerelle d'accès Duo en tant que **Certificate for Signing Requests (Certificat de signature des demandes)**.
6. Saisissez **`duo_username`** comme **Username Attribute (Attribut de nom d'utilisateur)**.




7. Sélectionnez **Advanced (Avancé)** pour **Add (Ajouter)** une liste d'autorisation.
8. Sélectionnez **all (Tous)**, puis cliquez sur **OK**.
9. **Commit (Validez)** les modifications.

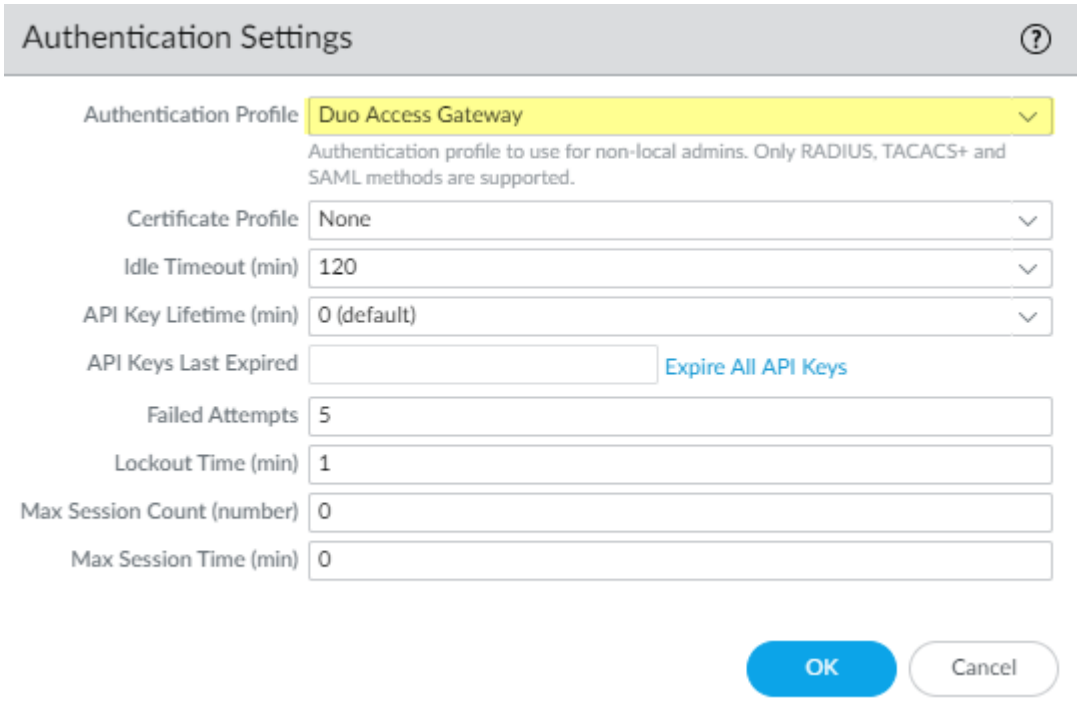
 



**STEP 3 |** Spécifiez les paramètres d'authentification que le pare-feu utilise pour l'authentification SAML avec Duo.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les **Authentication Settings (Paramètres d'authentification)**.
2. Sélectionnez **Duo Access Gateway (Passerelle d'accès Duo)** en tant que **Authentication Profile (Profil d'authentification)**, puis cliquez sur **OK**.




3. **Commit (Validez)** vos modifications.

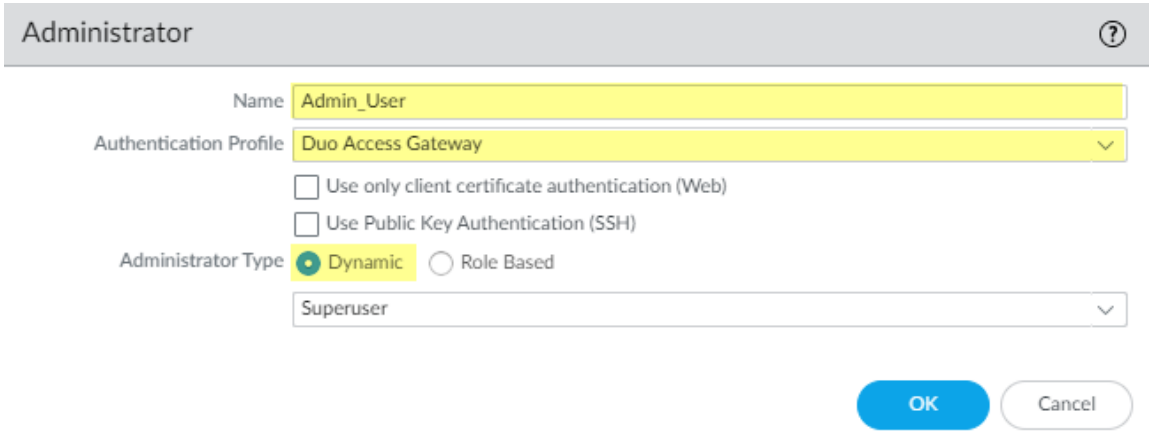
**STEP 4 |** Ajoutez les comptes des administrateurs qui s'authentifieront auprès du pare-feu au moyen de Duo.

1. Sélectionnez **Device (Périphérique)** > **Administrators (Administrateurs)** et **Add (Ajoutez)** un compte.
2. Saisissez un **Name (Nom)** d'utilisateur.
3. Sélectionnez **Duo Access Gateway (Passerelle d'accès Duo)** en tant que **Authentication Profile (Profil d'authentification)**.
4. Sélectionnez le **Administrator Type (Type d'administrateur)**, puis cliquez sur **OK**.

   Sélectionnez **Role Based (En fonction du rôle)** si vous souhaitez utiliser un rôle personnalisé pour l'utilisateur. Sinon, sélectionnez **Dynamic (Dynamique)**. Pour forcer

les administrateurs à se connecter à l'aide de la SSO avec Duo, affectez le profil d'authentification à tous les administrateurs actuels.




## Vérifier la MFA au moyen de Duo

**STEP 1 |** Connectez-vous à l'interface Web du pare-feu.

**STEP 2 |** Sélectionnez **Use Single Sign-on (utilisation de SSO)** sur **Continue (Continuer)**.

**STEP 3 |** Saisissez vos informations d'identification de connexion sur la page de connexion de la passerelle d'accès Duo.

**STEP 4 |** Sélectionnez une méthode d'authentification (notification poussée, appel ou saisie d'un code secret).

Une fois l'authentification réussie, vous serez redirigé vers l'interface Web du pare-feu.

# Configuration de l'authentification SAML

Pour configurer la Single Sign-On (ouverture de session unique ; SSO) SAML et le protocole SAML de Single Logout (déconnexion unique ; SLO), vous devez enregistrer le pare-feu auprès de l'IdP, et vice-versa, pour permettre la communication entre eux. Si l'IdP fournit un fichier de métadonnées qui contient les informations d'enregistrement, vous pouvez l'importer sur le pare-feu pour y enregistrer l'IdP et pour créer un profil de serveur IdP. Le profil de serveur définit comment se connecter à l'IdP et indique le certificat que l'IdP utilise pour signer les messages SAML. Vous pouvez également utiliser un certificat pour la signature des messages SAML par le pare-feu. L'utilisation de certificats est une exigence pour sécuriser les communications entre le pare-feu et l'IdP.

Palo Alto Networks a besoin de HTTPS pour assurer la confidentialité de toutes les transactions SAML plutôt que les approches alternatives, comme les assertions SAML chiffrées. Pour assurer l'intégrité de tous les messages traités dans une transaction SAML, Palo Alto Networks exige des certificats numériques pour signer tous les messages de manière cryptographique.

La procédure présentée ci-dessous décrit la configuration de l'authentification SAML pour les utilisateurs finaux et les administrateurs du pare-feu. Vous pouvez également procéder à la Configuration de l'authentification SAML pour les administrateurs de Panorama.

*La SSO est offerte aux administrateurs ainsi qu'aux utilisateurs finaux de GlobalProtect et du portail d'authentification. Le SLO est accessible aux administrateurs et aux utilisateurs finaux de GlobalProtect, mais pas aux utilisateurs finaux du portail d'authentification.*

*Les administrateurs peuvent utiliser SAML pour s'authentifier sur l'interface Web du pare-feu, mais pas sur la CLI.*

**STEP 1 |** Obtenez les certificats que l'IdP et le pare-feu utiliseront pour signer les messages SAML.

Si les certificats ne précisent pas les attributs d'utilisation des clés, toutes les utilisations sont autorisées par défaut, y compris la signature des messages. Dans ce cas, vous pouvez obtenir les certificats en utilisant la méthode de votre choix.

Si les certificats énumèrent les attributs d'utilisation des clés, l'un des attributs doit être la Signature numérique, qui n'est pas disponible dans les certificats que vous générez sur le pare-feu ou Panorama. Dans ce cas, vous devez importer les certificats :

- **Certificat que le pare-feu utilise pour signer des messages SAML** : importez le certificat de votre Certificate Authority (autorité de certification ; CA) d'entreprise ou d'une CA tierce.
- **Certificat que l'IdP utilise pour signer les messages SAML** (Obligatoire pour tous les déploiements) : importez un fichier de métadonnées qui contient le certificat de l'IdP (voir l'étape suivante). Le certificat IdP se limite aux algorithmes suivants :

  **Algorithmes à clé publique** : RSA (1 024 bits ou plus) et ECDSA (toutes les tailles). Un pare-feu en mode FIPS/CC prend en charge RSA (2 048 bits ou plus) et ECDSA (toutes les tailles).

  **Algorithmes de signature** : SHA1, SHA256, SHA384 et SHA512. Un pare-feu en mode FIPS/CC prend en charge SHA256, SHA384 et SHA512.

**STEP 2 |** Ajoutez un profil de serveur d'IDP en SAML.

Le profil de serveur enregistre l'IdP auprès du pare-feu et définit leur connexion.

Dans cet exemple, vous importez un fichier de métadonnées SAML de l'IdP, pour que le pare-feu puisse automatiquement créer un profil de serveur et renseigner les informations de connexion, d'enregistrement et de certificat IdP.

*Si l'IdP ne fournit pas de fichier de métadonnées, sélectionnez* ***Device (Périphérique) > Server Profiles (Profils de serveur) > SAML Identity Provider (Fournisseur d'identité SAML)***, ***Add (Ajoutez)*** *le profil de serveur et saisissez manuellement les informations (consultez votre administrateur IdP pour connaître les valeurs).*

1. Exportez le fichier de métadonnées SAML de l'IdP vers un système client à partir duquel vous pouvez charger les métadonnées sur le pare-feu.

   Le certificat indiqué dans le fichier doit répondre aux exigences énumérées à l'étape précédente. Consultez votre documentation sur l'IdP pour connaître les instructions relatives à l'exportation du fichier.
2. Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils) de serveur** > **SAML Identity Provider (Fournisseur d'identité SAML)** ou **Panorama** > **Server Profiles (Profils de serveur)** > **SAML Identity Provider (Fournisseur d'identité SAML)** sur Panorama™ et **Import (Importez)** le fichier de métadonnées sur le pare-feu.
3. Saisissez un **Profile Name (Nom de profil)** pour identifier le profil de serveur.
4. **Browse (Accédez)** au fichier **Identity Provider Metadata (De métadonnées du fournisseur d'identité)**.
5. Sélectionnez **Validate Identity Provider Certificate (Valider le certificat du fournisseur d'identité)** pour valider la chaîne de confiance et éventuellement l'état de révocation du certificat de l'IdP.

   Pour activez cette option, une autorité de certificat (CA) doit émettre votre certificat de signature de l'IDP. Vous devez créer un profil de certificat qui a l'autorité de certificat (CA) qui a émis le certificat de signature de l'IdP. Dans le profil d'authentification, sélectionnez le profil du serveur SAML et le profil de certificat pour valider le certificat de l'IdP.

   Si le certificat de signature de l'IdP est un certificat auto-signé, il n'y pas de chaîne de confiance, par conséquent, vous ne pouvez pas activer cette option. Le pare-feu valide toujours la signature des réponses et des assertions SAML auprès du certificat de fournisseur d'identité que vous activiez ou non l'option **Confirmer le certificat du fournisseur d'identité**. Si votre IdP fournit un certificat auto-signé, assurez-vous d'utiliser PAN-OS 10.1 ou une version ultérieure pour éviter l'exposition au CVE-2020-2021.

   *Validez le certificat pour vous assurer qu'il n'a pas été compromis et pour améliorer la sécurité.*
6. Saisissez le **Maximum Clock Skew (Décalage d'horloge maximum)**, c'est-à-dire l'écart en secondes permis entre l'heure système de l'IdP et du pare-feu au moment où le pare-

feu valide les messages IdP (par défaut : 60 ; plage comprise entre 1 et 900). Si l'écart est supérieur à cette valeur, l'authentification échoue.

7. Cliquez sur **OK** pour enregistrer le profil de serveur.
8. Cliquez sur le nom du profil de serveur pour afficher les paramètres du profil. Vérifiez que les informations importées sont justes et modifiez-les, au besoin.
9. Que vous importiez les métadonnées de l'IdP ou que vous saisissiez manuellement les informations de l'IdP, assurez-vous toujours que le certificat de signature de votre fournisseur d'identité SAML correspond au **Identity Provider Certificate (Certificat du fournisseur d'identité)** de votre profil de serveur et que votre IdP envoie des réponses SAML signées et des assertions SAML, ou les deux.

**STEP 3 |** Configurez un profil d'authentification.

Le profil définit les paramètres d'authentification qu'un ensemble d'utilisateurs ont en commun.

1. Sélectionnez **Device (Périphérique)** > **Authentication Profile (Profil d'authentification)** et **Add (Ajoutez)** un profil.
2. Saisissez un **Name (Nom)** pour identifier le profil.
3. Définissez le **Type** sur **SAML**.
4. Sélectionnez le **IdP Server Profile (Profil de serveur IdP)** que vous avez créé.
5. Sélectionnez **Certificate for Signing Requests (Certificat de signature des demandes)**.

   Le pare-feu utilise ce certificat pour signer les messages qu'il envoie à l'IdP. Vous pouvez importer un certificat générer par la CA de votre entreprise ou vous pouvez générer un certificat au moyen de la CA racine qui a été générée sur le pare-feu ou Panorama.
6. (Facultatif) **Enable Single Logout (Activer la déconnexion unique)** (désactivée par défaut).
7. Sélectionnez le **Certificate Profile (Profil de certificat)** que le pare-feu utilise pour valider le **Identity Provider Certificate (Certificat de fournisseur d'identité)**.
8. Entrez le **Username Attribute (Attribut du nom d'utilisateur)** que les messages IdP utilisent pour identifier les utilisateurs (**`username`** par défaut).

   *Lorsque vous définissez des rôles administrateur dynamiques pour les utilisateurs, utilisez des lettres minuscules pour préciser le rôle (par exemple, saisissez **`superreader`**, et non pas **`SuperReader`**). Si vous gérez l'autorisation des administrateurs dans l'annuaire d'identités IdP, indiquez également le **Admin Role Attribute (Attribut du rôle administrateur)** et le **Access Domain Attribute (Attribut du domaine d'accès)**.*
9. Sélectionnez **Advanced (Avancé)** et **Add (Ajoutez)** les utilisateurs et les groupes qui peuvent s'authentifier en utilisant ce profil d'authentification.
10. Cliquez sur **OK** pour enregistrer le profil d'authentification.

**STEP 4 |** Affectez le profil d'authentification aux applications du pare-feu qui exigent l'authentification.

1. Affectez le profil d'authentification :
   - aux comptes administrateur que vous gérez localement sur le pare-feu. Dans cet exemple, procédez à la configuration du compte administrateur du pare-feu avant de vérifier la configuration SAML plus loin dans cette procédure.
   - aux comptes administrateur que vous gérez à l'externe dans l'annuaire d'identités IdP. Select **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)**, modifiez les Authentication Settings (Paramètres d'authentification), puis sélectionnez le **Authentication Profile (Profil d'authentification)** que vous avez configuré.
   - aux règles de politique d'authentification qui sécurisent les services et les applications auxquels les utilisateurs finaux accèdent via le portail d'authentification. Reportez-vous à la section Configuration de la politique d'authentification.
   - aux portails et passerelles GlobalProtect auxquels les utilisateurs finaux accèdent.
2. **Commit (Validez)** vos modifications.

   Le pare-feu valide le **Identity Provider Certificate (Certificat de fournisseur d'identité)** que vous avez affecté au profil de serveur IdP en SAML.

**STEP 5 |** Créez un fichier de métadonnées SAML pour enregistrer l'application du pare-feu (accès de gestion, portail d'authentification ou GlobalProtection) auprès de l'IdP.

1. Sélectionnez **Device (Périphérique)** > **Authentication Profile (Profil d'authentification)**, puis, dans la colonne Authentication (Authentification) associée au profil d'authentification que vous avez configuré, cliquez sur **Metadata (Métadonnées)**.
2. Dans le menu déroulant **Service**, sélectionnez l'application que vous souhaitez enregistrer :
   - **management (gestion)** (par défaut) : accès administrateur à l'interface Web.
   - **Authentication-portal (portail d'authentification)** : accès de l'utilisateur final aux services et aux applications via le portail d'authentification.
   - **global-protect (globalprotect)** : accès de l'utilisateur final aux services et aux applications via GlobalProtect.
3. (Portail d'authentification ou GlobalProtect uniquement) Sous **Vsysname Combo (Nom du système virtuel Combo)**, sélectionnez le système virtuel pour lequel les paramètres du portail d'authentification ou du portail GlobalProtect sont définis.
4. Saisissez l'interface, l'adresse IP ou le nom d'hôte en fonction de l'application à enregistrer :
   - **management (gestion)** : sous **Management Choice (Choix de gestion)**, sélectionnez **Interface (Interface)** (par défaut) et sélectionnez une interface qui permet l'accès de gestion à l'interface Web. L'adresse IP de l'interface MGT est sélectionnée par défaut.
   - **Authentication-portal (portail d'authentification)** : sous **IP Hostname (nom d'hôte IP)**, saisissez l'adresse IP ou le nom d'hôte du **Redirect Host (Hôte de redirection)**

(consultez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Authentication Portal Settings (Paramètres du portail d'authentification)**).

- **global-protect (globalprotect)** : sous **IP Hostname (Nom d'hôte IP)**, saisissez le nom d'hôte ou l'adresse IP de la passerelle ou du portail GlobalProtect.

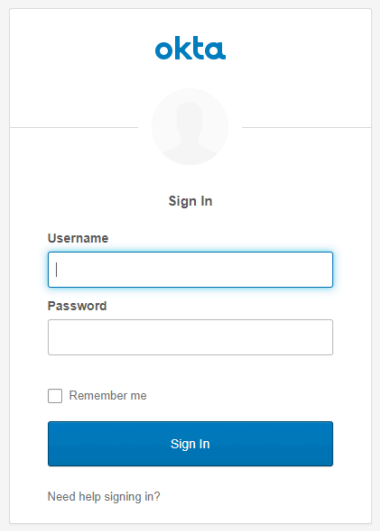
5. Cliquez sur **OK** pour enregistrer le fichier de métadonnées sur votre système client.
6. Importez le fichier de métadonnées sur le serveur IdP pour enregistrer l'application du pare-feu. Pour obtenir des instructions, reportez-vous à la documentation sur IdP.

**STEP 6 |** Vérifiez que les utilisateurs peuvent s'authentifier au moyen de la SSO SAML.

Par exemple, pour vérifier que SMAL fonctionne pour l'accès à l'interface Web à l'aide d'un compte administrateur local :

1. Rendez-vous à l'URL de l'interface Web du pare-feu.
2. Cliquez sur **Use Single Sign-On (Ouverture de session unique)**.
3. Saisissez le nom d'utilisateur de l'administrateur.
4. Cliquez sur **Continue (Continuer)**.

   Le pare-feu vous redirige pour vous demander de vous authentifier à l'IdP, qui présente une page de connexion. Par exemple :




5. Connectez-vous à l'aide de votre nom d'utilisateur et de votre mot de passe SSO.

   Une fois que vous serez authentifié à l'IdP, vous serez redirigé vers le pare-feu, où l'interface Web s'affichera.
6. Utilisez votre compte administrateur du pare-feu pour demander l'accès à une autre application SSO.

   Un accès réussi indique que l'authentification SSO SAML a fonctionné.

# Configuration d'une ouverture de session unique Kerberos

Les pare-feu Palo Alto Networks et Panorama prennent en charge la procédure Single Sign-On (ouverture de session unique ; SSO) Kerberos V5 pour authentifier les administrateurs dans l'interface Web et les utilisateurs finaux dans le portail d'authentification. Lorsque la SSO Kerberos est activée, l'utilisateur doit se connecter uniquement pour un premier accès au réseau (par exemple, une connexion à Microsoft Windows). Ensuite, l'utilisateur pourra accéder à tout service basé sur un navigateur dans le réseau (par exemple, l'interface Web du pare-feu) sans avoir à se reconnecter et jusqu'à l'expiration de la session SSO.

**STEP 1 |** Créez un fichier keytab Kerberos.

Un keytab est un fichier qui contient le nom principal et le mot de passe du pare-feu, il est nécessaire pour le processus SSO. Lorsque vous configurez Kerberos dans votre profil et séquence d'authentification, le pare-feu cherche d'abord un nom d'hôte SSO Kerberos. Si vous indiquez un nom d'hôte, le pare-feu cherche les keytabs d'un nom principal de service qui correspond au nom d'hôte et utilise uniquement ce keytab pour le déchiffrement. Si vous n'indiquez pas de nom d'hôte, le pare-feu essaie chaque keytan de la séquence d'authentification jusqu'à ce qu'il arrive à s'authentifier à l'aide de Kerberos.

*Si le nom d'hôte SSO Kerberos est inclus dans la requête envoyée au pare-feu, le nom d'hôte doit alors correspondre au nom principal du service du keytab ; autrement la requête d'authentification Kerberos n'est pas envoyée.*

1. Connectez-vous au serveur Active Directory et ouvrez une invite de commande.
2. Saisissez la commande suivante pour enregistrer le Service Principal Name (Nom principal du service ; SPN) de GlobalProtect ou du portail d'authentification, où *<portal_fqdn>* et *<service_account_username>* sont variables.

   **setspn -s HTTP/*<fqdn_du_portai>* *<nom d'utilisateur_du_compte_de_service>***
3. Créez un compte Kerberos pour le pare-feu. Pour connaître les étapes à suivre, reportez-vous à la documentation sur Kerberos.
4. Connectez-vous au centre KDC et ouvrez une invite de commande.
5. Saisissez la commande suivante, où *<fqdn_du_portail>*, *<partition_kerberos>*, *<nom_netbios>*, *<nom d'utilisateur_du_compte_de_service>*, *<mot_de_passe>*, *<nom_de_fichier>* et *<algorithme>* sont des variables.

   **ktpass /princ HTTP *<fqdn_du_portail>*@*<partition_kerberos>* / mapuser *<nom_netbios>**<nom d'utilisateur_du_compte_de_service>***

```
/pass <mot_de_passe>/out <nom_du_fichier>.keytab /ptype
KRB5_NT_PRINCIPAL /crypto <algorithme>
```

*La valeur <partition_kerberos> doit être en majuscules (par exemple, saisissez **AD1.EXAMPLE.COM**, et non pas **ad1.example.com**).*

*Si le pare-feu est en mode FIPS/CC, l'algorithme doit être **aes128-cts-hmac-sha1-96** or **aes256-cts-hmac-sha1-96**. Sinon, vous pouvez également utiliser **des3-cbc-sha1 ou arcfour-hmac**. Pour utiliser un algorithme Advanced Encryption Standard (norme de cryptage avancé ; AES), le niveau fonctionnel du KDC doit être Windows Server 2012 ou une version ultérieure et vous devez activer le cryptage AES sur le compte du pare-feu.*

*L'algorithme du keytab doit correspondre à celui du ticket de service que le service TGS génère pour ses clients. Le rôle de votre administrateur Kerberos est de déterminer les algorithmes utilisés par les tickets de service.*

**STEP 2 |** Procédez à la configuration d'un profil et d'une séquence d'authentification pour définir les paramètres Kerberos qu'un ensemble d'utilisateurs ont en commun.

- Saisissez la **Kerberos Realm (Partition Kerberos)** (généralement le domaine DNS des utilisateurs, à la différence que la partition est en majuscules).
- Cliquez sur **Import (Importer)** pour importer le **Kerberos Keytab (Keytab Kerberos)** que vous avez créé pour le pare-feu.

**STEP 3 |** Affectez le profil d'authentification à l'application du pare-feu qui exige l'authentification.

- Accès administratif à l'interface Web : Configuration du compte administrateur du pare-feu et affectez le profil d'authentification que vous avez configuré.
- Accès des utilisateurs finaux aux services et applications : affectez le profil d'authentification que vous avez configuré à un objet de mise en œuvre de l'authentification. Lors de la configuration de l'objet, définissez la **Authentication Method (Méthode d'authentification)** sur **browser-challenge (Navigateur/demande)**. Affectez l'objet à des règles de politique d'authentification. Pour obtenir la procédure de configuration de l'authentification des utilisateurs finaux complète, reportez-vous à la section Configuration de la politique d'authentification.

# Configuration de l'authentification via un serveur Kerberos

Vous pouvez utiliser Kerberos pour authentifier les utilisateurs finaux ainsi que les administrateurs du pare-feu ou de Panorama de manière native auprès d'un contrôleur de domaine Active Directory ou d'un serveur d'authentification compatible avec Kerberos V5. Cette méthode d'authentification est interactive ; les utilisateurs doivent entrer leurs noms d'utilisateur et leurs mots de passe.

*Pour utiliser un serveur Kerberos pour l'authentification, le serveur doit être accessible via une adresse IPv4. Les adresses IPv6 ne sont pas prises en charge.*

**STEP 1 |** Ajoutez un profil de serveur Kerberos.

Le profil définit comment le pare-feu se connecte au serveur Kerberos.

1. Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveur)** > **Kerberos** ou **Panorama** > **Server Profiles (Profils de serveur)** > **Kerberos** sur Panorama™, puis **Add (Ajoutez)** un profil de serveur.
2. Saisissez un **Profile Name (Nom de profil)** pour identifier le profil de serveur.
3. **Add (Ajoutez)** chaque serveur et indiquez un **Name (Nom)** (pour identifier le serveur), l'adresse IPv4 ou le FQDN du **Kerberos Server (Serveur Kerberos)**, ainsi qu'un numéro de **Port (Port)** facultatif pour les communications avec le serveur (par défaut 88).

   *Si vous utilisez un objet d'adresse FQDN pour identifier le serveur et qu'ensuite vous changez l'adresse, vous devez valider le changement pour que la nouvelle adresse du serveur soit appliquée.*
4. Cliquez sur **OK (OK)** pour enregistrer vos modifications du profil.

**STEP 2 |** Affectez le profil du serveur à un profil ou une séquence d'authentification.

Le profil d'authentification définit les paramètres d'authentification qui sont communs à un ensemble d'utilisateurs.

**STEP 3 |** Affectez le profil d'authentification à l'application du pare-feu qui exige l'authentification.

- Accès administratif à l'interface Web : Configuration du compte administrateur du pare-feu et affectez le profil d'authentification que vous avez configuré.
- Accès des utilisateurs finaux aux services et applications : affectez le profil d'authentification que vous avez configuré à un objet de mise en œuvre de l'authentification et affectez l'objet à des règles de politique d'authentification. Pour obtenir la procédure de configuration de l'authentification des utilisateurs finaux complète, reportez-vous à la section Configuration de la politique d'authentification.

**STEP 4 |** Vérifiez que le pare-feu peut procéder à la Vérification de la connectivité du serveur d'authentification pour authentifier les utilisateurs.

# Configuration de l'authentification TACACS+

Vous pouvez configurer l'authentification TACACS+ pour les utilisateurs finaux et le pare-feu ou pour les administrateurs de Panorama. Vous pouvez également utiliser un serveur TACACS + pour gérer l'autorisation des administrateurs (affectation des rôles et des domaines d'accès) en définissant les Vendor-Specific Attributes (Attributs Spécifiques au Fournisseur ; VSA). Pour tous les utilisateurs, vous devez configurer un profil de serveur TACACS+ qui définit la manière dont le pare-feu ou Panorama se connecte au serveur. Vous affectez ensuite le profil de serveur à un profil d'authentification pour chaque ensemble d'utilisateurs qui exigent des paramètres d'authentification communs. Ce que vous faites du profil d'authentification dépend des utilisateurs que le serveur TACACS+ authentifie :

- **Utilisateurs finaux** : affectez le profil d'authentification à un objet de mise en œuvre de l'authentification et affectez l'objet à des règles de politique d'authentification. Pour obtenir la procédure complète, reportez-vous à la section Configuration de la politique d'authentification.
- **Comptes administrateur dont l'autorisation est gérée localement sur le pare-feu ou sur Panorama** : affectez le profil d'authentification aux comptes administrateur du pare-feu ou administrateur de Panorama.
- **Comptes administrateur dont l'autorisation est gérée sur le serveur TACACS+** : la procédure suivante explique la configuration de l'autorisation et de l'authentification TACACS+ pour les administrateurs du pare-feu. Pour les administrateurs de Panorama, reportez-vous à la section Configuration de l'authentification TACACS+ pour les administrateurs de Panorama.

**STEP 1 |** Ajoutez un profil de serveur TACACS+.

Le profil définit comment le pare-feu se connecte au serveur TACACS+.

1. Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveur)** > **TACACS+** ou **Panorama** > **Server Profiles (Profils de serveur)** > **TACACS+** sur Panorama™, puis **Add (Ajoutez)** un profil.
2. Saisissez un **Profile Name (Nom de profil)** pour identifier le profil de serveur.
3. (Facultatif) Sélectionnez **Administrator Use Only (Utilisation par l'administrateur uniquement)** pour restreindre l'accès aux administrateurs uniquement.
4. Saisissez l'intervalle du **Timeout (Délai d'expiration)**, en secondes, après lequel une requête d'authentification arrive à expiration (plage de 1 à 20 ; par défaut 3).
5. Sélectionnez le **Authentication Protocol (Protocole d'authentification)** (par défaut, **CHAP (CHAP)**) que le pare-feu utilise pour s'authentifier au serveur TACACS+.

   *Sélectionnez **CHAP** si le serveur TACACS+ prend en charge ce protocole ; il est plus sécuritaire que **PAP**.*
6. **Add (Ajoutez)** chaque serveur TACACS+ et saisissez les renseignements suivants :
   - Le **Name (Nom)** qui permet d'identifier le serveur.
   - L'adresse IP ou le FQDN du **TACACS+ Server (Serveur TACACS+)**. Si vous utilisez un objet d'adresse FQDN pour identifier le serveur et qu'ensuite vous changez l'adresse,

vous devez valider le changement pour que la nouvelle adresse du serveur soit appliquée.

- Le **Secret** / **Confirm Secret (Phrase secrète / Confirmer une phrase secrète)**, une clé pour chiffrer les noms d'utilisateur et les mots de passe.
- Le **Port** du serveur pour les demandes d'authentification (49 par défaut).

7. Cliquez sur **OK** pour enregistrer le profil de serveur.

**STEP 2 |** Affectez le profil de serveur TACACS+ à un profil d'authentification.

Le profil d'authentification définit les paramètres d'authentification qui sont communs à un ensemble d'utilisateurs.

1. Sélectionnez **Device (Périphérique)** > **Authentication Profile (Profil d'authentification)** et **Add (Ajoutez)** un profil.
2. Saisissez un **Name (Nom)** pour identifier le profil.
3. Définissez le **Type** sur **TACACS+**.
4. Sélectionnez le **Server Profile (Profil de serveur)** que vous avez créé.
5. Sélectionnez **Retrieve user group from TACACS+ (Récupérer le groupe d'utilisateurs auprès de TACACS+)** pour recueillir de l'information sur le groupe d'utilisateurs auprès des VSA définis sur le serveur TACACS+.

   Le pare-feu fait correspondre l'information sur le groupe avec les groupes que vous avez spécifiés dans la liste d'autorisation du profil d'authentification.
6. Sélectionnez **Advanced (Avancé)** et, dans la liste d'autorisation, **Add (Ajoutez)** les utilisateurs et les groupes qui sont autorisés à s'authentifier avec ce profil d'authentification.
7. Cliquez sur **OK** pour enregistrer le profil d'authentification.

**STEP 3 |** Configurez le pare-feu pour utiliser le profil d'authentification pour tous les administrateurs.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Authentication Settings (Paramètres d'authentification).
2. Sélectionnez l'**Authentication Profile (Profil d'authentification)** que vous avez configuré et cliquez sur **OK**.

**STEP 4 |** Configurez les rôles et les domaines d'accès qui définissent les paramètres d'autorisation pour les administrateurs.

Si vous avez déjà défini les VSA de TACACS+ sur le serveur TACACS+, les noms que vous avez indiqués pour les rôles et les domaines d'accès sur le pare-feu doivent correspondre aux valeurs des VSA.

1. Configurez un profil de rôle Administrateur si l'administrateur utilisera un rôle personnalisé plutôt qu'un rôle prédéfini (dynamique).
2. Configurez un domaine d'accès s'il y a plus d'un système virtuel sur le pare-feu : Sélectionnez **Device (Périphérique)** > **Access Domain (Domaine d'accès)**, **Add (Ajoutez)** un domaine d'accès, saisissez un **Name (Nom)** pour identifier le domaine d'accès et **Add (Ajoutez)** chaque système virtuel auquel l'administrateur accédera, puis cliquez sur **OK**.

**STEP 5 |** **Commit (Validez)** les changements que vous avez apportés pour les activer sur le pare-feu.

**STEP 6 |** Configurez le serveur TACACS+ pour l'authentification et l'autorisation des administrateurs.

Reportez-vous à vos documents sur le serveur TACACS+ pour obtenir les directives particulières à suivre pour effectuer ces étapes :

1. Ajoutez l'adresse IP ou le nom d'hôte du pare-feu en tant que client TACACS+.
2. Ajoutez les comptes utilisateur.

   *Si vous avez sélectionné **CHAP** en tant que **Authentication Protocol (Protocole d'authentification)**, vous devez définir les comptes en utilisant* le chiffrement de mots de passe réversible*. Sinon, l'authentification CHAP échouera.*
3. Définissez les VSA de TACACS+ pour les rôles, le domaine d'accès et le groupe d'utilisateurs de chaque administrateur.

   *Lorsque vous définissez des rôles administrateur dynamiques pour les utilisateurs, utilisez des lettres minuscules pour préciser le rôle (par exemple, saisissez **`superuser`**, et non pas **`SuperUser`**).*

**STEP 7 |** Vérifiez que le serveur TACACS+ authentifie et autorise les administrateurs.

1. Connectez-vous à l'interface Web du pare-feu à l'aide d'un compte administrateur que vous avez ajouté au serveur TACACS+.
2. Vérifiez que vous pouvez accéder uniquement aux pages de l'interface Web qui sont autorisées pour le rôle que vous avez associé à l'administrateur.
3. Aux onglets **Monitor (Surveillance)**, **Policies (Politiques)** et **Objects (Objets)**, vérifiez que vous pouvez accéder uniquement aux systèmes virtuels qui sont autorisés pour le domaine d'accès que vous avez associé à l'administrateur.

# Configuration de l'authentification RADIUS

Vous pouvez configurer l'authentification RADIUS pour les utilisateurs finaux et le pare-feu ou pour les administrateurs de Panorama. Pour les administrateurs, vous pouvez également utiliser RADIUS pour gérer l'autorisation (affectation des rôles et des domaines d'accès) en définissant les Vendor-Specific Attributes (Attributs Spécifiques au Fournisseur ; VSA). Vous pouvez également utiliser RADIUS pour mettre en œuvre la Multi-Factor Authentication (authentification multifactorielle ; MFA) pour les administrateurs et les utilisateurs finaux. Pour activer l'authentification RADIUS, vous devez configurer un profil de serveur RADIUS qui définit la manière dont le pare-feu ou Panorama se connecte au serveur (voir l'étape 1 ci-dessous). Vous affectez ensuite le profil de serveur à un profil d'authentification pour chaque ensemble d'utilisateurs qui exigent des paramètres d'authentification communs (voir l'étape 5 ci-dessous). Ce que vous faites du profil d'authentification dépend des utilisateurs que le serveur RADIUS authentifie :

- **Utilisateurs finaux** : affectez le profil d'authentification à un objet de mise en œuvre de l'authentification et affectez l'objet à des règles de politique d'authentification. Pour obtenir la procédure complète, reportez-vous à la section Configuration de la politique d'authentification.

  *Vous pouvez également configurer les systèmes client pour qu'ils envoient les Vendor-Specific Attributes (Attributs spécifiques au fournisseur ;* VSA*) RADIUS au serveur RADIUS en affectant le profil d'authentification à une passerelle ou à un portail GlobalProtect. Les administrateurs RADIUS peuvent alors effectuer des tâches administratives en fonction de ces ASV.*

- **Comptes administrateur dont l'autorisation est gérée localement sur le pare-feu ou sur Panorama** : affectez le profil d'authentification aux comptes administrateur du pare-feu ou administrateur de Panorama.
- **Comptes administrateur dont l'autorisation est gérée sur le serveur RADIUS** : la procédure suivante explique la configuration de l'autorisation et de l'authentification RADIUS pour les administrateurs du pare-feu. Pour les administrateurs de Panorama, reportez-vous à la section Configuration de l'authentification RADIUS pour les administrateurs de Panorama.

**STEP 1 |** Ajoutez un profil de serveur RADIUS.

Le profil définit comment le pare-feu se connecte au serveur RADIUS.

1. Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveur)** > **TACACS+** ou **Panorama** > **Server Profiles (Profils de serveur)** > **TACACS+** sur Panorama™, puis **Add (Ajoutez)** un profil.
2. Saisissez un **Profile Name (Nom de profil)** pour identifier le profil de serveur.
3. (Facultatif) Sélectionnez **Administrator Use Only (Utilisation par l'administrateur uniquement)** pour restreindre l'accès aux administrateurs uniquement.
4. Saisissez l'intervalle du **Timeout (Délai d'expiration)**, en secondes, après lequel une requête d'authentification arrive à expiration (plage de 1 à 120 ; par défaut 3).

   *Si vous utilisez le profil de serveur pour intégrer le pare-feu avec un service MFA, indiquez un intervalle qui donne aux utilisateurs suffisamment de temps pour s'authentifier. Par exemple, si le service MFA demande un One-Time Password (Mot de passe à usage unique ; OTP), les utilisateurs ont besoin de temps pour visualiser l'OTP sur leur périphérique final, puis pour saisir l'OTP sur la page de connexion MFA.*
5. Entrez le numéro de **nouvelles tentatives**.
6. Sélectionnez le **Authentication Protocol (Protocole d'authentification)** (par défaut, **PEAP-MSCHAPv2**) que le pare-feu utilise pour s'authentifier au serveur RADIUS.

   Selon les facteurs que vous souhaitez utiliser pour authentifier les utilisateurs au sein d'un environnement Multi-Factor Authentication (Authentification multifacteur ; MFA), sélectionnez le protocole d'authentification approprié :

   - **Nom d'utilisateur, mot de passe et push (une demande hors bande automatiquement déclenchée)** : pris en charge par tous les protocoles d'authentification.
   - **Push, mot de passe, jeton et PIN (lorsque le mot de passe ou le jeton ou le PIN sont fournis ensemble)** : pris en charge par PAP, PEAP avec GTC et EAP-TTLS avec PAP.
   - **Nom d'utilisateur, mot de passe, jeton et PIN et mécanisme de demande/réponse (lorsque le mot de passe ou le jeton ou le PIN sont fournis ensemble)** : pris en charge par PAP et PEAP avec GTC.

   Si vous sélectionnez une méthode d'authentification EAP (PEAP-MSCHAPv2, PEAP avec GTC ou EAP-TTLS avec PAP), confirmez que votre serveur RADIUS prend en charge le Transport Layer Security (protocole de sécurité de la couche transport ; TLS) 1.1 ou une version ultérieure et que les autorités de certification racine et intermédiaire de votre serveur RADIUS sont incluses dans le profil associé au profil de serveur RADIUS.

Si vous sélectionnez une méthode EAP et que vous n'associez pas de profil de certificat correctement configuré au profil RADIUS, l'authentification échoue.

7. **Add (Ajoutez)** chaque serveur RADIUS et saisissez les renseignements suivants :
   - Le **Name (Nom)** qui permet d'identifier le serveur.
   - L'adresse IP ou le FQDN du **RADIUS Server (Serveur RADIUS)**. Si vous utilisez un FQDN pour identifier le serveur et qu'ensuite vous changez l'adresse, vous devez valider le changement pour que la nouvelle adresse du serveur soit appliquée.
   - **Secret**/**Confirm Secret (Secret/Confirmer le secret)** est une clé qui permet de chiffrer les mots de passe ; elle peut contenir un maximum de 64 caractères de longueur.
   - Le **Port** du serveur pour les demandes d'authentification (1812 par défaut).
8. Cliquez sur **OK** pour enregistrer le profil de serveur.

Pour procurer la redondance, ajoutez plusieurs serveurs RADIUS dans la séquence que vous voulez que le pare-feu utilise. Si vous avez sélectionné une méthode EAP, configurez une séquence d'authentification pour veiller à ce que les utilisateurs soient en mesure de répondre à la demande d'authentification. Avec EAP, il n'existe aucune autre méthode d'authentification : si l'utilisateur ne parvient pas à répondre à la demande d'authentification et que vous n'avez pas configuré de séquence d'authentification qui autorise une autre méthode d'authentification, l'authentification échoue.

**STEP 2 |** SI vous utilisez PEAP-MSCHAPv2 avec GlobalProtect, sélectionnez **Allow users to change passwords after expiry (Autoriser les utilisateurs à modifier les mots de passe après leur expiration)** pour autoriser les utilisateurs de GlobalProtect à modifier les mots de passe expirés lors de la connexion.

**STEP 3 |** (PEAP-MSCHAPv2, PEAP avec GTC ou EAP-TTLS avec PAP uniquement) Pour rendre l'identité de l'utilisateur anonyme dans le tunnel extérieur qui est créé après l'authentification auprès du serveur, sélectionnez **Make Outer Identity Anonymous (Rendre l'identité externe anonyme)**.

*Vous devez configurer le serveur RADIUS pour que la chaîne entière autorise l'accès aux utilisateurs anonymes. Certaines configurations du serveur Radius pourraient ne pas prendre en charge les ID externes anonymes, vous pourriez donc devoir décocher cette option. Lorsque cette option est décochée, le serveur RADIUS transmet les noms d'utilisateur en texte clair.*

**STEP 4 |** Si vous sélectionnez une méthode d'authentification EAP, sélectionnez un Profil de certificat.

**STEP 5 |** Affectez le profil de serveur RADIUS à un profil d'authentification.

Le profil d'authentification définit les paramètres d'authentification qui sont communs à un ensemble d'utilisateurs.

1. Sélectionnez **Device (Périphérique)** > **Authentication Profile (Profil d'authentification)** et **Add (Ajoutez)** un profil.
2. Entrez un **Name (Nom)** pour identifier le profil d'authentification.
3. Définissez le **Type** sur **RADIUS**.
4. Sélectionnez le **Server Profile (Profil de serveur)** que vous avez créé.
5. Sélectionnez **Retrieve user group from RADIUS (Récupérer le groupe d'utilisateurs auprès de TACACS+)** pour recueillir de l'information sur le groupe d'utilisateurs auprès des VSA définis sur le serveur TACACS+.

   Le pare-feu fait correspondre l'information sur le groupe avec les groupes que vous avez spécifiés dans la liste d'autorisation du profil d'authentification.
6. Sélectionnez **Advanced (Avancé)** et, dans la liste d'autorisation, **Add (Ajoutez)** les utilisateurs et les groupes qui sont autorisés à s'authentifier avec ce profil d'authentification.
7. Cliquez sur **OK** pour enregistrer le profil d'authentification.

**STEP 6 |** Configurez le pare-feu pour utiliser le profil d'authentification pour tous les administrateurs.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Authentication Settings (Paramètres d'authentification).
2. Sélectionnez l'**Authentication Profile (Profil d'authentification)** que vous avez configuré et cliquez sur **OK**.

**STEP 7 |** Configurez les rôles et les domaines d'accès qui définissent les paramètres d'autorisation pour les administrateurs.

Si vous avez déjà défini les VSA de RADIUS sur le serveur RADIUS, les noms que vous avez indiqués pour les rôles et les domaines d'accès sur le pare-feu doivent correspondre aux valeurs des VSA.

1. Configurez un profil de rôle Administrateur si l'administrateur utilise un rôle personnalisé plutôt qu'un rôle prédéfini (dynamique).
2. Configurez un domaine d'accès si le pare-feu comporte plusieurs systèmes virtuels :
   1. Sélectionnez **Device (Périphérique)** > **Access Domain (Domaine d'accès)**, **Add (Ajoutez)** un domaine d'accès et saisissez un **Name (Nom)** pour identifier le domaine d'accès.
   2. **Add (Ajoutez)** chaque système virtuel auquel l'administrateur aura accès, puis cliquez sur **OK (OK)**.

**STEP 8 |** **Commit (Validez)** les changements que vous avez apportés pour les activer sur le pare-feu.

**STEP 9 |** Configurez le serveur RADIUS pour l'authentification et l'autorisation des administrateurs.

Reportez-vous à vos documents sur le serveur RADIUS pour obtenir les directives particulières à suivre pour effectuer ces étapes :

1. Ajoutez l'adresse IP ou le nom d'hôte du pare-feu en tant que client RADIUS.
2. Ajoutez les comptes utilisateur.

   *Si le profil de serveur RADIUS indique **CHAP** en tant que **Authentication Protocol (Protocole d'authentification)**, vous devez définir les comptes en utilisant* le chiffrement de mots de passe réversible*. Sinon, l'authentification CHAP échouera.*
3. Définissez le code fournisseur du pare-feu (25461) et définissez les VSA RADIUS du rôle, du domaine d'accès et du groupe d'utilisateurs incombant à chaque administrateur.

   Lorsque vous définissez des rôles administrateur dynamiques pour les utilisateurs, utilisez des lettres minuscules pour préciser le rôle (par exemple, saisissez **`superuser`**, et non pas **`SuperUser`**).

   *Lorsque vous configurez les options de fournisseur avancées dans ACS, vous devez définir la **Vendor Length Field Size (Taille du champ relatif à la longueur du fournisseur)** et la **Vendor Type Field Size (Taille du champ relatif au type de fournisseur)** sur **1**. Sinon, l'authentification échouera.*
4. Si vous avez sélectionné une méthode EAP, le pare-feu valide le serveur, mais pas le client. Pour garantir la validité du client, restreignez les clients selon l'adresse IP ou le sous-domaine.

**STEP 10 |** Vérifiez que le serveur RADIUS authentifie et autorise les administrateurs.

1. Connectez-vous à l'interface Web du pare-feu à l'aide d'un compte administrateur que vous avez ajouté au serveur RADIUS.
2. Vérifiez que vous pouvez accéder uniquement aux pages de l'interface Web qui sont autorisées pour le rôle que vous avez associé à l'administrateur.
3. Aux onglets **Monitor (Surveillance)**, **Policies (Politiques)** et **Objects (Objets)**, vérifiez que vous pouvez accéder uniquement aux systèmes virtuels qui sont autorisés pour le domaine d'accès que vous avez associé à l'administrateur.
4. Sous **Monitor (Surveillance)** > **Authentication (Authentification)**, vérifiez le **Authentication Protocol (Protocole d'authentification)**.
5. Testez la connexion et la validité du profil de certificat au moyen de la commande CLI suivante :

```
admin@PA-220 > test authentication authentication-profile
 auth-profile username <username> password <password>
```

# Configuration de l'authentification LDAP

Vous pouvez utiliser LDAP pour authentifier les utilisateurs finaux qui accèdent aux applications et aux services via le portail d'authentification et pour authentifier les administrateurs du pare-feu ou de Panorama qui accèdent à l'interface Web.

*Vous pouvez également vous connecter à un serveur LDAP pour définir les règles de politique selon des groupes d'utilisateurs. Pour obtenir de plus amples précisions, reportez-vous à la section* Mappage d'utilisateurs à des groupes.

**STEP 1 |** Ajoutez un profil de serveur LDAP.

Le profil définit comment le pare-feu se connecte au serveur LDAP.

1. Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveur)** > **LDAP** ou **Panorama** > **Server Profiles (Profils de serveur)** > **LDAP** sur Panorama™, puis **Add (Ajoutez)** un profil de serveur.
2. Saisissez un **Profile Name (Nom de profil)** pour identifier le profil de serveur.
3. (Multi-vsys uniquement) Sélectionnez le **Location (Emplacement)** dans lequel le profil est disponible.
4. (Facultatif) Sélectionnez **Administrator Use Only (Utilisation par l'administrateur uniquement)** pour restreindre l'accès aux administrateurs uniquement.
5. **Add (Ajoutez)** les serveurs LDAP (maximum de quatre). Donnez un **Name (Nom)** à chaque serveur (pour l'identifier), ainsi qu'une adresse IP de **LDAP Server (Serveur LDAP)** ou un FQDN ainsi que le **Port (Port)** du serveur (valeur par défaut : 389).

   *Si vous utilisez un objet d'adresse FQDN pour identifier le serveur et qu'ensuite vous changez l'adresse, vous devez valider le changement pour que la nouvelle adresse du serveur soit appliquée.*
6. Sélectionnez le **Type (type)** de serveur.
7. Sélectionnez le **Base DN (DN de base)**.

   Pour déterminer le DN de base de votre répertoire, ouvrez les composants logiciels enfichables **Active Directory Domains and Trusts** de Microsoft Management Console et utilisez le nom du domaine de premier niveau.
8. Saisissez le **Bind DN (DN de liaison)** et le **Password (Mot de passe)** pour activer le service d'authentification permettant d'authentifier le pare-feu.

   *Le compte Bind DN doit avoir l'autorisation nécessaire pour consulter le répertoire LDAP.*
9. Entrez le **Bind Timeout (Délai de liaison)** et le **Délai de recherche** en secondes (la valeur par défaut est 30 pour les deux).
10. Saisissez la **Retry Interval (Intervalle de relance)** en secondes (valeur par défaut : 60).
11. Activez l'option visant à **Require SSL/TLS secured connection (Exiger une connexion sécurisée SSL/TLS)** (activée par défaut). Le protocole utilisé par le point de terminaison varie selon le Port de serveur :
    - 389 (par défaut) : TLS (le périphérique utilise plus précisément l'opération StartTLS, qui met à niveau la connexion en texte brut initiale en TLS.)
    - 636 : SSL.
    - Tout autre port : le périphérique tente tout d'abord d'utiliser TLS. Si le serveur d'annuaires ne prend pas en charge TLS, le périphérique fera appel à SSL.
12. (Facultatif) Pour une sécurité supplémentaire, activez l'option **Verify Server Certificate for SSL sessions (Vérifier le certificat du serveur pour les sessions SSL)** afin que le point de terminaison vérifie le certificat que le serveur d'annuaire présente pour les connexions SSL/TLS. Pour activer la vérification, vous devez également activer l'option visant à **Require**

**SSL/TLS secured connection (Exiger une connexion sécurisée SSL/TLS)**. Pour une vérification réussie, le certificat doit remplir l'une des conditions suivantes :

- Il se trouve dans la liste des certificats de périphérique : **Device (Périphérique)** > **Certificate Management (Gestion de certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique).** Si nécessaire, importez le certificat dans le périphérique.
- Le signataire du certificat figure dans la liste des autorités de certification de confiance : **Device (Périphérique)** > **Certificate Management (Gestion de Certificats)** > **Certificates (Certificats)** > **Default Trusted Certificate Authorities (Autorités de certificats fiables par défaut)**.

13. Cliquez sur **OK** pour enregistrer le profil de serveur.

**STEP 2 |** Affectez le profil du serveur pour configurer un profil ou une séquence d'authentification pour définir divers paramètres d'authentification.

**STEP 3 |** Affectez le profil d'authentification à l'application du pare-feu qui exige l'authentification.

- **Accès administratif à l'interface Web** : procédez à la configuration du compte administrateur du pare-feu et affectez le profil d'authentification que vous avez configuré.
- **Accès des utilisateurs finaux aux services et aux applications** : pour obtenir la procédure de configuration de l'authentification des utilisateurs finaux complète, reportez-vous à la section Configuration de la politique d'authentification.

**STEP 4 |** Vérifiez que le pare-feu peut procéder à la Vérification de la connectivité du serveur d'authentification pour authentifier les utilisateurs.

# Délai d'expiration de connexion des serveurs d'authentification

Vous pouvez configurer le pare-feu pour qu'il utilise les services d'authentification externes pour authentifier les administrateurs qui accèdent au pare-feu ou à Panorama et les utilisateurs finaux qui accèdent aux services et aux applications via le portail d'authentification. Pour s'assurer que le pare-feu ne gaspille pas de ressources en tentant continuellement de joindre un serveur d'authentification qui n'est pas joignable, vous pouvez définir un délai d'expiration après lequel le pare-feu cesse d'essayer de se connecter. Vous définissez ce délai dans les profils de serveur qui définissent la manière dont le pare-feu se connecte aux serveurs d'authentification. Lors de la sélection des valeurs d'expiration, votre objectif est d'établir un équilibre entre la nécessité de préserver les ressources du pare-feu et la prise en compte des délais de réseau normaux, lesquels ont une influence sur la vitesse à laquelle les serveurs d'authentification répondent au pare-feu.

- Directives en matière d'établissement des délais d'expiration des serveurs d'authentification
- Modifiez le délai d'expiration du serveur Web de PAN-OS
- Modifiez le délai d'expiration de session du portail

## Directives en matière d'établissement des délais d'expiration des serveurs d'authentification

Vous trouverez ci-dessous des directives concernant l'établissement des délais d'expiration applicables aux tentatives du pare-feu de se connecter aux services d'authentification externe.

- En plus des délais d'expiration que vous définissez dans les profil de serveur de certains serveurs, le pare-feu possède un délai d'expiration global pour le serveur Web de PAN-OS. Ce délai d'expiration global s'applique lorsque le pare-feu se connecte à un serveur externe pour authentifier les administrateurs qui accèdent à l'interface Web du pare-feu ou à l'API XML de PAN-OS ainsi que les utilisateurs finaux qui accèdent aux applications ou services via le portail d'authentification. Par défaut, le délai d'expiration global est de 30 secondes (la plage est comprise entre 3 et 125). Sa valeur doit être équivalente ou supérieure à la durée totale pendant laquelle un profil de serveur autorise les tentatives de connexion. La durée totale définie dans un profil de serveur correspond à la valeur du délai d'expiration multipliée par le nombre de tentatives et par le nombre de serveurs. Par exemple, si un délai d'expiration de trois secondes, trois tentatives et quatre serveurs sont définis pour un profil de serveur RADIUS, la durée totale pendant laquelle le profil autorise les tentatives de connexion est de 36 secondes (3 x 3 x 4). Modifiez le délai d'expiration du serveur Web de PAN-OS, au besoin.

  ***Ne modifiez pas le délai d'expiration du serveur Web de PAN-OS, à moins de constater des échecs d'authentification. Une valeur trop élevée pourrait nuire au rendement du pare-feu ou pourrait entraîner l'abandon des demandes d'authentification. Vous pouvez examiner les échecs d'authentification dans les journaux d'authentification.***

- Le pare-feu applique un délai d'expiration de la session du portail d'authentification qui définit le temps dont disposent les utilisateurs finaux pour répondre à la demande d'authentification qui se trouve dans le formulaire Web du portail d'authentification. Le formulaire Web s'affiche lorsque les utilisateurs demandent des services ou des applications qui correspondent à une règle de la politique d'authentification. Par défaut, le délai d'expiration d'une session est de 30 secondes (la

plage est comprise entre 1 et 1 599 999). La valeur doit être égale ou supérieure à celle indiquée pour le délai d'expiration du serveur Web de PAN-OS. Modifiez le délai d'expiration de session du portail si nécessaire. N'oubliez pas que l'augmentation des délais d'expiration du serveur Web de PAN-OS et de la session du portail d'authentification peut nuire au rendement du pare-feu ou entraîner l'abandon des demandes d'authentification.

***Le délai d'expiration de la session du portail d'authentification n'est pas liée aux minuteurs qui déterminent la durée pendant laquelle le pare-feu conserve les mappages adresse IP/nom d'utilisateur.***

- Les délais d'expiration des séquences d'authentification sont cumulatifs. Par exemple, prenons le cas d'une séquence d'authentification comportant deux profils d'authentification. Un profil d'authentification correspond à un profil de serveur RADIUS disposant d'un délai d'expiration de trois secondes, de trois tentatives et de quatre serveurs. L'autre profil d'authentification correspond à un profil de serveur TACACS+ disposant d'un délai d'expiration de trois secondes et de deux serveurs. La période la plus longue possible pendant laquelle le pare-feu peut tenter d'authentifier des comptes utilisateur au moyen de cette séquence d'authentification est de 42 secondes : 36 secondes pour le profil de serveur RADIUS plus 6 secondes pour le profil de serveur TACACS+.
- Le délai d'expiration non configurable pour les serveurs Kerberos est de 17 secondes pour chaque serveur indiqué dans le profil de serveur Kerberos.
- Pour configurer les délais d'expiration et les paramètres connexes des autres types de serveur, reportez-vous aux sections suivantes :
  - Ajoutez un profil de serveur MFA.
  - Ajoutez un profil de serveur d'IDP en SAML.
  - Ajoutez un profil de serveur TACACS+.
  - Ajoutez un profil de serveur RADIUS.
  - Ajoutez un profil de serveur LDAP.

## Modifiez le délai d'expiration du serveur Web de PAN-OS

Le délai d'expiration du serveur Web PAN-OS doit être égal ou supérieur au délai d'attente dans tout profil de serveur d'authentification multiplié par le nombre de tentatives et le nombre de serveurs dans ce profil.

***Ne modifiez pas le délai d'expiration du serveur Web de PAN-OS, à moins de constater des échecs d'authentification. Une valeur trop élevée pourrait nuire au rendement du pare-feu ou pourrait entraîner l'abandon des demandes d'authentification. Vous pouvez examiner les échecs d'authentification dans les journaux d'authentification.***

**STEP 1 |** Accédez à la CLI du pare-feu.

**STEP 2 |** Définissez le délai d'expiration du serveur Web PAN-OS en entrant les commandes suivantes, où ***<valeur>*** est le nombre de secondes (la valeur par défaut est 30, la plage est comprise entre 3 et 125).

```
> configure
# set deviceconfig setting l3-service timeout <value>
```

```
# commit
```

## Modifiez le délai d'expiration de session du portail

Le délai d'attente de la session du portail d'authentification doit être identique ou supérieur au délai d'expiration du serveur Web PAN-OS. Pour plus de détails, référez-vous à Délais de connexion pour les serveurs d'authentification.

*Plus vous augmentez les délais d'expiration du serveur Web PAN-OS et de session du portail d'authentification, plus la réponse du portail d'authentification aux utilisateurs sera lente.*

**STEP 1 |** Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Session (Session)** et modifiez les délais d'expiration de session.

**STEP 2 |** Entrez une nouvelle valeur de **Authentication Portal (Portail d'authentification)** en secondes (la valeur par défaut est 30, la plage est comprise entre 1 et 1 599 999) et cliquez sur **OK**.

**STEP 3 |** **Commit (Validez)** vos modifications.

# Configuration de l'authentification à l'aide d'une base de données locale

Vous pouvez configurer une base de données d'utilisateurs qui se trouve localement sur le pare-feu pour authentifier les administrateurs qui accèdent à l'interface Web du pare-feu et pour authentifier les utilisateurs finaux qui accèdent aux applications via le portail d'authentification ou GlobalProtect. Procédez comme suit pour configurer l'authentification locale à l'aide d'une base de données locale.

*Il faut généralement préférer les services d'authentification externe aux services d'authentification locale puisqu'ils offrent l'avantage d'une gestion centrale des comptes.*

*Vous pouvez également configurer l'authentification locale sans base de données, mais seulement pour les administrateurs du pare-feu ou de Panorama.*

**STEP 1 |** Ajoutez le compte utilisateur à la base de données locale.

1. Sélectionnez **Device (Périphérique)** > **Local User Database (Base de données d'utilisateurs locale)** > **Users (Utilisateurs)**, puis cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name (Nom)** d'utilisateur pour l'administrateur.
3. Saisissez un **Password (Mot de passe)** et **Confirm Password (Confirmez le mot de passe)** ou saisissez un **Password Hash (Mot de passe haché)**.
4. **Enable (Activez)** le compte (activé par défaut) et cliquez sur **OK (OK)**.

**STEP 2 |** Ajoutez le groupe d'utilisateurs à la base de données locale.

Cette étape est nécessaire si vos utilisateurs doivent appartenir à un groupe.

1. Sélectionnez **Device (Périphérique)** > **Local User Database (Base de données d'utilisateurs locale)** > **User Groups (Groupes d'utilisateurs)**, puis cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name (Nom)** pour identifier le groupe.
3. **Add (Ajoutez)** chaque utilisateur qui appartient au groupe, puis cliquez sur **OK (OK)**.

**STEP 3 |** Configurez un profil d'authentification.

Le profil d'authentification définit les paramètres d'authentification qui sont communs à un ensemble d'utilisateurs. Définissez le **Type (Type)** d'authentification sur la **Local Database (Base de données locale)**.

**STEP 4 |** Affectez le profil d'authentification à un compte administrateur ou à une règle de politique d'authentification pour les utilisateurs finaux.

- **Administrateurs** : Configuration du compte administrateur du pare-feu.

  Précisez le **Name (Nom)** d'un utilisateur que vous avez défini précédemment au cours de cette procédure.

  Affectez le **Authentication Profile (Profil d'authentification)** que vous avez configuré pour le compte.

- **Utilisateurs finaux** : Pour obtenir la procédure de configuration de l'authentification des utilisateurs finaux complète, reportez-vous à la section Configuration de la politique d'authentification.

**STEP 5 |** Vérifiez que le pare-feu peut procéder à la Vérification de la connectivité du serveur d'authentification pour authentifier les utilisateurs.

# Configuration d'un profil et d'une séquence d'authentification

Un profil d'authentification définit le service d'authentification qui valide les informations d'identification des administrateurs qui accèdent à l'interface Web du pare-feu et des utilisateurs finaux qui accèdent aux applications via le portail d'authentification ou GlobalProtect. Il peut s'agir d'un service d'authentification locale fourni par le pare-feu ou de services d'authentification externe. Le profil d'authentification définit également des options comme la Single Sign-On (Ouverture de session unique ; SSO) Kerberos.

Certains réseaux disposent de plusieurs bases de données (par exemple, TACACS+ et LDAP) pour différents utilisateurs et groupes d'utilisateurs. Dans de telles situations, pour authentifier les utilisateurs, configurez une ***séquence d'authentification*** : une liste classée de profils d'authentification à laquelle le pare-feu compare un utilisateur lors de la connexion. Le pare-feu vérifie chaque profil en suivant la séquence établie jusqu'à ce qu'il en atteigne un qui permet d'authentifier l'utilisateur. Un utilisateur se voit refuser l'accès si l'authentification de tous les profils qui figurent dans la séquence d'authentification a échoué. La séquence peut spécifier les profils d'authentification qui sont fondés sur n'importe quel service d'authentification que le pare-feu prend en charge, sauf la Multi-Factor Authentication (authentification à facteurs multiples ; MFA) et le SAML.

**STEP 1 |** (Service externe uniquement) Autorisez le pare-feu à se connecter à un serveur externe pour authentifier les utilisateurs :

1. Configurez le serveur externe. Pour obtenir des instructions, reportez-vous à la documentation sur votre serveur.
2. Configurez un profil de serveur pour le type de service d'authentification que vous utilisez.
   - Ajoutez un profil de serveur RADIUS.

     ***Si le pare-feu s'intègre à un service MFA via RADIUS, vous devez ajouter un profil de serveur RADIUS. Dans ce cas, le service MFA fournit tous les facteurs d'authentification. Si le pare-feu s'intègre à un service MFA via l'API d'un fournisseur, vous pouvez tout de même utiliser un profil de serveur RADIUS pour le premier facteur, mais des profils de serveur MFA sont requis pour les facteurs supplémentaires.***

   - Ajoutez un profil de serveur MFA.
   - Ajoutez un profil de serveur d'IDP en SAML.
   - Ajoutez un profil de serveur Kerberos.
   - Ajoutez un profil de serveur TACACS+.
   - Ajoutez un profil de serveur LDAP.

**STEP 2 |** (Authentification à l'aide d'une base de données locale uniquement) Configurez une base de données d'utilisateurs qui se trouve localement sur le pare-feu.

Effectuez ces étapes pour chaque utilisateur et groupe pour lesquels vous souhaitez configurer l'authentification locale en fonction d'un annuaire d'identités d'utilisateurs qui se trouve localement sur le pare-feu :

1. Ajoutez le compte utilisateur à la base de données locale.
2. (Facultatif) Ajoutez le groupe d'utilisateurs à la base de données locale.

**STEP 3 |** (SSO Kerberos uniquement) Créez un keytab Kerberos pour le pare-feu si la Single Sign-On (ouverture de session unique ; SSO) est le service d'authentification principal.

Créez un fichier keytab Kerberos. Un keytab est un fichier qui contient des informations concernant le compte Kerberos du pare-feu. Pour prendre en charge la SSO Kerberos, votre réseau doit être doté d'une infrastructure Kerberos.

**STEP 4 |** Configurez un profil d'authentification.

Définissez l'une des options suivantes, ou les deux :

- **SSO Kerberos** : le pare-feu essaie d'abord l'authentification SSO. En cas d'échec, il a recours au **Type (Type)** d'authentification indiqué.
- **Authentification externe ou authentification à l'aide d'une base de données locale** : le pare-feu invite l'utilisateur à saisir ces informations d'identification de connexion et utilise un service externe ou une base de données locale pour authentifier l'utilisateur.

1. Sélectionnez **Device (Périphérique)** > **Authentication Profile (Profil d'authentification)** et **Add (Ajoutez)** le nouveau profil d'authentification.
2. Entrez un **Name (Nom)** pour identifier le profil d'authentification.
3. Sélectionnez le **Type (Type)** de service d'authentification.
   - Si vous utilisez l'authentification à plusieurs facteurs, le type sélectionné ne s'applique qu'un premier facteur d'authentification. Vous sélectionnez les services à utiliser pour les autres facteurs MFA à l'onglet **Factors (Facteurs)**.
   - Si vous sélectionnez **RADIUS (RADIUS)**, **TACACS+ (TACACS+)**, **LDAP (LDAP)** ou **Kerberos (Kerberos)**, sélectionnez le **Server Profile (Profil de serveur)**.
   - Si vous sélectionnez **LDAP (LDAP)**, sélectionnez le **Server Profile (Profil de serveur)** et définissez le **Login Attribute (Attribut d'ouverture de session)**. Pour Active Directory, saisissez la valeur **sAMAccountName (sAMAccountName)**.
   - Si vous sélectionnez **SAML (SAML)**, sélectionnez le **IdP Server Profile (Profil de serveur de l'IDP)**.
   - Si vous sélectionnez **Cloud Authentication Service (Service d'authentification Cloud)**, configurez une instance Cloud Identity Engine pour communiquer avec le pare-feu. Pour plus d'informations sur Cloud Identity Engine, consultez le guide de Cloud Identity Engine Getting Started (démarrage de Cloud Identity Engine).
4. Pour activer SSO Kerberos, saisissez la **Kerberos Realm (Partition Kerberos)** (généralement le domaine DNS des utilisateurs, à la différence que la partition est en MAJUSCULES) et

cliquez sur **Import (Importer)** pour importer le **Kerberos Keytab (Keytab Kerberos)** que vous avez créé pour le pare-feu ou pour Panorama.

5. (MFA uniquement) Sélectionnez **Factors (Facteurs)**, **Enable Additional Authentication Factors (Activer les facteurs d'authentification supplémentaires)** et **Add (Ajoutez)** les profils de serveur MFA que vous avez configurés.

   Le pare-feu appellera chaque service MFA dans l'ordre indiqué, de haut en bas.

6. Sélectionnez **Advanced (Avancé)** et **Add (Ajoutez)** les utilisateurs et les groupes qui peuvent s'authentifier en utilisant ce profil.

   Vous pouvez sélectionner des utilisateurs et des groupes dans la base de données locale ou, si vous avez configuré le pare-feu pour qu'il effectue le mappage d'utilisateurs à des groupes, du serveur LDAP, dans un service d'annuaires LDAP, tel qu'Active Directory. Par défaut, la liste est vide, ce qui signifie qu'aucun utilisateur ne peut s'authentifier.

   *Vous pouvez également sélectionner des groupes personnalisés définis dans une configuration de mappage de groupe.*

7. (Facultatif) Pour modifier les informations utilisateur avant que le pare-feu envoi la demande d'authentification au serveur, configurez un **Username Modifier (Modificateur du nom d'utilisateur)**.

   - **%USERDOMAIN%\%USERINPUT% (%DOMAINEUTILISATEUR%\%SAISIEUTILISATEUR%)** : si la source n'inclut pas le domaine (par exemple, il utilise le sAMAccountName), le pare-feu ajoute le **User Domain (Domaine d'utilisateur)** que vous avez spécifié devant le nom d'utilisateur. Si la source inclut le domaine, le pare-feu remplace ce domaine par le **User Domain (Domaine d'utilisateur)**. Si le **User Domain (Domaine d'utilisateur)** est vide, le pare-feu supprime le domaine des informations utilisateur que le pare-feu reçoit de la source avant que le pare-feu envoie la demande au serveur d'authentification.

     *Comme les serveurs LDAP ne prennent pas en charge les barres obliques inverses dans le sAMAccountName, n'utilisez pas cette option pour vous authentifier auprès d'un serveur LDAP.*

   - **%USERINPUT% (%SAISIEUTILISATEUR%)** : (par défaut) Le pare-feu envoie les informations utilisateur au serveur d'authentification dans le format dans lequel il les a reçues de la source.
   - **%USERINPUT%@%USERDOMAIN% (%SAISIEUTILISATEUR%/%DOMAINEUTILISATEUR%)** : si la source n'inclut pas le domaine, le pare-feu ajoute la valeur du **User Domain (domaine d'utilisateur)** après le nom d'utilisateur. Si la source inclut le domaine, le pare-feu remplace ce domaine par le **User Domain (Domaine d'utilisateur)**. Si le **User Domain (Domaine d'utilisateur)** est vide, le pare-feu supprime le domaine des informations utilisateur que le pare-feu reçoit de la source avant que le pare-feu envoie la demande au serveur d'authentification.
   - **Aucun** : si vous saisissez manuellement **None** :
     - Pour les profils de serveur LDAP et Kerberos, le pare-feu utilise le domaine qu'il reçoit de la source pour sélectionner le profil d'authentification approprié, puis supprime le domaine lorsqu'il envoie la demande d'authentification au serveur. Cela vous permet d'inclure le **User Domain (Domaine d'utilisateur)** lors de la séquence d'authentification, mais supprime le domaine avec que le pare-feu envoie la demande

d'authentification au serveur. Par exemple, si vous utilisez un profil de serveur LDAP et le samAccountName en tant qu'attribut, utilisez cette option pour éviter que le pare-feu envoie le domaine au serveur d'authentification qui s'attend à recevoir uniquement un nom d'utilisateur, et non pas un domaine.

- Pour les profils de serveur RADIUS :
  - Si la source envoie les informations d'utilisateur au format **`domain\username`**, le pare-feu envoie les informations d'utilisateur dans le même format au serveur.
  - Si la source envoie les informations d'utilisateur au format **`username@domain`**, le pare-feu normalise les informations d'utilisateur au format **`domain\username`** avant de les envoyer au serveur.
  - Si la source envoie uniquement le nom d'utilisateur, le pare-feu ajoute le **User Domain (Domaine d'utilisateur)** que vous avez spécifié avant d'envoyer les informations au serveur au format **`domain\username`**.
- Pour les bases de données locales, TACACS+ et SAML, le pare-feu envoie les informations utilisateur au serveur d'authentification dans le format dans lequel il les a reçues de la source.

8. Cliquez sur **OK** pour enregistrer le profil d'authentification.

**STEP 5 |** Configurez une séquence d'authentification.

Requis si vous souhaitez que le pare-feu tente plusieurs profils d'authentification pour authentifier les utilisateurs. Le pare-feu évalue les profils de haut en bas jusqu'à ce qu'un profil arrive à authentifier l'utilisateur.

1. Sélectionnez **Device (Périphérique)** > **Authentication Sequence (Séquence d'authentification)** et **Add (Ajoutez)** la séquence d'authentification.
2. Saisissez un **Name (Nom)** pour identifier la séquence d'authentification.

   *Pour faciliter le processus d'authentification, cochez **Use domain to determine authentication profile (Utiliser le domaine pour déterminer le profil d'authentification)** : le pare-feu met en correspondance le nom de domaine saisi par un utilisateur lors de sa connexion avec le **User Domain (Domaine utilisateur)** ou la **Kerberos Realm (Partition Kerberos)** d'un profil d'authentification associé à la séquence, puis utilise ce profil pour authentifier l'utilisateur. Si le pare-feu ne trouve aucune correspondance, ou si vous décochez cette option, le pare-feu essaie les profils de haut en bas.*
3. Cliquez sur **Add (Ajouter)** pour ajouter chaque profil d'authentification. Pour modifier l'ordre d'évaluation des profils, sélectionnez un profil, puis **Move Up (Monter)** ou **Move Down (Descendre)**.
4. Cliquez sur **OK (OK)** pour enregistrer la séquence d'authentification.

**STEP 6 |** Affectez la séquence ou le profil d'authentification à un compte administrateur pour les administrateurs du pare-feu ou à la politique d'authentification pour les utilisateurs finaux.

- **Administrateurs** : affectez le profil d'authentification en fonction du moyen que vous utilisez pour gérer l'autorisation des administrateurs :

  Autorisation gérée localement sur le pare-feu : Configuration du compte administrateur du pare-feu.

  Autorisation gérée sur un serveur SAML, TACACS+ ou RADIUS : Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)**, modifiez les Authentication Settings (Paramètres d'authentification) et sélectionnez le **Authentication Profile (Profil d'authentification)**.

- **Utilisateurs finaux** : Pour obtenir la procédure de configuration de l'authentification des utilisateurs finaux complète, reportez-vous à la section Configuration de la politique d'authentification.

**STEP 7 |** Vérifiez que le pare-feu peut procéder à la Vérification de la connectivité du serveur d'authentification pour authentifier les utilisateurs.

# Configuration de la connectivité du serveur d'authentification

La fonctionnalité d'authentification test vous permet de déterminer si le pare-feu ou Panorama peut communiquer avec le serveur d'authentification défini dans le profil d'authentification et si une requête d'authentification a réussi pour un utilisateur défini. Vous pouvez effectuer des tests sur des profils d'authentification d'administrateurs ayant accès à l'interface web et aux utilisateurs finaux ayant accès aux applications via GlobalProtect ou le portail d'authentification. Vous pouvez effectuer des tests d'authentification sur la configuration candidate pour déterminer si la configuration est correcte avant que vous la validiez.

**STEP 1 |** Configurez un profil d'authentification. Vous n'avez pas besoin de valider la configuration du profil d'authentification ou de serveur préalablement au test.

**STEP 2 |** Connectez-vous à la CLI du pare-feu.

**STEP 3 |** (Pare-feu avec plusieurs systèmes virtuels) Définissez le système virtuel cible auquel la commande test va accéder.

Cette étape est requise pour les pare-feu avec plusieurs systèmes virtuels, afin que la commande d'authentification test puisse localiser l'utilisateur que vous allez tester

Définissez le système virtuel cible en saisissant :

```
admin@PA-325060> set system setting target-vsys <vsys-name>
```

Par exemple, si l'utilisateur est défini dans vsys2, saisissez :

```
admin@PA-3250> set system setting target-vsys vsys2
```

*L'option **target-vsys** est exécutée à chaque session de connexion, car le pare-feu désactive cette option chaque fois que vous vous déconnectez.*

**STEP 4 |** Testez un profil d'authentification en exécutant la commande suivante :

```
admin@PA-3250> test authentication authentication-
profile <authentication-profile-name> username <nom d'utilisateur>
 password
```

Par exemple, pour tester le profil d'authentification nommé **my-profile** d'un utilisateur nommé **bsimpson**, saisissez :

```
admin@PA-3250> test authentication authentication-profile my-
profile username bsimpson password
```

*Lorsque vous saisissez des noms dans la commande **test**, les noms de profils d'authentification et de profils de serveurs sont sensibles à la casse. De même, si un profil d'authentification contient un modificateur de nom d'utilisateur, vous devrez saisir le modificateur avec le nom d'utilisateur. Par exemple, si vous ajoutez le modificateur de nom d'utilisateur **%USERINPUT%@%USERDOMAIN%** pour un utilisateur nommé **bsimpson** et que le nom de domaine est **mydomain.com**, saisissez **bsimpson@mydomain.com** comme nom d'utilisateur. Cela permet de vous assurer que le pare-feu envoie les bons identifiants au serveur d'authentification. Dans cet exemple, mydomain.com est le domaine défini dans le champ **User Domain (Domaine utilisateur)** du profil d'authentification.*

**STEP 5 |** Consultez les résultats du test.

Si le profil d'authentification est correctement configuré, le résultat affichera `Authentication succeeded (authentification réussie)`. En cas de problème de configuration, le résultat affichera des informations pour vous aider à dépanner votre configuration.

*Les résultats varient selon plusieurs facteurs liés au type d'authentification et de problème que vous testez. Par exemple, RADIUS et TACACS+ utilisent plusieurs bibliothèques sous-jacentes, donc un même problème existant générera des erreurs différentes chez ces deux types d'authentifications. De même, en cas de problème réseau, tel que l'utilisation d'un port ou d'une adresse IP incorrect(e) dans le profil du serveur d'authentification, l'erreur générée ne sera pas spécifique, car la commande test ne pourra pas établir de connexion initiale entre le pare-feu et le serveur d'authentification pour fournir des détails sur le problème rencontré.*

# Politique d'authentification

Une politique d'Authentification vous permet d'authentifier les utilisateurs finaux avant qu'ils puissent accéder aux services et aux applications. Chaque fois qu'un utilisateur demande un service ou une application (par exemple lorsqu'il se rend sur une page Web), le pare-feu évalue la politique d'Authentification. En fonction de la règle de la politique d'Authentification de correspondance, le pare-feu invite alors l'utilisateur à s'authentifier au moyen d'une ou de plusieurs méthodes (facteurs), comme la connexion et le mot de passe, la voix, le SMS, la fonction push ou l'authentification du One-time Password (mot de passe à usage unique ; OTP). Pour le premier facteur, les utilisateurs s'authentifient au moyen d'un formulaire Web du portail d'authentification. Pour les autres facteurs, les utilisateurs s'authentifient au moyen d'une page de connexion Multi-Factor Authentication (authentification à plusieurs facteurs ; MFA).

***Pour mettre en œuvre la politique d'authentification de GlobalProtect, reportez-vous à la section Configuration de GlobalProtect pour faciliter les notifications d'authentication à plusieurs facteurs.***

Une fois que l'utilisateur s'authentifie pour tous les facteurs, le pare-feu évalue la politique de sécurité pour déterminer s'il faut autoriser l'accès au service ou à l'application.

Pour réduire la fréquence des demandes d'authentification qui interrompent le flux de travail des utilisateurs, vous pouvez spécifier une période d'expiration au cours de laquelle l'utilisateur s'authentifie uniquement pour un accès initial aux services et aux applications, et non pour les accès subséquents. La politique d'authentification s'intègre au portail d'authentification pour consigner les horodatages utilisés afin d'évaluer le délai d'expiration et d'activer les politiques et les rapports basés sur les utilisateurs.

Selon les informations sur les utilisateurs que le pare-feu recueille au cours de l'authentification, User-ID crée un nouveau mappage d'adresse IP/nom d'utilisateur ou met à jour le mappage qui existe déjà pour cet utilisateur (si les informations de mappage ont changé). Le pare-feu génère des journaux d'User-ID pour consigner les ajouts et les mises à jour. Le pare-feu génère également un journal d'authentification pour chaque requête qui est mise en correspondance avec une règle d'authentification. Si vous préférez la surveillance centralisée, vous pouvez configurer des rapports basés sur User-ID ou des journaux d'authentification et transmettre les journaux à Panorama ou aux services externes, comme vous le feriez pour tout autre type de journal.

- Horodatages d'authentification
- Configuration de la politique d'authentification

## Horodatages d'authentification

Lorsque vous configurez une règle de politique d'authentification, vous pouvez spécifier une période d'expiration au cours de laquelle l'utilisateur s'authentifie uniquement pour un accès initial aux services et aux applications, et non pour les accès subséquents. Votre objectif est de spécifier un délai d'expiration qui permet d'atteindre un équilibre entre la nécessité de sécuriser les services et les applications et la nécessité de minimiser les interruptions du flux de travail des utilisateurs. Lorsqu'un utilisateur s'authentifie, le pare-feu consigne un horodatage pour la première demande d'authentification (facteur) et un horodatage pour tous les autres facteurs de la Multi-Factor Authentication (authentification à facteurs multiples ; MFA). Par la suite, lorsque l'utilisateur demande des services et des applications qui correspondent à une règle d'authentification, le pare-

feu évalue le délai d'expiration spécifié dans la règle et le compare à chaque horodatage. C'est-à-dire qu'à l'expiration du délai, le pare-feu émet de nouvelles demandes d'authentification sur une base pré-factorielle. Si vous procédez à la redistribution des mappages d'utilisateur et des horodatages d'authentification, tous vos pare-feu appliqueront les délais d'expiration de la politique d'authentification de manière uniforme pour tous les utilisateurs.

***Le pare-feu consigne un horodatage distinct pour chaque fournisseur MFA. Par exemple, si vous utilisez des serveurs Duo v2 et PingID pour émettre des demandes aux facteurs MFA, le pare-feu consigne un horodatage pour la réponse au facteur Duo et un horodatage pour la réponse au facteur PingID.***

Au cours du délai d'expiration, un utilisateur qui s'authentifie avec succès à une règle d'authentification peut accéder aux services et aux applications que les autres règles protègent. Cependant, cette portabilité ne s'applique qu'aux règles qui font appel aux mêmes facteurs d'authentification. Par exemple, un utilisateur qui s'authentifie avec succès à une règle qui fait appel à l'authentification TACACS+ doit s'authentifier de nouveau à une règle qui faire appel à l'authentification SAML, même si les demandes d'accès se situent à l'intérieur du délai d'expiration établis pour les deux règles.

Lors de l'évaluation du délai d'expiration de chaque règle d'authentification et du minuteur global défini dans les paramètres du portail d'authentification (voir Configuration du portail d'authentification), le pare-feu invite l'utilisateur à se réauthentifier pour le paramètre qui expire en premier. Une fois que l'utilisateur s'est réauthentifié, le pare-feu consigne les nouveaux horodatages d'authentification pour les règles, et le minuteur du portail d'authentification retombe à zéro. Ainsi, pour permettre l'établissement de divers délais d'expiration applicables à différentes règles d'authentification, définissez le minuteur du portail d'authentification sur une valeur qui est égale ou supérieure à celle fixée pour le délai d'expiration dans toute règle.

## Configuration de la politique d'authentification

Effectuez les étapes suivantes pour configurer la politique d'authentification applicable aux utilisateurs finaux qui accèdent aux services via le portail d'authentification. Avant de commencer, assurez-vous que votre politique de sécurité permet aux utilisateurs d'accéder aux services et aux catégories d'URL qui doivent faire l'objet d'une authentification.

**STEP 1 |** Configuration du portail d'authentification. Si vous utilisez des services d'authentification à facteurs multiples pour authentifier les utilisateurs, vous devez définir le **Mode (Mode)** sur **Redirect (Rediriger)**.

**STEP 2 |** Configurez le pare-feu pour qu'il utilise l'un des services suivants pour authentifier les utilisateurs.

- Services d'authentification externe : configurez un profil de serveur pour définir comment le pare-feu se connecte au service.
- Authentification à l'aide d'une base de données locale : ajoutez chaque compte d'utilisateur à la base de données des utilisateurs locaux qui se trouve sur le pare-feu.
- Single sing-on (Ouverture de session unique ; SSO) Kerberos : créez un keytab Kerberos pour le pare-feu. Vous pouvez éventuellement configurer le pare-feu pour qu'il utilise la SSO Kerberos comme service d'authentification principal et, en cas d'échec de la SSO, un service externe ou l'authentification à l'aide d'une base de données locale.

**STEP 3 |** Procédez à la configuration d'un profil et d'une séquence d'authentification pour chaque ensemble d'utilisateurs et de règles de politique d'authentification qui requiert les mêmes paramètres et services d'authentification.

Sélectionnez le **Type (Type)** de service d'authentification et les paramètres connexes :

- **Service externe** : sélectionnez le **Type (Type)** de serveur externe et sélectionnez le **Server Profile (Profil de serveur)** que vous avez créé pour celui-ci.
- **Authentification à l'aide d'une base de données locale** : définissez le **Type (Type)** sur **Local Database (Base de données locale)**. Dans les paramètres **Advanced (Avancés)**, **Add (Ajoutez)** les utilisateurs du portail d'authentification et les groupes d'utilisateurs que vous avez créés.
- **Kerberos SSO (SSO Kerberos)** : spécifiez la **Kerberos Realm (Partition Kerberos)** et **Import (Importez)** le **Kerberos Keytab (Keytab Kerberos)**.

**STEP 4 |** Configurez un objet de mise en œuvre de l'authentification.

L'objet associe chaque profil d'authentification à une méthode du portail d'authentification. La méthode détermine si la première demande d'authentification (facteur) est transparente ou si elle exige une réponse de l'utilisateur.

1. Sélectionnez **Objects (Objets)** > **Authentication (Authentification)** et **Add (Ajoutez)** un objet.
2. Saisissez un **Name (Nom)** pour identifier l'objet.
3. Sélectionnez une **Authentication Method (Méthode d'authentification)** pour le **Type (Type)** de service d'authentification que vous avez indiqué dans le profil d'authentification :
   - **browser-challenge (défi de navigation)** : sélectionnez cette option si vous voulez que le navigateur client réponde au premier facteur d'authentification plutôt que l'utilisateur soit invité à saisir ses informations d'identification de connexion. Pour cette méthode, vous devez configurer le SSO Kerberos dans le profil d'authentification. En cas d'échec du défi de navigation, le pare-feu revient à la méthode **web-form (formulaire Web)**.
   - **web-form (formulaire Web)** : sélectionnez cette méthode si vous voulez que le pare-feu affiche un formulaire Web du portail d'authentification dans lequel les utilisateurs sont invités à saisir leurs informations d'identification de connexion.
4. Sélectionnez le **Authentication Profile (Profil d'authentification)** que vous avez configuré.
5. Saisissez le **Message (Message)** que le formulaire Web du portail d'authentification affichera pour indiquer aux utilisateurs comment s'authentifier au premier facteur d'authentification.
6. Cliquez sur**OK** pour enregistrer la règle.

**STEP 5 |** Configurez une règle de politique d'authentification.

Créez une règle pour chaque ensemble d'utilisateurs, de services et de catégories URL qui requièrent les mêmes paramètres et services d'authentification.

*Le pare-feu n'applique pas le délai du portail d'authentification si votre politique d'authentification utilise des objets d'application de l'authentification par défaut (par exemple, **default-browser-challenge (défi de navigateur par défaut)**). Pour obliger les utilisateurs à se ré-authentifier après le délai d'expiration du portail d'authentification, clonez la règle pour l'objet d'authentification par défaut et déplacez-la avant la règle existante pour l'objet d'authentification par défaut.*

1. Sélectionnez **Policies (Stratégies)** > **Authentication (Authentification)**, puis **Add (Ajoutez)** une règle.
2. Donnez un **Name (Nom)** à la règle afin de l'identifier.
3. Sélectionnez **Source (Source)** et **Add (Ajoutez)** des zones ou des adresses IP précises ou sélectionnez **Any (Toute)** zone ou adresse IP.

   La règle ne s'applique qu'au trafic provenant des adresses IP indiquées ou des interfaces qui se trouvent dans les zones indiquées.
4. Sélectionnez **User (Utilisateur)**, puis sélectionnez ou **Add (Ajoutez)** les utilisateurs sources et les groupes d'utilisateurs auxquels les règles s'appliquent (par défaut **any (indifférent)**).
5. Sélectionnez ou **Add (Ajoutez)** les profils d'informations sur l'hôte auxquels la règle s'applique (par défaut **any (indifférent)**).
6. Sélectionnez **Destination (Destination)** et **Add (Ajoutez)** des zones ou des adresses IP précises ou sélectionnez **Any (Toute)** zone ou adresse IP.

   Les adresses IP peuvent être des ressources (comme des serveurs) auxquelles vous souhaitez contrôler l'accès.
7. Sélectionnez **Service/URL Category (Service/Catégorie d'URL)**, puis sélectionnez ou **Add (Ajoutez)** les services et groupes de services auxquels la règle contrôle l'accès (par défaut **service-http (service-http)**).
8. Sélectionnez ou **Add (Ajoutez)** les catégories d'URL auxquelles la règle contrôle l'accès (par défaut **any (indifférent)**). Par exemple, vous pouvez créer une catégorie d'URL personnalisée qui spécifie vos sites internes les plus sensibles.
9. Sélectionnez **Actions (Actions)**, puis sélectionnez l'objet de **Authentication Enforcement (Mise en œuvre de l'authentification)** que vous avez créé.
10. Indiquez la période de **Timeout (Temporisation)** en minutes (par défaut 60) au cours de laquelle le pare-feu invite l'utilisateur à s'authentifier une seule fois pour un accès récurrent aux services et aux applications.

    *Le **Timeout (Délai d'expiration)** est un compromis entre une sécurité plus stricte (période plus courte entre les invites d'authentification) et l'expérience utilisateur (période plus longue entre les invites d'authentification). Une authentification plus fréquente est souvent le choix le plus indiqué pour accéder aux systèmes critiques et aux zones sensibles, comme un centre de données. Une authentification moins fréquente est souvent indiquée au périmètre du réseau de même que pour les entreprises pour lesquelles l'expérience utilisateur est clé.*

11. Cliquez sur **OK** pour enregistrer la règle.

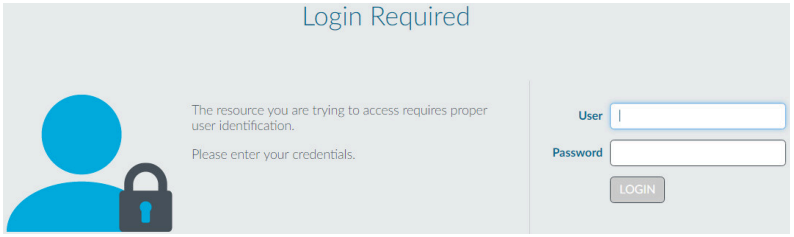
**STEP 6 |** (MFA uniquement) Personnalisez la page de connexion MFA.

Le pare-feu affiche cette page pour que les utilisateurs puissent s'authentifier aux autres facteurs de la MFA.

**STEP 7 |** Vérifiez que le pare-feu met en œuvre la politique d'authentification.

1. Connectez-vous à votre réseau en utilisant les informations d'identification de l'un des utilisateurs source indiqués dans une règle de politique d'authentification.
2. Demandez un service ou une catégorie d'URL qui correspond à l'une des règles indiquées.

   Le pare-feu affiche le formulaire Web du portail d'authentification correspondant au premier facteur d'authentification. Par exemple :




   ***Si vous avez configuré le pare-feu pour qu'il utilise un ou plusieurs services MFA, authentifiez-vous aux autres facteurs d'authentification.***
3. Mettez fin à la session du service ou de l'URL auquel vous venez d'accéder.
4. Commencez une nouvelle session pour ce même service ou cette même application. Assurez-vous d'effectuer cette étape dans la période de **Timeout (Temporisation)** que vous avez configurée dans la règle d'authentification.

   Le pare-feu autorise l'accès sans que vous ayez à vous authentifier de nouveau.
5. Attendez que la période de **Timeout (Temporisation)** soit écoulée et demandez l'accès au même service ou à la même application.

   Le pare-feu vous invite à vous authentifier de nouveau.

**STEP 8 |** (Facultatif) Redistribution des données et horodatages d'authentification aux autres pare-feu qui mettent en œuvre la politique d'authentification afin de vous assurer qu'ils appliquent les périodes de temporisation de manière uniforme pour tous les utilisateurs.

# Dépannage des problèmes d'authentification

Lorsque les utilisateurs ne parviennent pas à s'authentifier auprès d'un pare-feu Palo Alto Networks ou de Panorama que le processus d'Authentification dure plus longtemps que prévu, l'analyse des informations d'authentification peut vous aider à déterminer si l'échec ou le retard est dû aux éléments suivants :

- **Comportement de l'utilisateur** : par exemple, les utilisateurs sont verrouillés après avoir saisi des informations de connexion erronées ou un grand nombre d'utilisateurs essaient d'accéder simultanément à un périphérique.
- **Problèmes liés au système ou au réseau** : par exemple, un serveur d'authentification est inaccessible.
- **Problèmes de configuration** : par exemple, la liste d'autorisation d'un profil d'authentification n'affiche pas tous les utilisateurs censés y figurer.

Les commandes CLI suivantes affichent des informations pouvant vous aider à résoudre ces problèmes :

| Tâche | Commande |
|---|---|
| Affichez le nombre de comptes utilisateurs verrouillés et associés au profil d'authentification (option **auth-profile**), à la séquence d'authentification (option **is-seq**) ou au système virtuel (option **vsys**).<br><br>*Pour déverrouiller les utilisateurs, exécutez la commande opérationnelle suivante :*<br><br>`> request authentication [unlock-admin \| unlock-user]` | `PA-220> show authentication locked-users`<br>`{`<br>`vsys <value> \|`<br>`auth-profile <valeur> \|`<br>`is-seq`<br>`auth-profile <value> \|`<br>`{auth-profile \| vsys} <valeur>`<br>`}` |
| Utilisez la commande **debug authentication** pour dépanner des événements d'authentification.<br><br>Utilisez les options **show** pour afficher les statistiques des requêtes d'authentification et le niveau de débogage actuel :<br>• **show** affiche le niveau de débogage actuel du service d'authentification (authd).<br>• **show-active-requests** affiche le nombre de vérifications actives de requêtes d'authentification, de listes d'autorisations, de comptes utilisateur verrouillés et de | `PA-220> debug authentication`<br>`{`<br>`on {debug \| dump \| error \| info \| warn} \|`<br>`show \|`<br>`show-active-requests \|`<br>`show-pending-requests \|`<br>`connection-show \|`<br>`{`<br>`connection-id \|`<br>`protocol-type`<br>`{`<br>`Kerberos connection-id <value> \|` |

| Tâche | Commande |
| --- | --- |
| requêtes d'Authentification à plusieurs facteurs (MFA).<br>• **show-pending-requests** affiche le nombre de vérifications en attente de requêtes d'authentification, de listes d'autorisations, de comptes utilisateur verrouillés et de requêtes MFA.<br>• **connection-show** affiche les statistiques des requêtes et réponses d'authentification de tous les serveurs d'authentification ou pour un type de protocole spécifique.<br>Utilisez les options **connection-debug** pour activer ou désactiver de débogage de l'authentification :<br>• Utilisez l'option **on** ou **off** pour activer ou désactiver le débogage authd.<br>• Utilisez l'option **connection-debug-on** ou **connection-debug-off** pour activer ou désactiver le débogage de tous les serveurs d'authentification ou pour un type de protocole spécifique. | `LDAP connection-id <valeur> \| RADIUS connection-id <valeur> \| TACACS+ connection-id <valeur> \| } connection-debug-on \| { connection-id \| debug-prefix \| protocol-type { Kerberos connection-id <valeur> \| LDAP connection-id <valeur> \| RADIUS connection-id <valeur> \| TACACS+ connection-id <valeur> \| } connection-debug-off \| { connection-id \| protocol-type { Kerberos connection-id <valeur> \| LDAP connection-id <valeur> \| RADIUS connection-id <valeur> \| TACACS+ connection-id <valeur> \| } connection-debug-on }` |
| Testez la connexion et la validité du profil du certificat. | `PA-220> test authentication authentication-profile auth-profile username <username>password <password>` |
| Dépannez une authentification précise au moyen du **Authentication ID (ID d'authentification)** qui s'affiche sous **Monitor (Surveillance)** > **Logs (Journaux)** > **Authentication (Authentification)**. | `PA-220> grep <Authentication ID>` |

# Gestion des certificats

Les rubriques suivantes décrivent les différents certificats et clés utilisés par les pare-feu Palo Alto Networks® et Panorama, ainsi que la méthode à suivre pour les obtenir et les gérer :

# Clés et certificats

Pour garantir la confiance entre les parties lors d'une session de communication sécurisée, les pare-feu Palo Alto Networks et Panorama utilisent des certificats numériques. Chaque certificat contient une clé cryptographique pour crypter un texte brut ou décrypter un texte crypté. Chaque certificat contient également une signature numérique pour authentifier l'identité de l'émetteur. L'émetteur doit figurer dans la liste des Certificate Authorities (autorités de certification ; AC) de confiance de la partie chargée de l'authentification. La partie authentifiante a la possibilité de vérifier que l'émetteur n'a pas révoqué le certificat (voir Révocation de certificat).

Les pare-feu Palo Alto Networks et Panorama utilisent les certificats dans les applications suivantes :

- L'authentification de l'utilisateur pour le portail d'authentification, l'authentification multifacteur et l'accès d'une interface Web à un pare-feu ou à Panorama.
- Authentification du périphérique pour le VPN de GlobalProtect (utilisateur distant à site ou à grande échelle).
- Authentification du périphérique pour le VPN de site à site IPSec par Internet Key Exchange (échange de clés Internet ; IKE).
- Validation de la liste dynamique externe.
- Accès à l'agent User-ID et à l'agent TS.
- Décryptage du trafic SSL entrant et sortant.

  Un pare-feu décrypte du trafic pour y appliquer des règles de politiques, puis le re-crypte avant de le transférer à sa destination finale. Pour le trafic sortant, le pare-feu agit comme un serveur proxy de transfert, en établissant une connexion SSL/TLS au serveur de destination. Pour sécuriser une connexion entre lui-même et le client, le pare-feu utilise un ***certificat de signature*** pour générer automatiquement une copie du certificat du serveur de destination.

Le tableau suivant répertorie les clés et certificats utilisés par les pare-feu Palo Alto Networks ou par Panorama. Il est recommandé d'utiliser des clés/certificats différents pour chaque utilisation.

**Table 1: Clés/certificats des équipements Palo Alto Networks**

| Utilisation des clés/ certificats | Description |
|---|---|
| Accès administrateur | L'accès sécurisé aux interfaces d'administration des pare-feu ou de Panorama (accès HTTPS à l'interface Web) nécessite un certificat de serveur pour l'interface MGT (ou une interface désignée sur le plan de données si le pare-feu ou Panorama n'utilise par l'interface MGT) et, éventuellement, un certificat pour authentifier l'administrateur. |
| Portail d'authentification | Dans les déploiements où la stratégie d'authentification identifie les utilisateurs qui accèdent aux ressources HTTPS, désignez un certificat de serveur pour l'interface du portail d'authentification. Si vous configurez le portail d'authentification pour qu'il utilise des certificats pour identifier les utilisateurs (au lieu ou en plus de l'authentification interactive), déployez également des certificats clients. Pour plus d'informations sur le portail |

| Utilisation des clés/ certificats | Description |
|---|---|
| | d'authentification, voir Mapper les adresses IP aux noms d'utilisateur à l'aide du portail d'authentification. |
| Approbation de transfert | Pour le trafic SSL/TLS sortant, si un pare-feu fonctionnant comme un serveur proxy de transfert approuve la CA ayant signé le certificat du serveur de destination, le pare-feu utilise le certificat CA d'approbation de transfert pour générer une copie du certificat du serveur de destination à présenter au client. Pour définir la taille de la clé privée, voir Configurer la taille de la clé pour les certificats de serveur proxy de transfert SSL. Pour plus de sécurité, enregistrez la clé sur un module de sécurité matériel (pour plus de détails, voir Clés de sécurité avec un module de sécurité matérielle). |
| Non-approbation de transfert | Pour le trafic SSL/TLS sortant, si un pare-feu fonctionnant comme un proxy de transfert n'approuve pas la CA ayant signé le certificat du serveur de destination, le pare-feu utilisera le certificat CA de non-approbation de transfert pour générer une copie du certificat du serveur de destination à présenter au client. |
| Inspection SSL entrante | Clés qui décryptent le trafic SSL/TLS entrant afin d'inspecter et d'appliquer des politiques. Pour cette application, importez sur le pare-feu une clé privée pour chaque serveur qui est soumis à l'inspection SSL/TLS entrante. Voir Configuration de l'inspection SSL entrante |

| Utilisation des clés/ certificats | Description |
|---|---|
| | *À compter de PAN-OS 8.0, les pare-feu utilisent l'algorithme Elliptic-Curve Diffie-Hellman Ephemeral (Diffie-Hellman basé sur les courbes elliptiques éphémères ; ECDHE) pour effectuer une vérification stricte des certificats. C'est donc dire que si le pare-feu utilise un certificat intermédiaire, vous devez réimporter le certificat sur le pare-feu à partir du site Web après avoir effectué la mise à niveau vers PAN-OS 8.0 ou une version ultérieure et associer le certificat du serveur avec le certificat intermédiaire (installation d'un certificat en chaîne). Autrement, les sessions d'inspection SSL entrante qui possède un certificat intermédiaire dans la chaîne échoueront. Pour installer un certificat en chaîne :*<br>1. *Ouvrez chaque fichier de certificat (.cer) dans éditeur de texte, tel que le Bloc-notes.*<br>2. *Collez chaque certificat de bout en bout avec le certificat du serveur au haut et chaque signataire inclus au bas.*<br>3. *Enregistrez le fichier en tant que texte (.txt) ou certificat (.cer) (le nom du fichier ne peut pas contenir d'espaces).*<br>4. *Importez le certificat combiné (en chaîne) sur le pare-feu.* |
| Certificat d'exclusion SSL | Certificats des serveurs à exclure du décryptage SSL/TLS. Par exemple, si vous activez le décryptage SSL mais que votre réseau inclut des serveurs pour lesquels le pare-feu ne devrait pas déchiffrer le trafic (par exemple, les services Web pour vos systèmes HR), importez les certificats correspondants sur le pare-feu et configurez-les comme des certificats d'exclusion SSL. Créez des des exclusions de déchiffrement |
| GlobalProtect | Toute interaction entre les composants GlobalProtect se produit sur les connexions SSL/TLS. Par conséquent, dans le cadre du déploiement de GlobalProtect, déployez les certificats du serveur pour tous les portails, passerelles et gestionnaires de sécurité mobiles de GlobalProtect. De même, vous pouvez éventuellement déployer les certificats pour authentifier les utilisateurs.<br>*La fonctionnalité VPN (LSVPN) à grande échelle de GlobalProtect nécessite un certificat de signature AC.* |
| VPN de site à site (IKE) | Dans un déploiement de VPN de site à site IPSec, les périphériques homologues utilisent les passerelles Internet Key Exchange (échange de clés Internet ; IKE) pour établir un canal sécurisé. Les passerelles IKE |

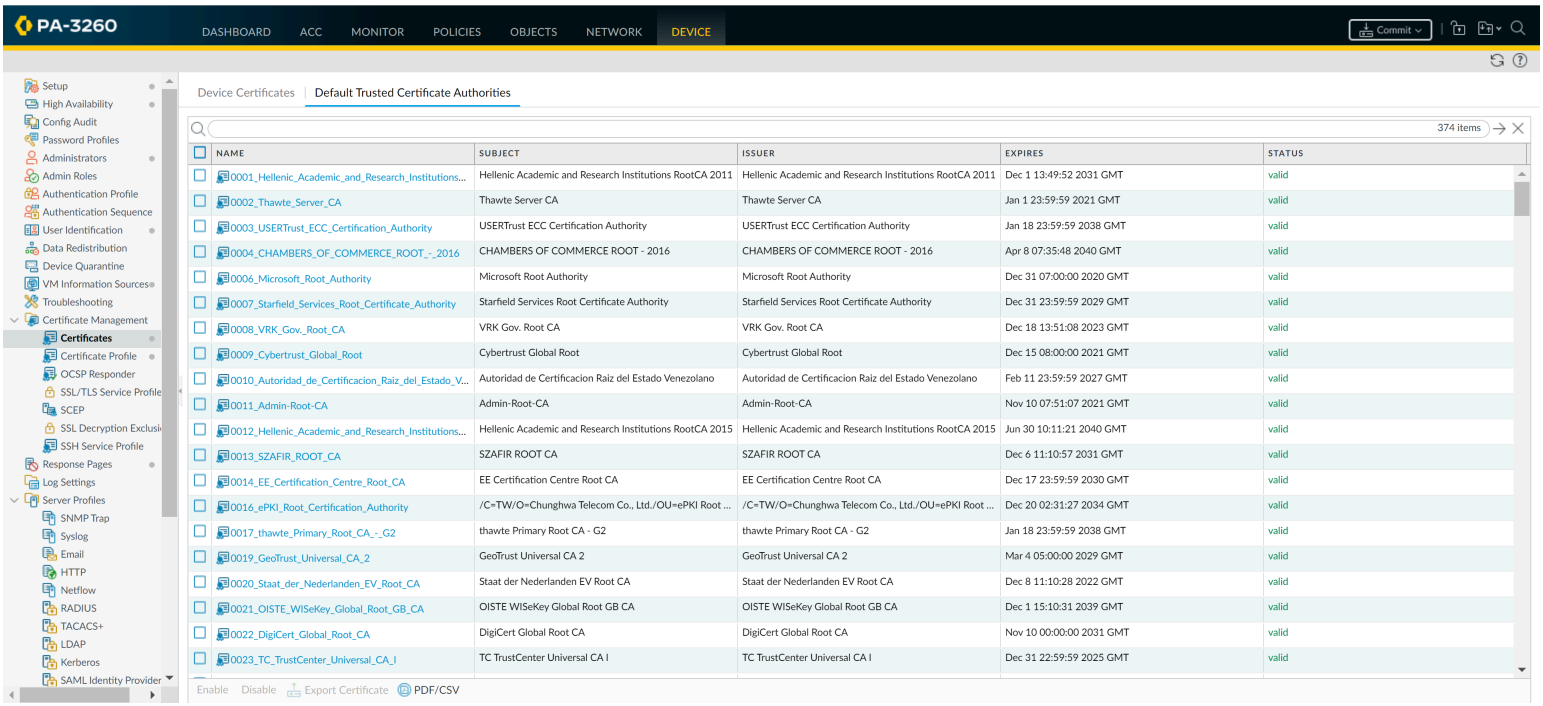
| Utilisation des clés/ certificats | Description |
|---|---|
| | utilisent des certificats ou des clés prépartagées pour authentifier les homologues les uns par rapport aux autres. Vous pouvez configurer et affecter des certificats ou des clés lors de la définition d'une passerelle IKE sur un pare-feu. Consultez Présentation du VPN de site à site. |
| Clé principale | Le pare-feu utilise une clé principale pour crypter toutes les clés privées et tous les mots de passe. Si votre réseau nécessite un emplacement sécurisé pour stocker les clés privées, vous pouvez utiliser une clé de cryptage (encapsulation) stockée sur un Hardware Security Module (module de sécurité matériel - HSM) pour chiffrer la clé principale. Pour obtenir tous les détails, procédez au cryptage d'une clé principale à l'aide d'un HSM. |
| Syslog sécurisé | Certificat permettant d'activer des connexions sécurisées entre le pare-feu et un serveur Syslog. Voir Descriptions des champs Syslog personnalisés |
| CA racine approuvée | Désignation d'un certificat racine généré par une CA approuvée par le pare-feu. Le pare-feu peut utiliser un certificat d'autorité de certification racine auto-signé pour émettre automatiquement des certificats pour d'autres applications (par exemple, SSL Forward Proxy).<br><br>De même, si un pare-feu doit établir des connexions sécurisées avec d'autres pare-feu, la CA racine qui génère leurs certificats doit figurer dans la liste des CA racines approuvées sur le pare-feu. |
| Communication entre dispositifs | Par défaut, Panorama, les pare-feu et les collecteurs de journaux utilisent un ensemble de certificats prédéfinis pour les connexions SSL / TLS utilisées pour la gestion et le transfert de journal. Toutefois, vous pouvez améliorer ces connexions en déployant des certificats personnalisés sur les périphériques de votre déploiement. Ces certificats peuvent également être utilisés pour sécuriser la connexion SSL / TLS entre les homologues Panorama HA. |

# Autorités de certification de confiance par défaut

Le pare-feu autorise les autorités les plus courantes et les plus fiables par défaut. Ces fournisseurs de certificats de confiance sont responsables de l'émission des certificats que le pare-feu exige pour sécuriser les connexions à l'Internet.

Pour afficher et gérer la liste des CA auxquelles le pare-feu fait confiance par défaut, sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Default Trusted Certificate Authorities (Autorités de certification de confiance par défaut)** :




Les seules autres autorités de certification que vous pourriez vouloir ajouter sont les autorités de certification de confiance d'entreprise que votre organisation exige ; reportez-vous à la section Obtention des certificats.

# Révocation de certificats

Les pare-feu Palo Alto Networks et Panorama utilisent des certificats numériques pour garantir la confiance entre les parties lors d'une session de communication sécurisée. La configuration d'un pare-feu ou de Panorama pour vérifier l'état de révocation des certificats confère un niveau de sécurité supplémentaire. Une partie présentant un certificat révoqué n'est pas approuvée. Lorsqu'un certificat fait partie d'une chaîne de certificats, le pare-feu ou Panorama vérifie l'état de chacun des certificats de la chaîne à l'exception du certificat CA racine, pour lequel le périphérique ne peut pas vérifier l'état de révocation.

Diverses circonstances peuvent invalider un certificat avant sa date d'expiration. Il peut s'agir par exemple d'un changement de nom, d'un changement d'association entre le sujet et l'autorité de certification (par exemple, un employé termine sa mission), et d'un état compromis (connu ou suspecté) de la clé privée. Dans ces circonstances, l'autorité de certification qui a généré le certificat doit le révoquer.

Le pare-feu Palo Alto Networks et Panorama prennent en charge les méthodes suivantes pour vérifier l'état de révocation d'un certificat. Si vous configurez les deux méthodes, le pare-feu ou Panorama essaie d'abord la méthode OCSP ; si le serveur OCSP est indisponible, il utilisera la méthode CRL.

- Certificate Revocation List (liste de révocation de certificats - CRL)
- Online Certificate Status Protocol (protocole de vérification en ligne de certificat ; OCSP)

***Sur PAN-OS, la vérification de l'état de révocation du certificat est une fonctionnalité facultative. Il est recommandé de l'activer pour les profils de certificats définissant l'authentification des utilisateurs et des équipements pour les applications Portail d'authentification, GlobalProtect, VPN IPSec de site à site et Accès à l'interface Web du pare-feu ou de Panorama pour vérifier que le certificat n'a pas été révoqué.***

## Certificate Revocation List (liste de révocation de certificats - CRL)

Chaque Certificate Authority (autorité de certification - CA) génère régulièrement une Certificate Revocation List (liste de révocation de certificats - CRL) sur un référentiel public. La CRL identifie les certificats révoqués via leur numéro de série. Une fois que la CA a révoqué un certificat, la mise à jour suivante de la CRL comprendra le numéro de série de ce même certificat. Le pare-feu prend en charge les CRL aux formats Distinguished Encoding Rules (DER) et Privacy Enhanced Mail (PEM).

Le pare-feu Palo Alto Networks télécharge et met en cache la dernière CRL générée pour chacune des CA répertoriées dans la liste des CA approuvées du pare-feu. La mise en cache s'applique uniquement aux certificats validés ; si un pare-feu n'a jamais validé un certificat, la mémoire cache du pare-feu ne stockera pas la CRL pour la CA émettrice. De même, la mémoire cache ne stocke une CRL que jusqu'à son expiration.

***Si vous configurez plusieurs points de distribution CRL (CDP) et que le pare-feu ne peut pas atteindre le premier CDP, le pare-feu ne vérifie pas les autres CDP. Pour rediriger les demandes CRL non valides,*** configurez un proxy DNS ***en tant que serveur alternatif.***

Pour utiliser les CRL afin de vérifier l'état de révocation des certificats utilisés pour le décryptage du trafic SSL/TLS entrant et sortant, reportez-vous à la section Configuration de la vérification de l'état de révocation des certificats utilisés pour le décryptage SSL/TLS.

Pour utiliser les CRL afin de vérifier l'état de révocation des certificats qui authentifient les utilisateurs et les périphériques, configurez un profil de certificat et affectez-le aux interfaces qui sont spécifiques à l'application : Portail d'authentification, GlobalProtect (utilisateur distant à site ou à grande échelle), VPN IPSec de site à site ou Accès à l'interface Web des pare-feu Palo Alto Networks ou de Panorama. Pour obtenir de plus amples précisions, reportez-vous à la section Configuration de la vérification de l'état de révocation des certificats.

## Online Certificate Status Protocol (protocole de vérification en ligne de certificat ; OCSP)

Lorsqu'une session SSL/TLS est établie, les clients peuvent utiliser le Online Certificate Status Protocol (protocole de vérification en ligne de certificat ; OCSP) pour vérifier le statut de révocation du certificat d'authentification. Le client qui s'authentifie envoie une requête contenant le numéro de série du certificat au répondeur OCSP (serveur). Le répondeur cherche dans la base de données de la Certificate Authority (autorité de certification ; CA) ayant généré le certificat et renvoie une réponse contenant l'état (good (valide), revoked (révoqué) ou unknown (inconnu)) au client. L'avantage de la méthode OCSP est qu'elle peut vérifier le statut en temps réel, au lieu de dépendre de la fréquence d'émission (toutes les heures, tous les jours ou toutes les semaines) des CRL.

Le pare-feu Palo Alto Networks télécharge et met en cache les informations sur le statut OCSP pour chacune des AC répertoriées dans la liste des AC approuvées du pare-feu. La mise en cache s'applique uniquement aux certificats validés ; si un pare-feu n'a jamais validé un certificat, la mémoire cache du pare-feu ne stockera pas les informations OCSP pour la CA émettrice. Si votre entreprise dispose de sa propre Public Key Infrastructure (infrastructure à clé publique ; PKI), vous pouvez configurer le pare-feu en tant que répondeur OCSP (reportez-vous à la section Configuration d'un répondeur OCSP).

Pour utiliser le protocole OCSP afin de vérifier l'état de révocation des certificats lorsque le pare-feu fonctionne comme un proxy de transfert SSL, exécuter les étapes de la section Configurer la vérification du statut de révocation des certificats utilisés pour le décryptage SSL/TLS.

Les applications suivantes utilisent les certificats pour authentifier les utilisateurs et/ou les périphériques : Portail d'authentification, GlobalProtect (utilisateur distant à site ou à grande échelle), VPN IPSec de site à site et Accès à l'interface Web des pare-feu Palo Alto Networks ou de Panorama. Pour utiliser le protocole OCSP afin de vérifier l'état de révocation des certificats :

- Configurez un répondeur OCSP (si vous configurez le pare-feu en tant que répondeur OCSP).
- Activez le service HTTP OCSP sur le pare-feu (si vous configurez le pare-feu en tant que répondeur OCSP).
- Créez ou récupérez un certificat pour chaque application.
- Configurez un profil de certificat pour chaque application.
- Affectez le profil de certificat à l'application correspondante.

Pour prendre en charge les situations dans lesquelles le répondeur OCSP est indisponible, configurez la CRL en tant que méthode de secours. Pour obtenir de plus amples précisions, reportez-vous à la section Configuration de la vérification de l'état de révocation des certificats.

# Déploiement de certificats

Les approches de base permettant de déployer des certificats pour les pare-feu Palo Alto Networks et Panorama sont les suivantes :

- **Obtenir des certificats auprès d'une CA tierce approuvée** : l'avantage d'obtenir un certificat auprès d'une Certificate Authority (autorité de certification - CA) tierce approuvée, telle que VeriSign ou GoDaddy, est que les clients finaux approuvent déjà le certificat parce que les navigateurs courants incluent des certificats CA racines générés par des CA connues dans leurs magasins de certificats racines approuvés. Par conséquent, pour les applications qui nécessitent des clients finaux pour établir des connexions sécurisées avec le pare-feu ou Panorama, vous devez acheter un certificat auprès d'une CA que les clients finaux approuvent pour éviter de déployer au préalable des certificats CA racines chez les clients finaux (Ces applications sont par exemple un portail GlobalProtect ou le Gestionnaire de sécurité mobile GlobalProtect.) Cependant, la plupart des CA tierces ne peuvent pas générer de certificats de signature. Par conséquent, ce type de certificat ne convient pas aux applications (par exemple, décryptage SSL/TLS et VPN à grande échelle) qui nécessitent que le pare-feu génère des certificats. Reportez-vous à la section Obtention d'un certificat auprès d'une CA externe.
- **Obtenir des certificats auprès d'une CA d'entreprise** : les entreprises qui disposent de leur propre CA interne peuvent l'utiliser afin d'émettre les certificats pour les applications de pare-feu et les importer sur le pare-feu. L'avantage est que les clients finaux approuvent probablement déjà la CA d'entreprise. Vous pouvez soit générer les certificats nécessaires et les importer sur le pare-feu, soit générer une Certificate Signing Request (demande de signature de certificat - CSR) sur le pare-feu et l'envoyer à la CA d'entreprise pour signature. L'avantage de cette méthode est que la clé privée ne quitte pas le pare-feu. Une CA d'entreprise peut aussi générer un certificat de signature, que le pare-feu utilise pour générer automatiquement des certificats (par exemple, pour le VPN à grande échelle de GlobalProtect ou les sites nécessitant un décryptage SSL/TLS). Reportez-vous à la section Importation d'un certificat et d'une clé privée.
- **Générer des certificats auto-signés** : vous pouvez créer un certificat racine CA auto-signé sur le pare-feu et l'utiliser pour émettre automatiquement des certificats pour les autres applications du pare-feu.

*Si vous utilisez cette méthode pour générer des certificats pour une application qui nécessite un client final pour approuver le certificat, les utilisateurs finaux verront une erreur de certificat parce que le certificat CA racine ne figurera pas dans leur magasin de certificats racines approuvés. Pour éviter ce problème, déployez le certificat CA racine auto-signé sur tous les systèmes des utilisateurs finaux. Vous pouvez déployer les certificats manuellement ou utiliser une méthode de déploiement centralisée comme un Group Policy Object (objet de politique de groupe - GPO) Active Directory (AD).*

# Configuration du paramétrage de l'état de révocation des certificats

Pour vérifier l'état de révocation des certificats, le pare-feu utilise le Online Certificate Status Protocol (protocole de vérification des certificats en ligne ; OCSP) et/ou des Certificate Revocation Lists (listes de révocation de certificats ; CRL). Pour plus d'informations sur ces méthodes, reportez-vous à la section Révocation des Certificats. Si vous configurez les deux méthodes, le pare-feu essaie d'abord le protocole OCSP et ne fait appel à la méthode CRL en secours que si le répondeur OCSP est indisponible. Si votre entreprise dispose de sa propre Public Key Infrastructure (infrastructure à clé publique ; PKI), vous pourrez configurer le pare-feu afin qu'il fonctionne comme un répondeur OCSP.

Les rubriques suivantes expliquent comment configurer le pare-feu pour vérifier l'état de révocation des certificats :

- Configuration d'un répondeur OCSP
- Configuration de la vérification de l'état de révocation des certificats
- Configuration de la vérification de l'état de révocation des certificats utilisés pour le décryptage SSL/TLS

## Configuration d'un répondeur OCSP

Pour utiliser le Online Certificate Status Protocol (protocole de vérification des certificats en ligne ; OCSP) afin de vérifier l'état de révocation des certificats, vous devez configurer le pare-feu pour qu'il accède à un répondeur OCSP (serveur). L'entité qui gère le répondeur OCSP peut être une autorité de certification tierce. Si votre entreprise dispose de sa propre Public Key Infrastructure (infrastructure à clé publique ; PKI), vous pouvez utiliser dws répondeurs OCSP externes ou configurer le pare-feu en tant que répondeur OCSP. Pour plus d'informations sur le OSCP, reportez-vous à la section Révocation de certificats.

*Configurez un Certificate Profile (profil de certificat) de répondeur OCSP uniquement lorsque vous générez un nouveau certificat (**Device (périphérique) > Certificate Management (Gestion de certificats) > Certificates (Certificats)**). Spécifiez le **OCSP Responder (répondeur OCSP)** lorsque vous générez un nouveau certificat afin que le pare-feu remplisse le champ Authority Information Access (AIA) avec l'URL appropriée, puis spécifiez le nouveau certificat dans le profil de certificat. La configuration d'un profil de certificat ne remplace pas le profil de certificat pour les certificats existants ou les autorités de certification racine.*

*Vous pouvez activer la validation OCSP ou remplacer le champ AIA du certificat dans le Certificate Profile (profil de certificat). La configuration du profil de certificat détermine quels mécanismes de validation de certificat sont utilisés sur les certificats qui s'authentifient auprès des services hébergés sur le pare-feu, tels que GlobalProtect.*

**STEP 1 |** Définissez un répondeur OCSP externe ou configurez le pare-feu lui-même en tant que répondeur OCSP.

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **OCSP Responder (Répondeur OCSP)** et cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name (Nom)** pour identifier le répondeur (31 caractères maximum). Ce nom est sensible à la casse. Il doit être unique et utiliser uniquement des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement.
3. Si le pare-feu comporte plusieurs systèmes virtuels (vsys), sélectionnez un **Location (Emplacement)**(vsys ou **Shared (Partagé)**) pour le certificat.
4. Dans le champ **Host Name (Nom d'hôte)**, saisissez le nom d'hôte (recommandé) ou l'adresse IP du répondeur OCSP. Vous pouvez entrer une adresse IPv4 ou IPv6. À partir de cette valeur, PAN-OS déduit automatiquement une URL et l'ajoute au certificat en cours de vérification.

   Si vous configurez le pare-feu lui-même comme un répondeur OCSP, le nom d'hôte doit se résoudre en une adresse IP dans l'interface que le pare-feu utilise pour les services OCSP.
5. Cliquez sur **OK**.

**STEP 2 |** Si vous souhaitez que le pare-feu utilise l'interface de gestion comme interface du répondeur OCSP, activez la communication OCSP sur le pare-feu. Autrement, passez à l'étape suivante pour configurer une autre interface.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Interfaces** > **Management (Gestion)**.
2. Dans la section Services réseau, cochez la case **HTTP OCSP**, puis cliquez sur **OK**.

**STEP 3 |** Pour utiliser une autre interface en tant que répondeur OCSP, ajoutez un profil de gestion d'interface à l'interface utilisée pour les services OCSP.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **Interface Mgmt (Gestion de l'interface)**.
2. Cliquez sur **Add (Ajouter)** pour créer un nouveau profil ou cliquez sur le nom d'un profil existant.
3. Cochez la case **HTTP OCSP (OCSP HTTP)**, puis cliquez sur **OK (OK)**.
4. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)**, puis cliquez sur le nom de l'interface qui sera utilisée par le pare-feu pour les services OCSP. Le **Host Name (Nom d'hôte)** OCSP indiqué à l'étape 1 doit se résoudre en une adresse IP dans cette interface.
5. Sélectionnez **Advanced (Avancé)** > **Other info (Autres informations)**, puis sélectionnez le profil de gestion d'interface que vous venez de créer.
6. Cliquez sur **OK**, puis sur **Commit (Valider)**.

## Configuration de la vérification de l'état de révocation des certificats

Le pare-feu et Panorama utilisent les certificats pour authentifier les utilisateurs et les périphériques pour les applications, telles que Portail d'authentification, GlobalProtect, VPN IPSec de site à site et Accès à l'interface Web du pare-feu/de Panorama. Pour une meilleure sécurité, il est recommandé de configurer le pare-feu pour vérifier l'état de révocation des certificats qu'il utilise pour l'authentification des utilisateurs/périphériques.

**STEP 1 |** Configurez un profil de certificat pour chaque application.

Affectez un ou plusieurs certificats CA racines au profil et indiquez comment le pare-feu vérifie l'état de révocation des certificats.

Pour plus d'informations sur les certificats utilisés par les différentes applications, reportez-vous à la section Clés et certificats.

**STEP 2 |** Affectez les profils de certificat aux applications correspondantes.

Suivez les étapes ci-dessous pour affecter un profil de certificat en fonction de l'application qui l'exige.

## Configuration de la vérification de l'état de révocation des certificats utilisés pour le décryptage SSL/TLS

Le pare-feu décrypte le trafic SSL/TLS entrant et sortant afin d'inspecter le trafic à la recherche de menaces. Lorsque vous créez une règle de politique de sécurité qui autorise le trafic et que vous appliquez des profils de sécurité à la règle, créez une règle de politique de décryptage analogue pour décrypter ce trafic. Si vous ne décryptez pas le trafic, le pare-feu ne peut pas utiliser les profils de sécurité pour inspecter le trafic (vous ne pouvez pas inspecter ce que vous ne pouvez pas voir). Le pare-feu re-crypte le trafic avant de le transférer. (Consultez les sections Inspection SSL entrante et Proxy de transfert SSL). Vous pouvez configurer le pare-feu pour vérifier l'état de révocation des certificats utilisés pour le décryptage comme suit.

***L'activation de la vérification de l'état de révocation des certificats de décryptage SSL/TLS va rallonger la durée du processus établissant la session. Il se peut que la première tentative d'accès à un site échoue si la vérification n'est pas finie avant que la session n'expire. C'est pourquoi la vérification est désactivée par défaut.***

**STEP 1 |** Définissez les durées du délai d'expiration spécifiques au service pour les demandes d'état de révocation.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Session (Session)** puis, dans la section Session Features (Caractéristiques de la session), sélectionnez **Decryption Certificate Revocation Settings (Paramètres de révocation du certificat de décryptage)**.
2. Effectuez l'une des deux étapes suivantes, ou les deux, selon que le pare-feu doit utiliser le Online Certificate Status Protocol (OCSP) (protocole de statut de certificat ouvert ; OCSP) ou la méthode de la Certificate Revocation List (CRL) (liste de révocation de certificats ; CRL) pour vérifier le statut de révocation des certificats. Si le pare-feu doit utiliser les deux méthodes, il essaiera d'abord le protocole OCSP ; si le répondeur OCSP est indisponible, le pare-feu essaiera alors la méthode CRL.
   - Dans la section CRL (CRL), cochez la case **Enable (Activer)** et saisissez le **Receive Timeout (Délai de réception)**. Il s'agit de la durée (de 1 à 60 secondes) au bout de laquelle le pare-feu n'attend plus la réponse du service CRL.
   - Dans la section OCSP (OCSP), cochez la case **Enable (Activer)** et saisissez le **Receive Timeout (Délai de réception)**. Il s'agit de la durée (de 1 à 60 secondes) au bout de laquelle le pare-feu n'attend plus la réponse du répondeur OCSP.

   En fonction de la valeur **Certificate Status Timeout (Délai d'expiration de l'état du certificat)** que vous aurez indiquée à l'étape 2, le pare-feu peut enregistrer un délai

d'expiration avant l'expiration de l'une des deux durées du **Receive Timeout (Délai d'expiration de la réception)**, ou des deux.

**STEP 2 |** Définissez la durée du délai d'expiration total pour les demandes d'état de révocation.

Saisissez le **Certificate Status Timeout (Délai d'expiration du statut du certificat)**. Il s'agit de la durée (de 1 à 60 secondes) au bout de laquelle le pare-feu n'attend plus la réponse d'aucun service d'état de certificat et applique la logique de blocage de la session que vous pouvez éventuellement définir à l'étape 3. Le **Délai d'expiration du statut du certificat** correspond au **Délai de réception** des méthodes OCSP/CRL de la manière suivante :

- Si vous activez les deux méthodes, OCSP et CRL : le pare-feu enregistre un délai d'expiration de la demande après l'expiration de la plus courte des deux durées : la valeur **Certificate Status Timeout (Délai d'expiration du statut du certificat)** ou l'agrégation des deux valeurs **Receive Timeout (Délai de réception)**.
- Si vous activez uniquement la méthode OCSP : le pare-feu enregistre un délai d'expiration de la demande après l'expiration de la plus courte des deux durées : la valeur **Certificate Status Timeout (Délai d'expiration du statut du certificat)** ou la valeur **Receive Timeout (Délai de réception)** par la méthode OCSP.
- Si vous activez uniquement la méthode CRL : le pare-feu enregistre un délai d'expiration de la demande après l'expiration de la plus courte des deux durées : la valeur **Délai d'expiration du statut du certificat** ou la valeur **Délai de réception** par la méthode CRL.

**STEP 3 |** Définissez le comportement de blocage de l'état du certificat inconnu ou un délai d'expiration de la demande d'état de révocation.

Si vous souhaitez que le pare-feu bloque les sessions SSL/TLS lorsque le service OCSP ou CRL renvoie un statut de révocation de certificat inconnu, cochez la case **Block Session With Unknown Certificate Status (Bloquer une session si le statut du certificat est inconnu)**. Sinon, le pare-feu poursuit la session.

Si vous souhaitez que le pare-feu bloque les sessions SSL/TLS une fois qu'il a enregistré un délai d'expiration de la demande, cochez la case **Block Session On Certificate Status Check Timeout (Bloquer une session à l'expiration de la vérification du statut du certificat)**. Sinon, le pare-feu poursuit la session.

**STEP 4 |** Cliquez sur **OK**, puis sur **Commit (Valider)**.

# Configuration de la clé principale

Chaque serveur de gestion du pare-feu ou de Panorama inclut une clé principale par défaut qui chiffre toutes les clés privées et les mots de passe de la configuration pour les sécuriser (comme la clé privée utilisée pour le déchiffrement du proxy de transfert SSL).

*Changez la clé principale par défaut dès que possible afin de vous assurer que vous utilisez une clé principale unique pour le cryptage.*

Dans une configuration à haute disponibilité (HA), vous devez utiliser la même clé principale sur les deux pare-feu car la clé principale n'est pas synchronisée entre les homologues HA. Dans le cas contraire, la synchronisation HA ne fonctionnera pas bien.

Si vous utilisez Panorama pour gérer vos pare-feu, vous pouvez configurer la même clé principale sur Panorama et tous les pare-feu gérés ou configurer une clé principale unique pour chaque pare-feu géré. Pour les pare-feu gérés dans une configuration HA, vous devez configurer la même clé principale pour chaque homologue HA.

Assurez-vous de stocker la clé principale dans un lieu sûr. Vous ne pouvez récupérer la clé principale et le rétablissement des paramètres d'usine du pare-feu est la seule façon de restaurer la clé principale par défaut.

**STEP 1 |** Backup the configuration (Sauvegarde de la configuration).

**STEP 2 |** (HA uniquement) Désactivez la HA.

Vous devez effectuer cette étape avant de pouvoir déployer une nouvelle clé principale vers une paire de pare-feu HA. Si vous ne désactivez pas la HA avant de déployer une nouvelle clé principale, Panorama perdra la connectivité au pare-feu principal.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, puis modifiez la configuration.
2. Désactivez (effacez) le paramètre **Enable HA (Activer la HA)** et cliquez sur **OK**.
3. **Commit (validez)** vos modifications de configuration.

**STEP 3 |** Sélectionnez **Device (Périphérique)** > **Master Key and Diagnostics (Clé principale et diagnostics)**, puis modifiez la section Master Key (Clé principale).

**STEP 4 |** Saisissez la **Current Master Key (Clé principale active)** si elle existe.

**STEP 5 |** Définissez une **New Master Key (Nouvelle clé principale)**, puis **Confirm New Master Key (Confirmez la nouvelle clé principale)**. La clé doit contenir exactement 16 caractères.

**STEP 6 |** Pour indiquer la **LifeTime (Durée de vie)** de la clé principale, saisissez le nombre de **Days (Jours)** et/ou d'**Hours (Heures)** au bout desquel(le)s la clé arrive à expiration.

Vous devez configurer une nouvelle clé principale avant que la clé actuelle n'expire. Si la clé principale expire, le pare-feu ou Panorama redémarre automatiquement en mode Maintenance. Vous devez alors effectuer le rétablissement des paramètres d'usine du pare-feu.

*Réglez la **Lifetime (Durée de vie)** sur deux ans ou moins, en fonction du nombre de cryptages effectués par le périphérique. Plus un périphérique effectue de cryptages, plus la **Lifetime (Durée de vie)** que vous devez définir est courte. L'essentiel est de ne pas être à court de cryptages uniques avant de changer la clé principale. Chaque clé principale peut fournir jusqu'à $2^{32}$ cryptages uniques basés sur la valeur de la clé principale et la valeur du vecteur d'initialisation (IV). Après $2^{32}$ cryptages uniques, les cryptages se répètent (ne sont plus uniques), ce qui constitue un risque pour la sécurité.*

*Définissez une valeur de **Time for Reminder (Délai de rappel)** (voir l'étape suivante) pour la clé principale et lorsque la notification de rappel a lieu, modifiez la clé principale.*

**STEP 7 |** Saisissez une **Time for Reminder (Heure de rappel)** qui précise le nombre de **Days (Jours)** et de **Hours (Heures)** avant que la clé principale n'expire lorsque le pare-feu génère une alarme d'expiration. Le pare-feu ouvre automatiquement la boîte de dialogue System Alarms (Alarmes système) pour afficher l'alarme.

*Réglez le rappel de manière à ce qu'il vous laisse suffisamment de temps pour configurer une nouvelle clé principale avant son expiration dans une fenêtre de maintenance programmée. Lorsque le **Time for Reminder (Délai de rappel)** expire et que le pare-feu ou Panorama envoie un journal de notification, changez la clé principale, n'attendez pas l'expiration de la **Lifetime (Durée de vie)**. Pour les périphériques groupés, suivez chaque dispositif (par exemple, les pare-feu que Panorama gère et les paires HA de pare-feu) et lorsque la valeur de rappel expire pour un dispositif quelconque du groupe, changez la clé principale.*

*Pour s'assurer que l'alarme d'expiration s'affiche, sélectionnez **Device (Périphérique)** > **Log Settings (Paramètres du journal)**, modifiez les paramètres d'alarme et cliquez sur **Enable Alarms (Activer les alarmes)**.*

**STEP 8 |** Activez **Auto Renew Master Key (Renouvellement automatique de la clé principale)** pour configurer le pare-feu pour qu'il renouvellement automatiquement la clé principale. Pour configurer le **Auto Renew With Same Master Key (Renouvellement automatique de la même clé principale)**, indiquez le nombre de **Days (Jours)** et/ou **Hours (Heures)** pendant lesquels renouveler la même clé principale. Le prolongement du délai de la clé permet au pare-feu de demeurer fonctionnel et de continuer à sécuriser votre réseau. Vous devrez toutefois configurer une nouvelle clé si la durée de vie de la clé principale expire prochainement.

Le renouvellement automatique de la clé principale présente des avantages et des risques. L'avantage est que la prolongation de la **Lifetime (Durée de vie)** de la clé principale protège contre l'impossibilité de changer la clé principale avant l'expiration de sa durée de vie. Le risque est que les cryptages se répètent et entraînent un risque de sécurité si le nombre de cryptages

que le dispositif effectue avec la clé principale dépasse le nombre de cryptages uniques que la clé principale peut générer ($2^{32}$ cryptages uniques).

*Si la clé principale expire (vous ne la renouvelez pas automatiquement et vous ne la remplacez pas à temps), le périphérique passe en mode de maintenance.*

*Si vous activez la fonction **Auto Renew Master Key (Renouvellement automatique de la clé principale)**, réglez-la de manière à ce que la durée totale (durée de vie plus durée de renouvellement automatique) n'entraîne pas l'épuisement des cryptages uniques du périphérique. Par exemple, si vous pensez que le périphérique consommera le nombre de cryptages uniques de la clé principale dans deux ans et demi, vous pouvez fixer la **Lifetime (Durée de vie)** à deux ans, fixer le **Time for Reminder (Délai de rappel)** à 60 jours et fixer le **Auto Renew Master Key (Renouvellement automatique de la clé principale)** à 60-90 jours pour disposer du temps supplémentaire nécessaire pour configurer une nouvelle clé principale avant l'expiration de la **Lifetime (Durée de vie)**. Toutefois, la meilleure pratique consiste toujours à changer la clé principale avant l'expiration de la durée de vie pour s'assurer qu'aucun périphérique ne répète les cryptages.*

*Tenez compte du nombre de jours avant votre prochaine fenêtre de maintenance disponible lors de la configuration du renouvellement automatique de la clé principale après l'expiration de la durée de vie de la clé.*

**STEP 9 |** (Facultatif) Pour accroître la sécurité, cochez ou décochez la case pour activer ou désactiver l'utilisation d'un **HSM (Module de sécurité matériel)** pour crypter la clé principale. Pour obtenir tous les détails, procédez au cryptage d'une clé principale à l'aide d'un HSM.

**STEP 10 |** Cliquez sur **OK**, puis sur **Commit (Valider)**.

**STEP 11 |** (HA uniquement) Réactivez la HA.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, puis modifiez la configuration.
2. Sélectionnez **Enable HA (Activer la haute disponibilité)**, puis cliquez sur **OK**.
3. **Commit (validez)** vos modifications de configuration.

# Cryptage de la clé principale

Sur les périphériques physiques et virtuels de Palo Alto Networks, vous pouvez configurer la clé principale pour utiliser l'algorithme de chiffrement AES-256-CBC ou AES-256-GCM (introduit dans PAN-OS 10.0) pour chiffrer les données telles que les clés et les mots de passe. L'AES-256-GCM offre un cryptage plus puissant que l'AES-256-CBC et améliore votre posture de sécurité. Il comprend également un contrôle d'intégrité intégré. La clé principale utilise l'algorithme de cryptage configuré pour crypter les données sensibles stockées sur le pare-feu et sur Panorama. Lorsque vous réglez l'algorithme de cryptage sur AES-256-GCM, vous pouvez toujours utiliser un HSM pour crypter la clé principale avec une clé de cryptage qui est stockée sur le HSM.

L'algorithme de cryptage par défaut que la clé principale utilise pour crypter les données est AES-256-CBC - le même algorithme que la clé principale utilisée avant PAN-OS 10.0. AES-256-CBC est le niveau de cryptage par défaut car lorsque vous gérez des pare-feu avec Panorama, les pare-feu gérés peuvent être sur des versions PAN-OS différentes, et les pare-feu sur des versions PAN-OS antérieures à PAN-OS 10.1 ne prennent pas en charge AES-256-GCM. C'est pourquoi Panorama doit utiliser le niveau de cryptage le plus bas que ses appareils gérés peuvent utiliser. Par exemple, si certains appareils gérés fonctionnent avec PAN-OS 10.1 et d'autres avec des versions antérieures, Panorama doit utiliser AES-256-CBC. Cependant, si tous les appareils gérés fonctionnent sous PAN-OS 10.1 ou une version ultérieure, alors Panorama et tous ses appareils gérés peuvent utiliser AES-256-GCM.

***Utilisez le même niveau de cryptage sur Panorama et ses appareils gérés et utilisez le même niveau de cryptage sur les paires de pare-feu. Mettez à niveau les appareils pour utiliser l'algorithme de cryptage le plus puissant possible. Si tous les appareils gérés par Panorama fonctionnent sous PAN-OS 10.0, utilisez AES-256-GCM sur tous les appareils. La configuration des appareils gérés ou appariés qui utilisent différents niveaux de cryptage peut se désynchroniser.***

Lorsque vous changez l'algorithme de cryptage pour AES-256-GCM, les appareils l'utilisent au lieu de AES-256-CBC pour crypter les données sensibles. Lorsque vous passez d'un algorithme à un autre, vous pouvez également préciser si vous souhaitez :

- Re-crypter les données cryptées existantes avec le nouvel algorithme.
- Laisser les données existantes cryptées avec l'ancien algorithme de cryptage et utiliser le nouvel algorithme uniquement pour les nouveaux (futurs) cryptages.

***Par défaut, lorsque vous modifiez l'algorithme de cryptage, l'appareil utilise le nouvel algorithme pour re-crypter les données cryptées existantes ainsi que pour crypter de nouvelles données. Si vous gérez des appareils avec Panorama, il se peut qu'ils soient sur des versions différentes de PAN-OS et qu'ils ne prennent pas en charge les algorithmes de cryptage les plus récents. Assurez-vous de bien comprendre quels algorithmes de cryptage Panorama et ses dispositifs gérés prennent en charge avant de changer l'algorithme de cryptage ou de re-crypter des données qui ont déjà été cryptées.***

- Configuration du niveau de cryptage de la clé principale
- Cryptage de la clé principale sur un pare-feu paire HA
- Journaux de cryptage de la clé principale

- Cryptages uniques de clé principale pour AES-256-GCM

## Configuration du niveau de cryptage de la clé principale

Vous configurez le niveau de l'algorithme de cryptage de la clé principale et vous déterminez s'il faut re-crypter toutes les données actuellement cryptées avec un nouveau niveau d'algorithme de cryptage en utilisant la CLI. Selon l'ordre des mots clés, vous pouvez changer le niveau de cryptage ou vous pouvez changer le niveau de cryptage et également spécifier s'il faut re-crypter les données précédemment cryptées.

La commande CLI opérationnelle suivante modifie le niveau de cryptage et re-crypte automatiquement toutes les données actuellement cryptées avec le niveau de cryptage spécifié :

```
admin@PA-NGFW>request encryption-level level <0|1|2>
```

La commande CLI opérationnelle suivante modifie le niveau de cryptage et spécifie s'il faut re-crypter toutes les données actuellement cryptées avec le nouveau niveau de cryptage :

```
admin@PA-NGFW>request encryption-level re-encrypt <yes|no> level <0|
1|2>
```

| Mot clé | Options (Options) |
|---|---|
| niveau | **0** = Utiliser l'algorithme par défaut (AES-256-CBC) pour crypter les données<br>**1** = Utiliser l'algorithme AES-256-CBC pour crypter les données<br>**2** = Utiliser l'algorithme AES-256-GCM pour crypter les données<br>Le pare-feu re-crypte toutes les données actuellement cryptées et crypte les nouvelles données sensibles en utilisant l'algorithme spécifié. Si vous ne voulez pas re-crypter les données cryptées existantes avec le nouvel algorithme, spécifiez **re-encrypt no (ne pas re-crypter** dans la chaîne de commande. Cela empêche le pare-feu de re-crypter automatiquement les données qu'il a déjà cryptées.<br>*N'utilisez l'AES-256-GCM que lorsque Panorama et tous ses appareils gérés (ou les deux périphérique d'une paire HA) exécutent PAN-OS 10.1 ou plus et configurent tous les périphériques pour utiliser l'AES-256-GCM. Les périphériques gérés ou couplés qui utilisent différents niveaux de cryptage peuvent se désynchroniser.* |

| Mot clé | Options (Options) |
|---|---|
| re-encrypt | **no** = Ne pas re-crypter les données actuellement cryptées. Le pare-feu ne re-crypte pas les données actuellement cryptées. Les données actuellement cryptées restent cryptées avec l'algorithme que le pare-feu a utilisé à l'origine pour crypter les données. Le pare-feu utilise l'algorithme spécifié uniquement pour crypter les données sensibles à l'avenir.<br>**yes** = Re-crypter les données actuellement cryptées avec l'algorithme spécifié et utiliser cet algorithme pour crypter les données sensibles à l'avenir. |

Utilisez la commande CLI opérationnelle **show system masterkey-properties** pour vérifier l'algorithme de cryptage (niveau) actuellement configuré sur le dispositif, par exemple :

```
admin@PA-NGFW>show system masterkey-properties
```

```
Master key expires at: unspecified
Reminders will begin at: unspecified
Master key on hsm: no
Automatically renew master key lifetime: 0
Encryption Level: 1
```

La sortie montre que le niveau de cryptage actuel est 1, c'est-à-dire AES-256-CBC.

Si vous passez à une version antérieure du PAN-OS, le périphérique rétablit automatiquement l'algorithme de cryptage à un niveau que la version PAN-OS déclassée prend en charge et re-crypte automatiquement les données cryptées en utilisant ce niveau afin que le périphérique puisse décrypter et utiliser les données selon les besoins. Par exemple, si votre périphérique est sous PAN-OS 10.1 et utilise AES-256-GCM comme algorithme de cryptage (qui n'est pas pris en charge sur les versions antérieures du PAN-OS), et que vous passez à PAN-OS 9.1, alors le périphérique re-crypte les données cryptées en AES-256-CBC, qui est pris en charge dans PAN-OS 9.1.

## Cryptage de la clé principale sur un pare-feu paire HA

Pour utiliser le niveau de cryptage AES-256-GCM sur une paire de pare-feu haute disponibilité (HA), les deux pare-feu doivent exécuter PAN-OS 10.0 afin que les deux pare-feu prennent en charge AES-256-GCM. Si l'un des pare-feu de la paire HA fonctionne avec une version antérieure à PAN-OS 10.0, vous ne pouvez pas utiliser AES-256-GCM. Lorsque les deux pare-feu sont sur PAN-OS 10.0, les deux pare-feu peuvent décoder les clés de cryptage AES-256-CBC ou AES-256-GCM, ils peuvent donc utiliser l'un ou l'autre niveau de cryptage. Cependant, les deux pare-feu devraient utiliser le même niveau de cryptage pour éviter la possibilité de se désynchroniser.

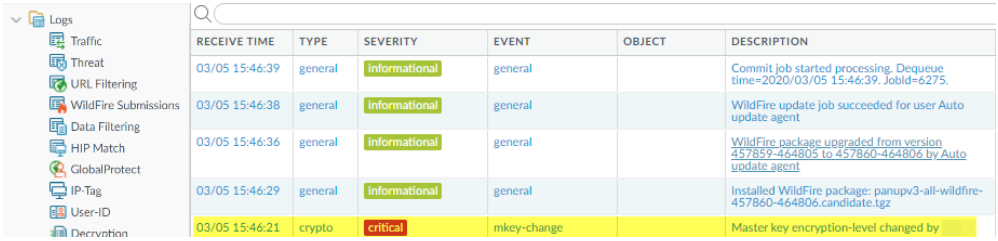
*Utilisez le cryptage AES-256-GCM sur les deux pare-feu de la paire HA. Que vous utilisiez AES-256-GCM ou AES-256-CBC, utilisez le même algorithme sur les deux pare-feu.*

Vous n'avez pas besoin de désactiver HA pour changer le niveau de cryptage sur un pare-feu dans une paire de HA où les deux pare-feu exécutent PAN-OS 10.0.

## Journaux de cryptage de la clé principale

Le pare-feu génère un journal système (**Monitor (Moniteur)** > **Logs (Journaux)** > **System (Système)**) lorsque vous changez l'algorithme de cryptage de la clé principale (niveau).




Pour afficher tous les journaux du système pour le cryptage par clé principale, créez un filtre qui affiche tous les journaux du **Type** crypto : **`(subtype eq crypto)`**.

## Cryptages uniques de clé principale pour AES-256-GCM

La clé principale ne peut générer qu'un nombre fini de cryptages uniques avant d'être à court de combinaisons uniques et doit répéter les cryptages. Le pare-feu crée des cryptages uniques en utilisant l'algorithme de cryptage AES-256-GCM avec un vecteur d'initialisation (IV). Un IV est un numéro arbitraire qui ne doit être utilisé qu'une seule fois pour créer un cryptage afin de garantir que chaque cryptage est unique.

Chaque cryptage utilisant la clé principale et l'IV doit être unique afin de prévenir les attaques de contrefaçon. Le pare-feu répond à la condition d'unicité selon laquelle la probabilité que le cryptage authentifié soit jamais créé avec la même IV et la même clé sur deux ou plusieurs ensembles distincts de données d'entrée n'est pas supérieure à $2^{32}$.

Lorsque l'IV parcourt toutes ses valeurs uniques, la valeur de l'IV se répète. Lorsque la valeur IV se répète, l'utilisation de la même clé principale et de la valeur IV répétée pour crypter les données signifie que le cryptage est le même qu'un cryptage précédemment utilisé sur d'autres données. Change the Master Key (Modifiez la clé principale) avant que le système ne soit à court de cryptages uniques pour empêcher le pare-feu d'utiliser le même cryptage (combinaison de clé principale et de valeur IV) sur plus d'une donnée sensible. Les combinaisons de cryptage uniques ne doivent jamais être répétées ou réutilisées.

Pour savoir quand vous devez changer la clé maîtresse, définissez les valeurs **Lifetime (Durée de vie)** et **Reminder (Rappel)** de la clé principale sur chaque périphérique (**Device (Périphérique)** > **Master Key (Clé principale)**Diagnostics et modifiez la clé principale). Fixez les valeurs de manière conservatrice, en fonction du volume prévu de cryptages par clé principale, afin de garantir que tous les cryptages sont uniques et qu'aucune combinaison de cryptage n'est répétée ou réutilisée.

# Obtention des certificats



## Création d'un certificat CA racine auto-signé

Un certificat Certificate Authority (autorité de certification - CA) racine auto-signé est le niveau supérieur d'un certificat dans une chaîne de certificats. Un pare-feu peut utiliser ce certificat pour générer automatiquement des certificats destinés à d'autres utilisations. Par exemple, le pare-feu génère des certificats pour le décryptage SSL/TLS et pour les satellites dans un VPN à grande échelle de GlobalProtect.

Lorsque vous établissez une connexion sécurisée avec le pare-feu, le client distant doit approuver la CA racine qui a généré le certificat. Sinon, le navigateur du client affichera un message d'avertissement indiquant que le certificat n'est pas valide et qu'il pourrait (en fonction des paramètres de sécurité) bloquer la connexion. Pour empêcher cela, suite à la génération du certificat CA racine auto-signé, importez-le sur les systèmes clients.

*Sur un pare-feu Palo Alto Networks ou Panorama, vous pouvez générer des certificats auto-signés uniquement s'il s'agit de certificats CA.*

**STEP 1 |** Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**.

**STEP 2 |** Si le pare-feu comporte plusieurs systèmes virtuels (vsys), sélectionnez un **Location (Emplacement)**(vsys ou **Shared (Partagé)**) pour le certificat.

**STEP 3 |** Cliquez sur **Generate (Générer)**.

**STEP 4 |** Saisissez un **Certificate Name (Nom de certificat)**, tel que **`GlobalProtect_CA`**. Le nom est sensible à la casse et peut contenir 63 caractères maximum sur le pare-feu et 31 caractères maximum sur Panorama. Il doit être unique et utiliser uniquement des lettres, des nombres, des traits d'union et des traits de soulignement.

**STEP 5 |** Dans le champ **Common Name (Nom commun)**, saisissez le nom de domaine complet (FQDN) (recommandé) ou l'adresse IP de l'interface sur laquelle vous allez configurer le service qui utilisera ce certificat.

**STEP 6 |** Si le pare-feu comporte plusieurs vsys et que vous souhaitez que le certificat soit disponible pour chaque vsys, cochez la case **Shared (Partagé)**.

**STEP 7 |** Laissez le champ **Signed By (Signé par)** vide pour indiquer que le certificat est auto-signé.

**STEP 8 |** (Obligatoire) Cochez la case **Certificate Authority (Autorité de certification)**.

**STEP 9 |** Laissez le champ **OCSP Responder (Répondeur OCSP)** vide ; la vérification de l'état de révocation ne s'applique pas aux certificats CA racines.

**STEP 10 |** Cliquez sur **Generate (Générer)** et sur **Commit (Valider)**.

## Génération d'un certificat

Les pare-feu Palo Alto Networks et Panorama utilisent des certificats pour authentifier les clients, les serveurs, les utilisateurs et les périphériques dans plusieurs applications, notamment le décryptage SSL/TLS, Portail d'authentification, GlobalProtect, VPN IPSec de site à site et Accès à l'interface Web du pare-feu/de Panorama. Générez des certificats pour chaque utilisation : reportez-vous à la section Clés et certificats.

Pour générer un certificat, vous devez d'abord procéder à la création d'un certificat CA racine auto-signé ou en importer un (Importation d'un certificat et d'une clé privée) que vous signerez. Pour utiliser le Online Certificate Status Protocol (protocole de vérification des certificats en ligne ; OCSP) afin de vérifier l'état de révocation du certificat, vous devez procéder à la Configuration d'un répondeur OCSP avant de générer un certificat.

**STEP 1 |** Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**.

**STEP 2 |** Si le pare-feu comporte plusieurs systèmes virtuels (vsys), sélectionnez un **Location (Emplacement)**(vsys ou **Shared (Partagé)**) pour le certificat.

**STEP 3 |** Cliquez sur **Generate (Générer)**.

**STEP 4 |** Sélectionnez **Local (Local)** (par défaut) en tant que **Certificate Type (Type de certificat)**, sauf si vous voulez déployer des certificats SCEP vers les points de terminaison GlobalProtect.

**STEP 5 |** Saisissez un **Certificate Name (Nom de certificat)**. Le nom est sensible à la casse et peut contenir 63 caractères maximum sur le pare-feu et 31 caractères maximum sur Panorama. Il doit être unique et utiliser uniquement des lettres, des nombres, des traits d'union et des traits de soulignement.

**STEP 6 |** Dans le champ **Common Name (Nom commun)**, saisissez le nom de domaine complet (FQDN) (recommandé) ou l'adresse IP de l'interface sur laquelle vous allez configurer le service qui utilisera ce certificat.

**STEP 7 |** Si le pare-feu comporte plusieurs vsys et que vous souhaitez que le certificat soit disponible pour chaque vsys, cochez la case **Shared (Partagé)**.

**STEP 8 |** Dans le champ **Signed By (Signé par)**, sélectionnez le certificat CA racine qui émettra le certificat.

**STEP 9 |** (Facultatif) Sélectionnez un **OCSP Responder (Répondeur OCSP)**.

**STEP 10 |** Pour l'**Algorithm (Algorithme)** de génération de clés, sélectionnez **RSA (RSA)** (par défaut) ou **Elliptical Curve DSA (Algorithme de signature numérique à courbe elliptique)** (ECDSA).

L'ECDSA est recommandé pour les navigateurs et systèmes d'exploitation clients qui le prennent en charge.

*Les pare-feu exécutant PAN-OS 6.1 et versions antérieures supprimeront tous les certificats ECDSA que vous appliquez à partir de Panorama™ et aucun certificat RSA signé par une Certificate Authority (autorité de certification - CA) de certificat ECDSA ne sera valide sur ces pare-feu.*

Vous ne pouvez pas utiliser un Hardware Security Module (module de sécurité matériel ; HSM) pour stocker les clés ECDSA utilisées pour le déchiffrement SSL/TLS.

**STEP 11 |** Sélectionnez le **Number of Bits (Nombre de bits)** pour définir la longueur de la clé du certificat. Des valeurs plus élevées sont plus sûres mais nécessitent un délai de traitement plus long.

**STEP 12 |** Sélectionnez l'algorithme **Digest (Résumer)**. Classées par niveau de sûreté (de la plus à la moins sûre), les options sont les suivantes : **sha512**, **sha384**, **sha256** (par défaut), **sha1** et **md5**.

*Les certificats clients utilisés lors de la demande de services de pare-feu basés sur TLSv1.2 (comme l'accès administrateur à l'interface Web) ne peuvent avoir **sha512** comme algorithme Résumer. Les certificats clients doivent utiliser un algorithme Résumer inférieur (tel que **sha384 (sha384)**) ou vous devez limiter la **Max Version (Version max)** à **TLSv1.1 (TLSv1.1)** lorsque vous configurez les profils de service SSL/TLS pour les services de pare-feu.*

**STEP 13 |** Dans **Expiration (Expiration)**, saisissez le nombre de jours (la valeur par défaut étant 365) pendant lesquels le certificat est valide.

**STEP 14 |** (Facultatif) Cliquez sur **Add (Ajouter)** des **Certificate Attributes (Attributs du certificat)** pour identifier de façon unique le pare-feu et le service qui utiliseront le certificat.

*Si vous ajoutez un attribut **Host Name (Nom d'hôte)** (nom DNS), il est recommandé de le faire correspondre au **Common Name (Nom commun)**, car le nom d'hôte renseigne le champ autre nom de l'objet du certificat et certains navigateurs exigent que le SAN spécifie les domaines que le certificat protège. De plus, le **Host Name (Nom d'hôte)** correspondant au **Common Name (Nom commun)** est obligatoire pour GlobalProtect.*

**STEP 15 |** Cliquez sur **Generate (Générer)** puis, dans la page Device Certificates (Certificats du périphérique), cliquez sur le nom du certificat.

*Quel que soit le fuseau horaire du pare-feu, ce dernier indique toujours le Greenwich Mean Time (temps moyen de Greenwich ; GMT) correspondant pour la validité du certificat ainsi que les dates et heures d'expiration.*

**STEP 16 |** Cochez les cases qui correspondent à l'utilisation prévue du certificat sur le pare-feu.

Par exemple, si le pare-feu doit utiliser ce certificat pour sécuriser le transfert de messages Syslogs vers un serveur Syslog externe, cochez la case **Certificate for Secure Syslog (Certificat pour un message Syslog sécurisé)**.

**STEP 17 |** Cliquez sur **OK**, puis sur **Commit (Valider)**.

# Importation d'un certificat et d'une clé privée

Si votre entreprise dispose de sa propre Public Key Infrastructure (infrastructure à clé publique - PKI), vous pouvez importer un certificat et une clé privée sur le pare-feu depuis votre Certificate Authority (autorité de certification - CA) d'entreprise. Les certificats CA d'entreprise (contrairement à la plupart des certificats achetés auprès d'une CA tierce approuvée) peuvent générer automatiquement des certificats CA pour des applications, telles que le décryptage SSL/TLS ou le VPN à grande échelle.

*Sur un pare-feu Palo Alto Networks ou Panorama, vous pouvez importer des certificats auto-signés uniquement s'il s'agit de certificats CA.*

*Au lieu d'importer un certificat CA racine auto-signé sur tous les systèmes clients, il est recommandé d'importer un certificat depuis la CA d'entreprise car les clients auront déjà établi une relation de confiance avec la CA d'entreprise, ce qui simplifie le déploiement.*

*Si le certificat que vous devez importer fait partie d'une chaîne de certificats, il est recommandé d'importer toute la chaîne.*

**STEP 1 |** Depuis la CA d'entreprise, exportez le certificat et la clé privée que le pare-feu utilisera pour l'authentification.

Pour exporter une clé privée, vous devez saisir une phrase secrète pour crypter la clé en vue de son transport. Assurez-vous que le système de gestion peut accéder aux fichiers de certificats et de clés. Pour importer une clé sur le pare-feu, vous devez saisir la même phrase secrète pour la décrypter.

**STEP 2 |** Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**.

**STEP 3 |** Si le pare-feu comporte plusieurs systèmes virtuels (vsys), sélectionnez un **Location (Emplacement)**(vsys ou **Shared (Partagé)**) pour le certificat.

**STEP 4 |** Cliquez sur **Import (Importer)** et saisissez un **Certificate Name (Nom de certificat)**. Le nom est sensible à la casse et peut contenir 63 caractères maximum sur le pare-feu et 31 caractères maximum sur Panorama. Il doit être unique et utiliser uniquement des lettres, des nombres, des traits d'union et des traits de soulignement.

**STEP 5 |** Pour que le certificat soit disponible sur tous les systèmes virtuels, cochez la case **Shared (Partagé)**. Cette case à cocher apparaît uniquement si le pare-feu prend en charge plusieurs systèmes virtuels.

**STEP 6 |** Saisissez le chemin et le nom du **Certificate File (Fichier du certificat)** reçu de la part de l'autorité de certification, ou utilisez **Browse (Parcourir)** pour trouver le fichier.

**STEP 7 |** Sélectionnez un **File Format (Format de fichier)** :

- **Encrypted Private Key and Certificate (PKCS12) (Clé privée et certificat cryptés (PKCS12))** : il s'agit du format, par défaut et le plus courant, dans lequel la clé et le certificat sont enregistrés dans un conteneur unique (**Certificate File (Fichier du certificat)**). Si un module de sécurité matériel doit stocker la clé privée pour ce certificat, cochez la case **Private key resides on Hardware Security Module (La clé privée se trouve sur le module de sécurité matériel)**.

- **Base64 Encoded Certificate (PEM) (Certificat codé en base-64 (PEM))** : vous devez importer la clé séparément du certificat. Si un Hardware Security Module (module de sécurité matériel ; HSM) stocke la clé privée pour ce certificat, cochez la case **Private key resides on Hardware Security Module (La clé privée se trouve sur le module de sécurité matériel)** et ignorez l'étape suivante. Sinon, cochez la case **Import Private Key (Importer la clé privée)**, saisissez le **Key File (Fichier de clé)** ou cliquez sur **Browse (Parcourir)** pour y accéder, puis passez à l'étape suivante.

**STEP 8 |** Saisissez et confirmez la **Passphrase (Phrase secrète)** utilisée pour crypter la clé privée.

**STEP 9 |** Cliquez sur **OK**. La page Certificats du périphérique affiche le certificat importé.

## Obtention d'un certificat auprès d'une CA externe

L'avantage lorsque vous vous procurez un certificat auprès d'une Certificate Authority (autorité de certification ; CA) externe est que la clé privée ne quitte pas le pare-feu. Pour obtenir un certificat auprès d'une CA externe, générez une Certificate Signing Request (demande de signature de certificat ; CSR) et envoyez-la à la CA. Une fois que la CA aura généré un certificat doté des attributs spécifiés, importez-le sur le pare-feu. La CA peut être une CA publique réputée ou une CA d'entreprise.

Pour utiliser le Online Certificate Status Protocol (protocole de vérification des certificats en ligne ; OCSP) afin de vérifier l'état de révocation du certificat, vous devez Configurer un répondeur OCSP avant de générer la CSR.

**STEP 1 |** Demandez un certificat auprès d'une CA externe.

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**.
2. Si le pare-feu comporte plusieurs systèmes virtuels (vsys), sélectionnez un **Location (Emplacement)**(vsys ou **Shared (Partagé)**) pour le certificat.
3. Cliquez sur **Generate (Générer)**.
4. Saisissez un **Certificate Name (Nom de certificat)**. Le nom est sensible à la casse et peut contenir 63 caractères maximum sur le pare-feu et 31 caractères maximum sur Panorama.

Il doit être unique et utiliser uniquement des lettres, des nombres, des traits d'union et des traits de soulignement.

5. Dans le champ **Common Name (Nom commun)**, saisissez le nom de domaine complet (FQDN) (recommandé) ou l'adresse IP de l'interface sur laquelle vous allez configurer le service qui utilisera ce certificat.
6. Si le pare-feu comporte plusieurs vsys et que vous souhaitez que le certificat soit disponible pour chaque vsys, cochez la case **Shared (Partagé)**.
7. Dans le champ **Signed By (Signé par)**, sélectionnez **External Authority (CSR) (Autorité externe (CSR)**).
8. Le cas échéant, sélectionnez un **OCSP Responder (Répondeur OCSP)**.
9. (Facultatif) Cliquez sur **Add (Ajouter)** des **Certificate Attributes (Attributs du certificat)** pour identifier de façon unique le pare-feu et le service qui utiliseront le certificat.

   *Si vous ajoutez un attribut **Host Name (Nom d'hôte)**, il doit correspondre au **Common Name (Nom commun)** (cela est obligatoire pour GlobalProtect). Le nom d'hôte renseigne le champ Subject Alternative Name (Autre nom de l'objet) du certificat.*
10. Cliquez sur **Generate (Générer)**. L'onglet **Device Certificates (Certificats du périphérique)** affiche la CSR avec l'état `pending`.

**STEP 2 |** Envoyez la CSR à la CA.

1. Sélectionnez la CSR et cliquez sur **Export (Exporter)** pour enregistrer le fichier .csr sur un ordinateur local.
2. Chargez le fichier .csr sur la CA.

**STEP 3 |** Importez le certificat.

1. Dès que la CA envoie un certificat signé en réponse à la CSR, retournez dans l'onglet **Device Certificates (Certificats du périphérique)** et cliquez sur **Import (Importer)**.
2. Saisissez le **Certificate Name (Nom de certificat)** utilisé pour générer la CSR à l' à .
3. Saisissez le chemin et le nom du **Certificate File (Fichier du certificat)** PEM que la CA a envoyé ou cliquez sur **Browse (Parcourir)** pour y accéder.
4. Cliquez sur **OK**. L'onglet **Certificats de périphérique** affiche le certificat avec le statut `valide`.

**STEP 4 |** Configurez le certificat.

1. Cliquez sur le **Name (Nom)** du certificat.
2. Cochez les cases qui correspondent à l'utilisation prévue du certificat sur le pare-feu. Par exemple, si le pare-feu doit utiliser ce certificat pour sécuriser le transfert de messages Syslogs vers un serveur Syslog externe, cochez la case **Certificate for Secure Syslog (Certificat pour un message Syslog sécurisé)**.
3. Cliquez sur **OK**, puis sur **Commit (Valider)**.

## Installation d'un certificat de périphérique

Votre pare-feu nouvelle génération peut exploiter des services dans le cloud tels que la télémétrie du périphérique et l'IdO. Pour ce faire, vous devez installer un certificat de périphérique pour

authentifier avec succès le pare-feu auprès du portail de support client (CSP) de Palo Alto Networks afin d'exploiter ces services dans le cloud. Les circonstances dans lesquelles un certificat de périphérique est requis diffèrent d'une fonctionnalité à l'autre. N'installez donc un certificat de périphérique que si la documentation de configuration de la fonctionnalité vous indique que cela doit être fait.

Vous ne devez installer un certificat de périphérique qu'une seule fois. Toutes les fonctionnalités qui utilisent des certificats de périphériques utiliseront le certificat installé sur votre pare-feu s'il existe déjà.

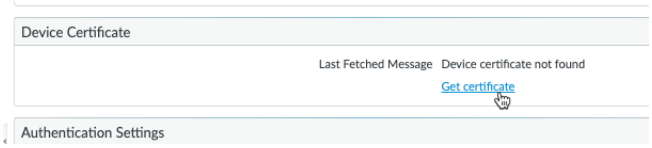
Vous pouvez installer un certificat de périphérique sur les pare-feu gérés par Panorama. Si vous souhaitez installer un certificat de périphérique directement sur un pare-feu nouvelle génération individuel (c'est-à-dire que vous n'utilisez ***pas*** Panorama) :

**STEP 1 |** Générer le One-Time Password (mot de passe à usage unique ; OTP).

1. Ouvrez une session dans le portail de support client.
2. Sélectionnez **Assets (Ressources)** > **Device Certificates (Certificats de périphériques)** et **Generate OTP (Générer un OTP)**.
3. Pour le **Device Type (Type de périphérique)**, sélectionnez **Generate OTP for Next-Gen Firewalls (Générer un OTP pour les pare-feu nouvelle génération)**.
4. Sélectionnez votre numéro de série **PAN OS Device (Périphérique PAN OS)**.
5. **Generate OTP (Générez un OTP)** puis copiez-le.

**STEP 2 |** Connectez-vous à votre pare-feu nouvelle génération en tant qu'utilisateur admin.

**STEP 3 |** Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **Device Certificate (Certificat de périphérique)** et **Get Certificate (Obtenir un certificat)**.




**STEP 4 |** Saisissez le **One-Time Password (mot de passe à usage unique - OTP)** que vous avez généré puis cliquez sur **OK**.

**STEP 5 |** Votre pare-feu nouvelle génération récupère et installe le certificat avec succès.

## Déploiement de certificats au moyen de SCEP

Si vous disposez d'un serveur Simple Certificate Enrollment Protocol (protocole de recrutement de certificat simple ; SCEP) dans votre infrastructure à clé publique d'entreprise, vous pouvez configurer un profil SCEP pour automatiser la génération et la distribution de certificats de clients uniques. L'opération SCEP est dynamique dans la mesure où la CPI d'entreprise génère un certificat spécifique à l'utilisateur lorsque le client SCEP le demande et envoie le certificat au client SCEP. Le client SCEP déploie de manière transparente le certificat au périphérique client.

Vous pouvez utiliser un profil SCEP avec GlobalProtect pour associer des certificats clients spécifiques à l'utilisateur à chaque utilisateur GlobalProtect. Dans le présent cas pratique, le portail GlobalProtect fait office de client SCEP pour le serveur SCEP de votre infrastructure à clé publique d'entreprise. De plus, vous pouvez utiliser un profil SCEP pour affecter des certificats de clients à des

périphériques Palo Alto Networks pour l'authentification mutuelle avec d'autres périphériques Palo Alto Networks pour l'accès de gestion et la communication entre appareils.

**STEP 1 |** Créez un profil SCEP.

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **SCEP (SCEP)**, puis **Add (Ajouter)** un nouveau profil.
2. Saisissez un **Name (Nom)** pour identifier le profil.
3. S'il s'agit du profil d'un pare-feu pouvant prendre en charge de multiples systèmes virtuels, sélectionnez un système virtuel ou sélectionnez l'option **Shared (Partagé)** en tant que **Location (Emplacement)** où le profil est disponible.

**STEP 2 |** (**Facultatif**) Pour rendre la génération de certificats basée sur SCEP plus sécurisée, configurez un mécanisme de réponse au défi SCEP entre l'ICP et le portail pour chaque demande de certificat.

Après avoir configuré ce mécanisme, son fonctionnement est invisible et aucune autre intervention de votre part n'est nécessaire.

Pour vous conformer à la U.S. Federal Information Processing Standard (norme de traitement de l'information fédérale ; FIPS), utilisez un mécanisme SCEP **Dynamic** (Dynamique) et précisez un **Server URL** (URL du serveur) qui utilise HTTPS.

Sélectionnez l'une des options suivantes :

- **None (Aucune)** (**par défaut**) : le serveur SCEP n'envoie pas de demande d'authentification au portail avant de générer un certificat.
- **Fixed (Réglé)** : obtenez le mot de passe du défi d'inscription du serveur SCEP dans l'infrastructure ICP, puis saisissez le mot de passe dans le champ Mot de passe.
- **Dynamic (Dynamique)** : indiquez un nom d'utilisateur et un MPUU de votre choix (peuvent être les informations d'identification de l'administrateur ICP) et l'**Server URL (URL du serveur)** SCEP où le portail/client enverra ces informations d'identification. L'utilisation des informations d'identification pour s'authentifier auprès du serveur SCEP qui génère de manière transparente un mot de passe UU pour le portail sur chaque demande de certificat. (Lors de chaque demande de certificat, vous pouvez afficher ce changement de MPUU après un rafraîchissement de l'écran dans le champ « `Le mot de passed'authentification est` ».) L'ICP transmet au portail de manière transparente chaque nouveau mot de passe. Le portail utilise ensuite le mot de passe pour sa demande de certificat.

**STEP 3 |** Spécifiez les paramètres de connexion entre le serveur SCEP et le portail pour permettre au portail de demander et de recevoir des certificats clients.

Vous pouvez inclure des informations supplémentaires sur le périphérique client ou l'utilisateur en spécifiant des signes dans le nom du **Subject (sujet)** du certificat.

Le portail inclut la valeur de signe et l'ID d'hôte dans la demande RSE au serveur SCEP.

1. Configurez la **Server URL (URL du serveur)** que le portail utilise pour atteindre le serveur SCEP dans la PKI (par exemple, `http://10.200.101.1/certsrv/mscep/`).
2. Saisissez une chaîne (jusqu'à 255 caractères de longueur) dans le champ **CA-IDENT Name (Nom AC-IDENT)** pour identifier le serveur SCEP.
3. Saisissez le nom de **Subject (Sujet)** à utiliser pour les certificats générés par le serveur SCEP. Le sujet doit être un nom différent au format **<attribute>=<value>** et doit

inclure l'attribut du nom commun (CN) (**CN=<variable>**). Le CN prend en charge les jetons dynamiques suivants :

- **$USERNAME** : utilisez ce jeton pour permettre au portail de demander des certificats pour un utilisateur spécifique. Pour utiliser cette variable avec GlobalProtect, vous devez également Activer le mappage de groupe. Le nom d'utilisateur saisi par l'utilisateur doit correspondre au nom figurant dans la table de mappage du groupe d'utilisateurs.
- **$EMAILADDRESS** : utilisez ce jeton pour demander des certificats associés à une adresse e-mail spécifique. Pour utiliser cette variable, vous devez également Activer le mappage de groupe et configurer les **Mail Attributes (Attributs de messagerie)** dans la section des domaines de messagerie du profil de serveur. Si GlobalProtect ne peut pas identifier une adresse e-mail pour l'utilisateur, il génère un identifiant unique et remplit le CN avec cette valeur.
- **$HOSTID** : pour demander des certificats pour le périphérique uniquement, spécifiez le jeton ID d'hôte. Lorsqu'un utilisateur tente de se connecter au portail, le point de terminaison envoie des informations d'identification qui incluent sa valeur d'ID d'hôte. La valeur d'ID d'hôte varie selon le type de périphérique, soit GUID (Windows), adresse MAC de l'interface (Mac), Android ID (appareils Android), UDID (périphériques iOS), ou un nom unique qui GlobalProtect assigne (Chrome).
- **$UDID** : utilisez l'attribut de nom commun UDID pour demander des certificats en fonction de l'UDID de GlobalProtect ou le numéro de série du périphérique aux fins de l'authentification mutuelle entre les périphériques Palo Alto Networks.

Lorsque le portail GlobalProtect applique les paramètres SCEP à l'agent, la portion CN du nom du sujet est remplacée par la valeur réelle (username, ID d'hôte ou adresse e-mail) du propriétaire du certificat (par exemple, **O=acme,CN=johndoe**).

4. Sélectionnez le **Subject Alternative Name Type (Type de nom alternatif de sujet)** :

   *Utilisez des entrées statiques pour l'autre type de nom de l'objet. Le pare-feu ne prend pas en charge les jetons dynamiques tels que **$USERNAME**.*

   - **RFC 822 Name (Nom RFC 822)** : saisissez le nom de la messagerie dans l'objet du certificat ou l'extension alternative du nom de l'objet.
   - **DNS Name (Nom DNS)** : saisissez le nom DNS utilisé pour évaluer les certificats.
   - **Uniform Resource Identifier (Identificateur de ressource uniforme)** : saisissez le nom de la ressource à partir de laquelle le client obtient le certificat.
   - **None (Aucun)** : ne spécifiez pas d'attributs pour le certificat.

**STEP 4 |** (**Facultatif**) Configurez les paramètres cryptographiques du certificat.

- Sélectionnez la longueur de la clé (**Number of Bits (Nombre de bits)**) pour le certificat.

  Si le pare-feu est en mode FIPS-CC et que l'algorithme de génération de clés est RSA. Les clés RSA doivent être de 2.048 bits ou plus.
- Sélectionnez le **Digest for CSR (Résumé pour CSR)** qui indique l'algorithme de synthèse pour la demande de signature de certificat (CSR) : sha1, sha256 ou sha384.

**STEP 5 |** (**Facultatif**) Configurez les utilisations autorisées du certificat, soit pour la signature ou le chiffrement.

- Pour utiliser ce certificat pour la signature, activez la case à cocher **Use as digital signature (Utiliser comme signature numérique)**. Cela permet au point de terminaison d'utiliser la clé privée dans le certificat pour valider une signature numérique.
- Pour utiliser ce certificat pour le chiffrement, activez la case à cocher **Use for key encipherment (Utiliser pour le chiffrement des clés)**. Sélectionnez cette option pour configurer le terminal client afin d'utiliser la clé privée dans le certificat dans le but de crypter les données échangées par le biais de la connexion HTTPS établie avec les certificats générés par le serveur SCEP.

**STEP 6 |** (**Facultatif**) Pour veiller à ce que le portail se connecte au bon serveur SCEP, saisissez le **CA Certificate Fingerprint (Empreinte du certificat de l'autorité de certification)**. Vous pouvez obtenir cette empreinte auprès de l'interface du serveur SCEP dans le champ « Empreinte numérique ».

1. Entrez l'URL de l'interface utilisateur du serveur SCEP (par exemple, **`http://<hostname or IP>/CertSrv/mscep_admin/`**).
2. Copiez l'empreinte numérique et saisissez-la dans le champ **CA Certificate Fingerprint (Empreinte du certificat de l'autorité de certification)**.

**STEP 7 |** Activez l'authentification SSL mutuelle entre le serveur SCEP et le pare-feu. C'est nécessaire pour se conformer à la norme FIPS (Federal Information Processing Standard) des États-Unis.

*(L'opération FIPS-CC est indiquée sur la page de connexion du pare-feu et dans la barre d'état du pare-feu.)*

Sélectionnez le **CA Certificate (Certificat CA)** racine du serveur SCEP. Vous pouvez activer l'authentification SSL mutuelle entre le serveur SCEP et le pare-feu en sélectionnant **Client Certificate (Certificat client)**.

**STEP 8 |** Enregistrez et validez la configuration.

1. Cliquez sur **OK** pour enregistrer les paramètres puis fermez la boîte de dialogue SCEP.
2. **Commit (Validez)** la configuration.

Le portail tente de demander un certificat CA à l'aide des paramètres du profil SCEP et l'enregistre sur le pare-feu hébergeant le portail. En cas de succès, le certificat CA est affiché dans **Device (Périphérique)** > **Certificate Management (Gestion de certificat)** > **Certificates (Certificats)**.

**STEP 9 |** (**Facultatif**) Si, après avoir enregistré le profil SCEP, le portail ne parvient pas à obtenir le certificat, vous pouvez générer manuellement une demande de signature de certificat (CSR) à partir du portail.

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphériques)**, puis cliquez sur **Generate (Générer)**.
2. Saisissez un **Certificate Name (Nom de certificat)**. Ce nom ne peut contenir d'espaces.
3. Sélectionnez le **SCEP Profile (Profil SCEP)** qui doit servir à l'envoi d'une CSR à la PKI de votre entreprise.
4. Cliquez sur **OK** pour soumettre la demande et générer le certificat.

# Exportation d'un certificat et d'une clé privée

Palo Alto Networks recommande d'utiliser la Public Key Infrastructure (infrastructure à clés publiques - PKI) de votre entreprise pour attribuer un certificat et une clé privée à votre organisation. Cependant, le cas échéant, vous pouvez également exporter un certificat et une clé privée depuis le pare-feu ou Panorama. Vous pouvez utiliser un certificat et une clé privée exportés dans les cas suivants :

- Configuration de l'authentification administrateur basée sur les certificats pour l'interface Web
- Activation de SSL entre des composants du LSVPN GlobalProtect dans le but de configurer l'authentification de l'application ou de l'agent GlobalProtect aux portails et aux passerelles
- Décryptage du proxy de transfert SSL
- Obtention d'un certificat auprès d'une CA externe

**STEP 1 |** Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**.

**STEP 2 |** Si le pare-feu comporte plusieurs systèmes virtuels (vsys), sélectionnez un **Location (Emplacement)** (un vsys spécifique ou **Shared (Partagé)**) pour le certificat.

**STEP 3 |** Sélectionnez le certificat, cliquez sur **Export (Exporter)** et sélectionnez un **File Format (Format de fichier)** :

- **Base64 Encoded Certificate (PEM) (Certificat codé Base64 (PEM))** : il s'agit du format par défaut. Ce format est le plus répandu et le plus largement pris en charge sur Internet. Si vous souhaitez que le fichier exporté puisse inclure la clé privée, cochez la case **Export Private Key (Exporter la clé privée)**.
- **Encrypted Private Key and Certificate (PKCS12) (Clé privée et certificat cryptés (PKCS12))** : ce format est plus sûr que le format PEM, mais n'est pas aussi répandu ou aussi largement pris en charge. Le fichier exporté inclura automatiquement la clé privée.
- **Binary Encoded Certificate (DER) (Certificat codé binaire (DER))** : davantage de types de systèmes d'exploitation prennent ce format en charge contrairement aux autres formats. Vous ne pouvez exporter que le certificat (pas la clé) : ignorez la case à cocher **Export Private Key (Exporter la clé privée)** et les champs Phrase secrète.

**STEP 4 |** Saisissez une **Passphrase (Phrase secrète)** et cliquez sur **Confirm Passphrase (Confirmer la phrase secrète)** pour crypter la clé privée si le **File Format (Format de fichier)** est PKCS12 ou si le format est PEM et que vous avez coché la case **Export Private Key (Exporter la clé privée)**. Vous utiliserez cette phrase secrète lorsque vous importerez le certificat et la clé dans les systèmes clients.

**STEP 5 |** Cliquez sur **OK (OK)** pour enregistrer le certificat/fichier de clé sur votre ordinateur.

# Configuration d'un profil de certificat

Les profils de certificat définissent l'authentification de l'utilisateur et du périphérique pour le portail d'authentification, l'authentification multifacteur (MFA), GlobalProtect, VPN IPSec de site à site, la validation de la liste dynamique externe (EDL), le DNS dynamique (DDNS), l'accès à l'agent User-ID et à l'agent TS et l'accès à l'interface Web aux pare-feu Palo Alto Networks ou à Panorama. Les profils indiquent les certificats qui doivent être utilisés, comment vérifier l'état de révocation des certificats et de quelle façon cet état permet de restreindre l'accès. Configurez un profil de certificat pour chaque application.

*Il est recommandé d'activer Online Certificate Status Protocol (protocole de vérification des certificats en ligne ; OCSP) et la vérification de l'état de la Certificate Revocation List (liste de révocation de certificats ; CRL) des profils de certificats pour vérifier que le certificat n'a pas été révoqué. Activez OCSP et CRL de sorte que le pare-feu utilise CRL en cas d'indisponibilité du serveur OCSP. Pour plus d'informations sur ces méthodes, reportez-vous à la section* Révocation de certificats**.**

**STEP 1 |** Récupérez des certificats Certificate Authority (autorité de certification - CA) que vous allez affecter.

Exécutez l'une des étapes suivantes pour obtenir des certificats CA que vous affecterez au profil. Vous devez en affecter au moins un.

- Génération d'un certificat.
- Exportez un certificat depuis votre CA d'entreprise, puis importez-le sur le pare-feu (reportez-vous à l'étape 3).

**STEP 2 |** Identifiez le profil de certificat.

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil des certificats)** et cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name (Nom)** pour identifier le profil. Celui-ci est sensible à la casse, doit être unique et peut contenir un maximum de 63 caractères sur le pare-feu ou de 31 caractères sur Panorama, composés uniquement de lettres, de nombres, d'espaces, de traits d'union et de traits de soulignement.
3. Si le pare-feu comporte plusieurs systèmes virtuels (vsys), sélectionnez un **Location (Emplacement)**(vsys ou **Shared (Partagé)**) pour le certificat.

**STEP 3 |** Affectez un ou plusieurs certificats.

Procédez comme suit pour chaque certificat CA :

1. Dans le tableau Certificats AC, cliquez sur **Add (Ajouter)**.
2. Sélectionnez un **CA Certificate (Certificat CA)**. Vous pouvez également importer un certificat. Pour cela, cliquez sur **Import (Importer)**, saisissez un **Certificate Name (Nom de certificat)**, cliquez sur **Browse (Parcourir)** pour accéder au **Certificate File (Fichier de certificat)** que vous avez exporté depuis votre CA d'entreprise, puis cliquez sur **OK (OK)**.
3. (**Facultatif**) Si le pare-feu utilise la méthode OCSP pour vérifier l'état de révocation du certificat, vous pouvez configurer les champs suivants pour appliquer un contrôle

prioritaire sur le comportement par défaut. Pour la plupart des déploiements, ces champs ne s'appliquent pas.

- Par défaut, le pare-feu utilise les informations tension d'Authority Information Access (accès aux informations de l'autorité ; AIA) du certificat pour extraire les informations du répondeur OCSP. Pour appliquer un contrôle prioritaire sur les informations d'AIA, saisissez une **Default OCSP URL (URL OCSP par défaut)** (commençant par **`http://`** ou par **`https://`**).
- Par défaut, le pare-feu utilise le certificat sélectionné dans le champ **CA Certificate (Certificat AC)** pour valider les réponses OCSP. Pour utiliser un certificat différent pour la validation, sélectionnez-le dans le champ **OCSP Verify CA Certificate (Certificat AC pour la vérification OCSP)**.

4. Cliquez sur **OK**. Le tableau Certificats CA affiche le certificat affecté.

**STEP 4 |** Définissez les méthodes de vérification de l'état de révocation du certificat et le comportement de blocage associé.

1. Sélectionnez **Use CRL (Utiliser CRL)** et/ou **Use OCSP (Utiliser OCSP)**. Si vous sélectionnez les deux méthodes, le pare-feu essaiera d'abord le protocole OCSP et ne fera appel à la méthode CRL que si le répondeur OCSP est indisponible.
2. En fonction de la méthode de vérification, saisissez le **CRL Receive Timeout (Délai de réception CRL)** et/ou le **OCSP Receive Timeout (Délai de réception OCSP)**. Il s'agit de la durée (1-60 secondes) au bout de laquelle le pare-feu n'attend plus la réponse du service CRL/OCSP.
3. Saisissez le **Certificate Status Timeout (Délai d'expiration du statut du certificat)**. Il s'agit de la durée (1-60 secondes) au bout de laquelle le pare-feu n'attend plus la réponse d'aucun service d'état de certificat et applique la logique de blocage de la session que vous avez définie. Le **Certificate Status Timeout (Délai d'expiration du statut du certificat)** correspond au **Receive Timeout (Délai de réception)** des méthodes OCSP/CRL de la manière suivante :
   - Si vous activez les deux méthodes, OCSP et CRL : le pare-feu enregistre un délai d'expiration de la demande après l'expiration de la plus courte des deux durées : la valeur **Certificate Status Timeout (Délai d'expiration du statut du certificat)** ou l'agrégation des deux valeurs **Receive Timeout (Délai de réception)**.
   - Si vous activez uniquement la méthode OCSP : le pare-feu enregistre un délai d'expiration de la demande après l'expiration de la plus courte des deux durées : la valeur **Certificate Status Timeout (Délai d'expiration du statut du certificat)** ou la valeur **Receive Timeout (Délai de réception)** par la méthode OCSP.
   - Si vous activez uniquement la méthode CRL : le pare-feu enregistre un délai d'expiration de la demande après l'expiration de la plus courte des deux durées : la valeur **Certificate Status Timeout (Délai d'expiration du statut du certificat)** ou la valeur **Receive Timeout (Délai de réception)** par la méthode CRL.
4. Si vous souhaitez que le pare-feu bloque les sessions lorsque le service OCSP ou CRL renvoie l'état de révocation de certificat inconnu, sélectionnez **Block session if certificate status is unknown (Bloquer une session si l'état du certificat est inconnu)**. Sinon, le pare-feu autorise la session.
5. Si vous souhaitez que le pare-feu bloque les sessions après avoir enregistré un délai d'expiration de la demande OCSP ou CRL, sélectionnez **Block session if certificate status**

**cannot be retrieved within timeout (Bloquer une session si l'état du certificat ne peut pas être récupéré avant le délai d'expiration)**. Sinon, le pare-feu autorise la session.

6. (**GlobalProtect uniquement**) Si vous souhaitez que le pare-feu bloque les sessions lorsque l'attribut numéro de série qui figure dans le champ sujet du certificat client ne correspond par à l'ID de l'hôte que l'application GlobalProtect signale pour le point de terminaison, sélectionnez **Block sessions if the certificate was not issued to the authenticating device (Bloquer des sessions si le certificat n'a pas été délivré au périphérique d'authentification)**.

**STEP 5 |** Cliquez sur **OK (OK)**, puis sur **Commit (Valider)**.

# Configuration d'un profil de service SSL/TLS

Les pare-feu Palo Alto Networks et Panorama utilisent les profils de service SSL/TLS pour spécifier un certificat ainsi que les versions de protocole autorisées pour les services SSL/TLS. Le pare-feu et Panorama utilisent SSL/TLS pour le portail d'authentification, les portails et passerelles GlobalProtect, le trafic entrant sur l'interface de gestion (MGT), la fonctionnalité de contrôle prioritaire sur l'URL par l'administrateur et le service d'écoute Syslog User-ID™. En définissant les versions de protocole, vous pouvez utiliser un profil pour limiter les suites de cryptage disponibles pour sécuriser les communications avec les clients demandant les services. En permettant au pare-feu ou à Panorama d'éviter les versions SSL/TLS qui ont des lacunes connues, la sécurité du réseau est ainsi renforcée. Si une requête de service touche une version de protocole qui ne figure pas dans la plage précisée, le pare-feu ou Panorama met à niveau la connexion vers une version ultérieure ou antérieure qui est prise en charge.

*En ce qui concerne les systèmes clients qui requièrent les services d'un pare-feu, la Certificate Trust Liste (liste d'approbation de certificats ; CTL) doit inclure le certificat de la Certificate Authority (autorité de certification ; CA) qui a délivré le certificat spécifié dans le profil de service SSL/TLS. Dans le cas contraire, les utilisateurs constateront une erreur de certificat lorsqu'ils solliciteront les services du pare-feu. La plupart des certificats d'une tierce CA sont présents par défaut sur les navigateurs des clients. Si une entreprise ou une CA de certificat généré par un pare-feu est l'émetteur, vous devez déployer ce certificat CA à la liste CTL dans les navigateurs des clients.*

**STEP 1 |** Pour chaque service souhaité, générez ou importez un certificat sur le pare-feu (reportez-vous à la section Obtention des certificats).

*N'utilisez pas de certificats CA pour les profils de service SSL/TLS ; utilisez uniquement des certificats signés.*

**STEP 2 |** Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **SSL/TLS Service Profile (Profil de service SSL/TLS)**.

**STEP 3 |** Si le pare-feu comporte plusieurs systèmes virtuels (vsys), sélectionnez le **Location (Emplacement)** (vsys ou **Shared (Partagé)**) dans lequel le profil est disponible.

**STEP 4 |** Cliquez sur **Add (Ajouter)** et saisissez un **Name (Nom)** pour identifier le profil.

**STEP 5 |** Sélectionnez le **Certificate (Certificat)** que vous venez d'obtenir.

**STEP 6 |** Définissez la plage de protocoles que le service peut utiliser :

- Pour la **Min Version (Version min.)**, sélectionnez la version TLS la plus ancienne autorisée : **TLSv1.0 (TLSv1.0)** (par défaut), **TLSv1.1 (TLSv1.1)** ou **TLSv1.2 (TLSv1.2)**.
- Pour la **Max Version (Version max.)**, sélectionnez la version TLS la plus récente autorisée : **TLSv1.0 (TLSv1.0)**, **TLSv1.1 (TLSv1.1)**, **TLSv1.2 (TLSv1.2)** ou **Max (Max)** (version disponible la plus récente). La valeur par défaut est **Max (Max)**.

*Il est recommandé de définir la **Min Version (Version min)** sur **TLSv1.2** et la **Max Version (Version max)** sur **Max**.*

*__TLSv1.1 (TLSv1.1)__ est la version de TLS la plus ancienne qui est prise en charge sur les pare-feu en mode FIPS-CC sur lesquels PAN-OS 8.0 ou une version ultérieure de PAN-OS est installé ; ne sélectionnez pas __TLSv1.0 (TLSv1.0)__.*

*Les certificats clients qui sont utilisés lors de la demande de services de pare-feu reposant sur TLSv1.2 ne peuvent pas avoir SHA512 en tant qu'algorithme de cryptage. Les certificats clients doivent utiliser un algorithme de cryptage inférieur (tel que SHA384) ou vous devez limiter la __Max Version (Version max)__ à __TLSv1.1 (TLSv1.1)__ pour les services du pare-feu.*

**STEP 7 |** Cliquez sur **OK**, puis sur **Commit (Valider)**.

# Configuration d'un profil de service SSH

Les profils de service SSH vous permettent de personnaliser les paramètres SSH afin d'améliorer la sécurité et l'intégrité des connexions SSH à vos appareils de gestion et de haute disponibilité (HA) Palo Alto Networks. Par défaut, SSH prend en charge tous les chiffrements, les algorithmes d'échange de clés et les codes d'authentification des messages, ce qui rend votre connexion vulnérable aux attaques. Avec un profil de service SSH, vous pouvez restreindre les algorithmes que votre serveur SSH prend en charge. Vous pouvez également générer une nouvelle clé hôte et spécifier des seuils de volume de données, de temps et de paquets pour la régénération et l'échange de clés de session SSH.

Selon l'instance du serveur SSH, configurez un profil de service SSH de gestion ou HA. Vous pouvez configurer les profils depuis le pare-feu ou l'interface web Panorama™ (si vous appliquez des paramètres sur plusieurs pare-feu ou appareils) ou le CLI.

*Vous pouvez configurer un maximum de quatre profils de gestion et de quatre profils de serveur HA.*

*Pour utiliser les mêmes paramètres de connexion SSH pour chaque collecteur de journaux dédié (M-Series ou appareil virtuel Panorama en mode collecteur de journaux) dans un Collector Group (Groupe de collecteurs), configurez un profil de service SSH à partir du serveur de gestion Panorama, **Commit (validez)** les changements dans Panorama, puis **Push (poussez)** la configuration vers les collecteurs de journaux. Vous pouvez également effectuer ces étapes depuis le CLI en utilisant les commandes **`set log-collector-group <name> general-setting management ssh`**.*

- Création d'un profil de gestion SSH
- Création d'un profil HA SSH

## Création d'un profil de gestion SSH

Vous devez créer un profil de gestion SSH pour personnaliser les paramètres SSH des connexions de gestion.

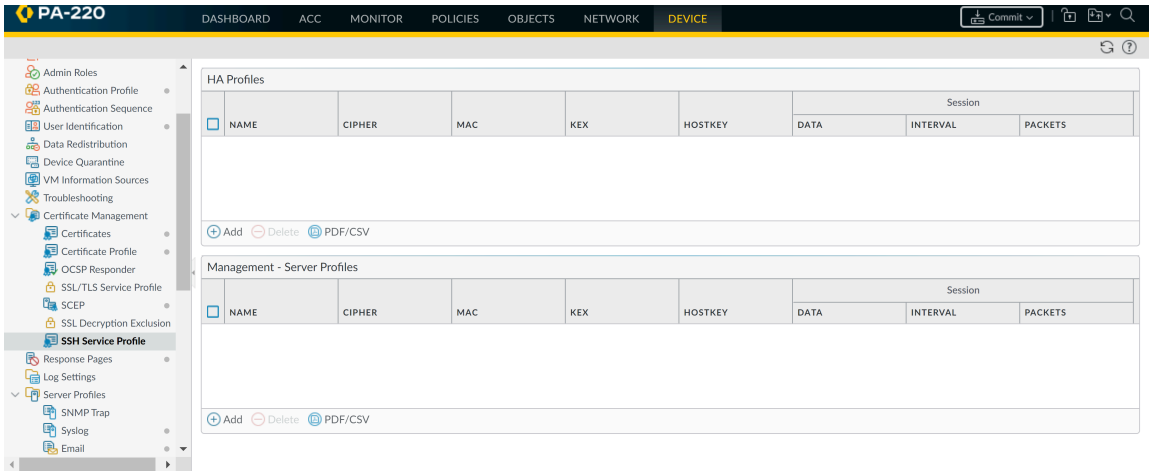
*Vous pouvez configurer ou mettre à jour un profil de gestion existant à partir de votre CLI.*

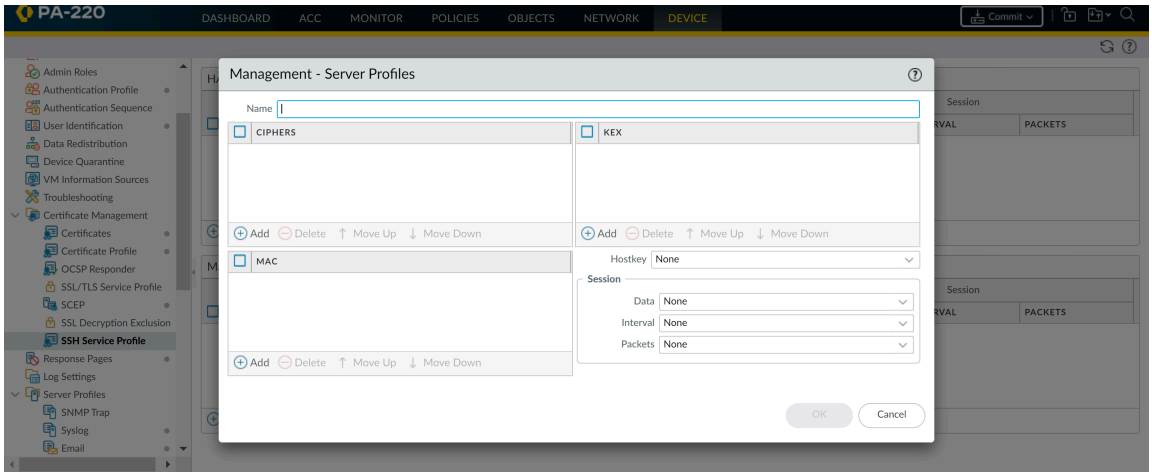
**STEP 1 |** Création d'un profil de gestion - serveur.

1. Sélectionnez **Device (Périphérique)** > **Certification Management (Gestion de certification)** > **SSH Service Profile (Profil de service SSH)**.
2. **Add (ajoutez)** un profil de gestion - serveur.



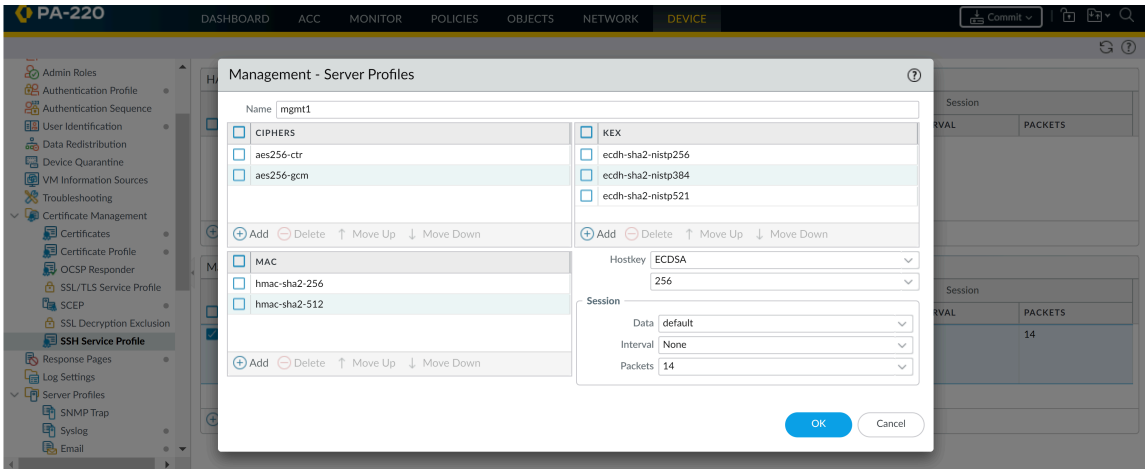

 



3. Saisissez un **Name (Nom)** pour identifier le profil.
4. (Facultatif) **Add (ajoutez)** les chiffrements, les codes d'authentification de message ou les algorithmes d'échange de clés que le profil prendra en charge.
5. (Facultatif) Sélectionnez une **Hostkey (Clé d'hôte)** et une longueur de clé.
6. (Facultatif) Saisissez les valeurs des paramètres de changement de clé de la session SSH : **Data (Données)**, **Interval (Intervalle)** et **Packets (Paquets)**.



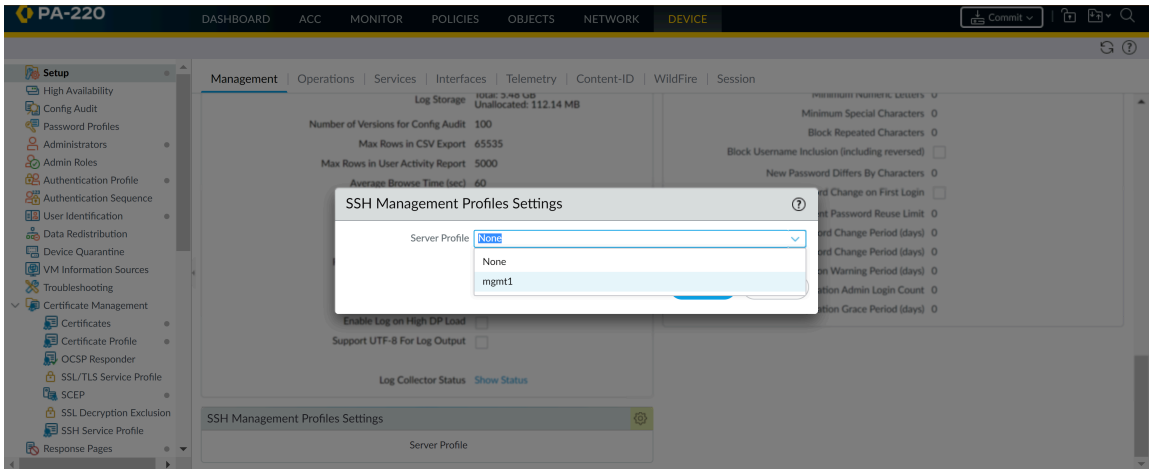
7. Cliquez sur **OK**, puis sur **Commit (Valider)**.

**STEP 2 |** Sélectionnez un profil de gestion à appliquer.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)**. Sous SSH Management Profiles Settings (Paramètres des profils de gestion SSH), sélectionnez un profil existant.



2. Cliquez sur **OK** et sur **Commit (Valider)** pour enregistrer les modifications.

**STEP 3 |** Redémarrer le service SSH de gestion de la CLI pour appliquer le profil.

Vous devez redémarrer la connexion chaque fois que vous appliquez un nouveau profil ou que vous apportez des modifications à un profil en cours d'utilisation ; cela permet de redémarrer l'appareil. Les nouvelles configurations n'affecteront pas les sessions actives. Le profil s'appliquera aux connexions (ou sessions) ultérieures.

1. admin@PA-3260> **set ssh service-restart mgmt**

## Création d'un profil HA SSH

Pour sécuriser les communications SSH entre les appareils d'une paire HA, vous devez créer un profil HA SSH. Avant de pouvoir créer un profil, vous devez établir une connexion HA entre les appareils. Si une connexion HA n'a pas été établie, vous devez activer le chiffrement sur la connexion de la liaison de contrôle, exportez la clé HA vers un emplacement réseau et importez la clé HA sur l'homologue. (Reportez-vous aux rubriques Configuration de la HA active/passive ou Configuration de la HA active/active).

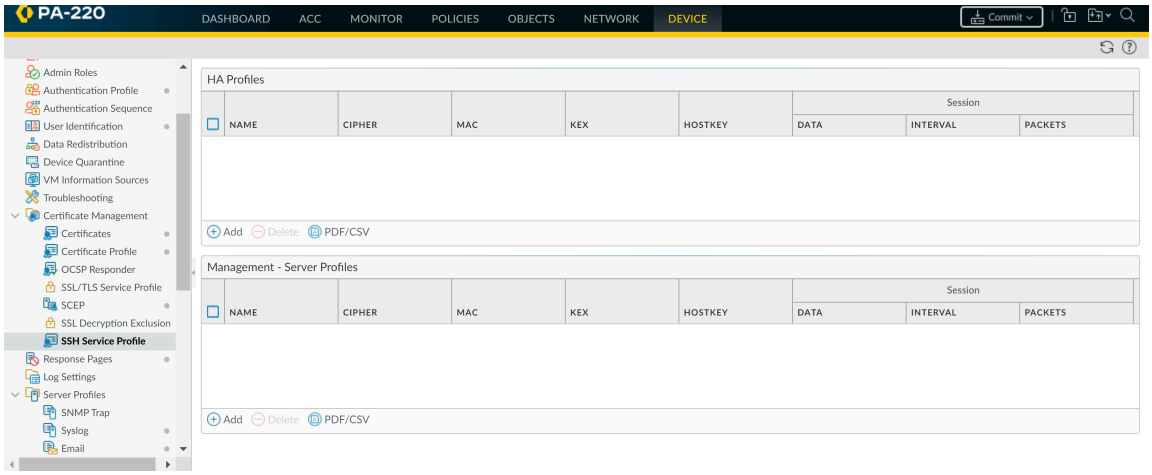
*Vous pouvez configurer ou mettre à jour un profil HA existant à partir de votre CLI.*

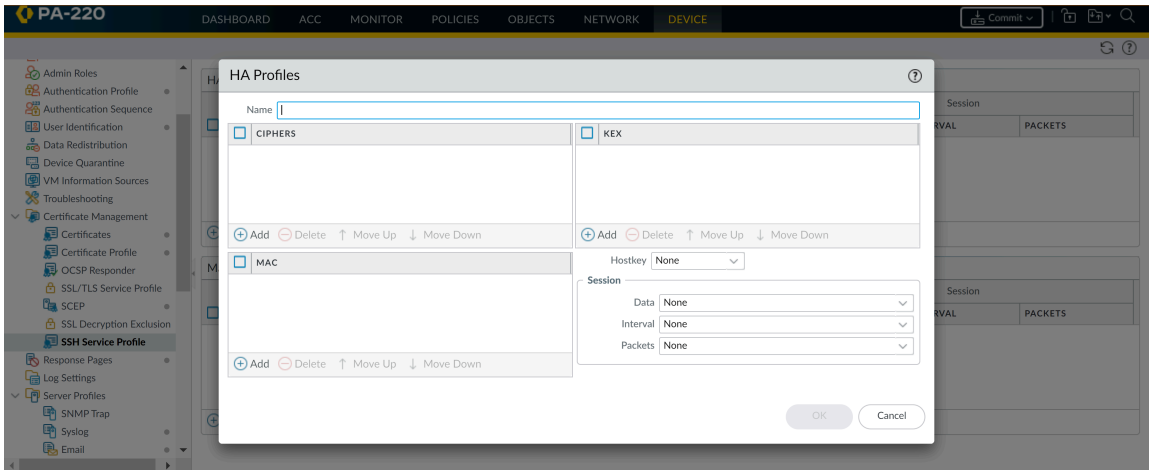
**STEP 1 |** Création d'un profil HA.

1. Sélectionnez **Device (Périphérique)** > **Certification Management (Gestion de certification)** > **SSH Service Profile (Profil de service SSH)**.
2. **Add (ajoutez)** un profil HA.



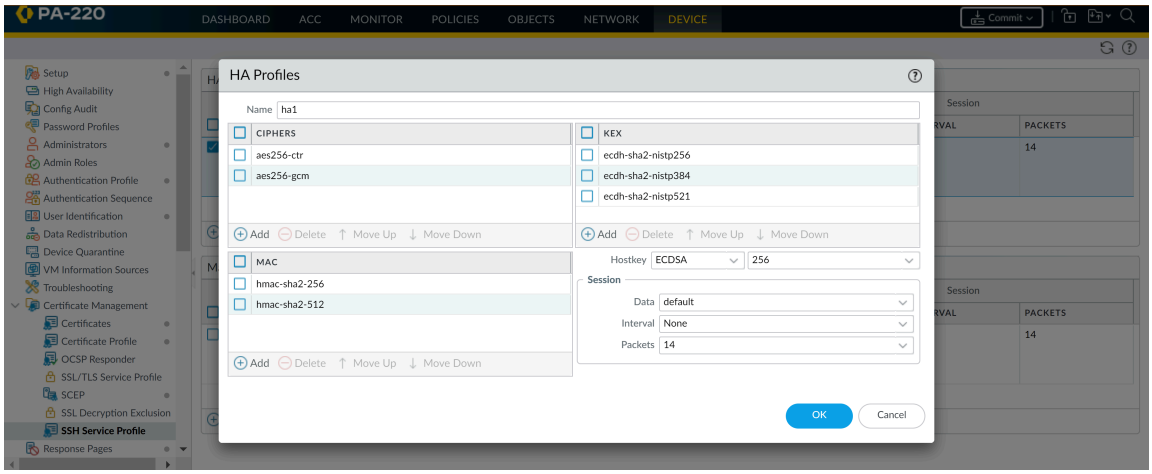

 



3. Saisissez un **Name (Nom)** pour identifier le profil.
4. (Facultatif) **Add (ajoutez)** les chiffrements, les codes d'authentification de message ou les algorithmes d'échange de clés que le profil prendra en charge.
5. (Facultatif) Sélectionnez une **Hostkey (Clé d'hôte)** et une longueur de clé.
6. (Facultatif) Saisissez les valeurs des paramètres de changement de clé de la session SSH : **Data (Données)**, **Interval (Intervalle)** et **Packets (Paquets)**.



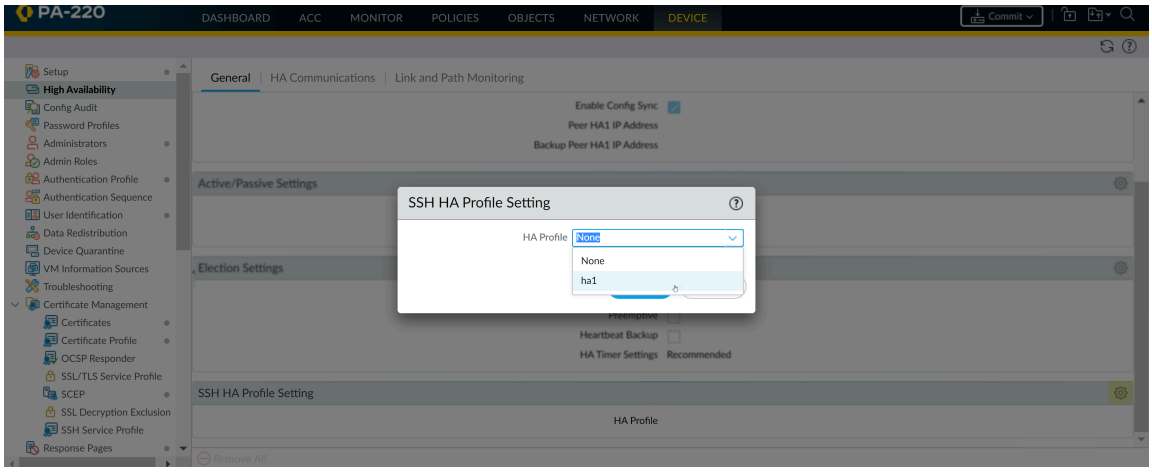
7. Cliquez sur **OK**, puis sur **Commit (Valider)**.

**STEP 2 |** Sélectionnez un profil HA à appliquer.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**. Sous SSH HA Profile Setting (Paramètres du profil HA SSH), sélectionnez un profil existant.



2. Cliquez sur **OK** et sur **Commit (Valider)** pour enregistrer les modifications.

**STEP 3 |** Redémarrer le service SSH HA1 de la CLI pour appliquer le profil.

Vous devez redémarrer la connexion chaque fois que vous appliquez un nouveau profil ou que vous apportez des modifications à un profil en cours d'utilisation ; cela permet de redémarrer l'appareil. La nouvelle configuration n'affectera pas les sessions actives. Le profil s'appliquera aux connexions (ou sessions) ultérieures.

1. admin@PA-3260> **set ssh service-restart ha**

   *Vous pouvez utiliser les commandes suivantes si la connexion entre la paire HA a été établie et que vous souhaitez minimiser le temps d'arrêt qui accompagne un redémarrage du service SSH. Si aucune connexion HA n'a été établie, vous devez redémarrer le service SSH.*

   - *(La liaison HA1 de secours est configurée) admin@PA-3260>* ***request high-availability session-reestablish***
   - *(Aucune liaison HA1 de secours n'est configurée ou la liaison HA1 de secours est en panne) admin@PA-3260>* ***request high-availability session-reestablish force***

     *Vous pouvez forcer le pare-feu à rétablir les sessions HA1 s'il n'y a pas de liaison HA1 de secours, ce qui cause une brève situation de « split brain » entre les homologues HA. (L'utilisation de l'option* ***force*** *lorsqu'une liaison HA1 de secours est configurée n'a aucun effet.)*

# Remplacement du certificat du trafic de gestion entrant

Lorsque vous démarrez le pare-feu ou Panorama pour la première fois, ce dernier génère automatiquement un certificat par défaut qui autorise l'accès HTTPS à l'interface Web et l'API XML sur l'interface de gestion (MGT) et (sur le pare-feu uniquement) sur toute interface qui prend en charge le trafic de gestion HTTPS (pour plus d'informations, reportez-vous à la section Utilisation des profils de gestion d'interface pour limiter l'accès). Pour renforcer la sécurité du trafic de gestion sortant, remplacez le certificat défini par défaut par un nouveau certificat délivré spécialement pour votre organisation.

*Vous ne pouvez afficher, modifier ou supprimer le certificat par défaut.*

*Pour sécuriser le trafic de gestion, il faut également* Configurer les comptes administrateurs et les authentifications**.**

**STEP 1 |** Obtenez le certificat qui permettra d'authentifier le pare-feu ou Panorama auprès des systèmes client des administrateurs.

Vous pouvez simplifier votre Déploiement des certificats en utilisant un certificat qui est déjà approuvé par les systèmes client. Par conséquent, nous vous recommandons de procéder à l'Importation d'un certificat et d'une clé privée à partir de votre certificate authority (autorité de certificat ; CA) d'entreprise ou à l'Obtention d'un certificat auprès d'une CA externe ; la boutique des certificats racines approuvés des systèmes client dispose probablement déjà du certificat CA racine approuvé qui garantit la confiance.

*Si vous procédez à la* Génération d'un certificat *sur le pare-feu ou sur Panorama, les administrateurs constateront une erreur de certificat, étant donné que le certificat CA racine ne se trouve pas dans la boutique des certificats racines approuvés des systèmes client. Pour éviter ce problème, déployez le certificat CA racine auto-signé sur tous les systèmes client.*

*Peu importe la méthode utilisée pour obtenir le certificat, nous recommandons d'opter pour un algorithme* ***Digest sha256*** *ou supérieur pour renforcer la sécurité.*

**STEP 2 |** Configurez un profil de service SSL/TLS.

Sélectionnez le **Certificate (Certificat)** que vous venez d'obtenir.

*Pour une sécurité renforcée, nous vous recommandons de définir la* ***Min Version (Version min)*** *(version TLS la plus ancienne autorisée) sur* ***TLSv1.2*** *pour le trafic de gestion entrant. Nous vous recommandons d'utiliser un profil de service SSL/TLS distinct pour chaque service du pare-feu ou de Panorama plutôt que de réutiliser ce profil pour tous les services.*

**STEP 3 |** Appliquer le profil de service SSL/TLS au trafic de gestion entrant.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les paramètres généraux.
2. Sélectionnez le **SSL/TLS Service Profile (Profil de service SSL/TLS)** que vous venez de configurer.
3. Cliquez sur **OK**, puis sur **Commit (Valider)**.

# Configuration de la taille de clé des certificats du serveur proxy de transfert SSL

Lorsqu'il répond à un client dans une session de proxy de transfert SSL, le pare-feu crée une copie du certificat qui lui est présenté par le serveur de destination et l'utilise pour établir une connexion avec le client. Par défaut, le pare-feu génère des certificats avec la même taille de clé que le certificat que le serveur de destination a présenté. Vous pouvez toutefois modifier la taille de clé du certificat généré par le pare-feu comme suit :

**STEP 1 |** Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Session (Session)** puis, dans la section Decryption Settings (Paramètres de décryptage), cliquez sur **SSL Forward Proxy Settings (Paramètres du proxy de transfert SSL)**.

**STEP 2 |** Sélectionnez une **Key Size (Taille de clé)** :

- **Defined by destination host (Définie par l'hôte de destination)** : le pare-feu détermine la taille de clé et l'algorithme de hachage avec lesquels les certificats sont générés pour établir des sessions de proxy SSL avec les clients en fonction du certificat du serveur de destination. Si le serveur de destination utilise une clé RSA de 1,024 bits, le pare-feu générera un certificat avec une clé RSA de 1 024 bits. Si le serveur de destination utilise une taille de clé supérieure à 1 024 bits (par exemple, 2 048 ou 4 096 bits), le pare-feu générera un certificat qui utilisera une clé RSA de 2 048 bits. Si le serveur de destination utilise l'algorithme de hachage SHA-1, le pare-feu génère un certificat avec l'algorithme de hachage SHA-1. Si le serveur de destination utilise un algorithme de hachage plus fort que SHA-1, le pare-feu génère un certificat avec l'algorithme de hachage SHA-256. Il s'agit du paramètre par défaut.
- **1024-bit RSA (RSA de 1 024 bits)** : le pare-feu génère des certificats qui utilisent une clé RSA de 1 024 bits et un algorithme de hachage SHA-256, quelle que soit la taille de clé des certificats du serveur de destination. Depuis le 31 décembre 2013, les Certificate Authorities (autorités de certification - CA) publiques et les navigateurs les plus courants ont limité la prise en charge des certificats X.509 qui utilisent des clés de moins de 2 048 bits. À l'avenir, selon les paramètres de sécurité définis, lorsque de telles clés lui sont présentées, un navigateur peut avertir l'utilisateur ou bloquer entièrement la session SSL/TLS.
- **2048-bit RSA (RSA de 2 048 bits)** : le pare-feu génère des certificats qui utilisent une clé RSA de 2 048 bits et un algorithme de hachage SHA-256, quelle que soit la taille de clé des certificats du serveur de destination. Les CA publiques et les navigateurs les plus courants prennent en charge les clés de 2 048 bits qui offrent une meilleure sécurité que les clés de 1 024 bits.

*La modification de la taille de clé efface le cache actuel des certificats.*

**STEP 3 |** Cliquez sur **OK**, puis sur **Commit (Valider)**.

# Révocation et renouvellement des certificats



## Révocation d'un certificat

Diverses circonstances peuvent invalider un certificat avant sa date d'expiration. Il peut s'agir par exemple d'un changement de nom, d'un changement d'association entre le sujet et l'autorité de certification (par exemple, un employé termine sa mission), et d'un état compromis (connu ou suspecté) de la clé privée. Dans ces circonstances, la Certificate Authority (autorité de certification ; CA) qui a généré le certificat doit le révoquer. La tâche qui suit explique comment révoquer un certificat pour lequel le pare-feu est la CA.

**STEP 1 |** Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**.

**STEP 2 |** Si le pare-feu prend en charge les systèmes virtuels multiples, l'onglet affiche une liste déroulante **Location (Emplacement)**. Sélectionnez le système virtuel auquel le certificat appartient.

**STEP 3 |** Sélectionnez le certificat à révoquer.

**STEP 4 |** Cliquez sur **Revoke (Révoquer)**. PAN-OS définit immédiatement l'état du certificat sur révoqué et ajoute le numéro de série à la mémoire cache du répondeur Online Certificate Status Protocol (protocole de vérification des certificats en ligne ; OCSP) ou à la Certificate Revocation List (liste de révocation de certificats ; CRL). Aucune validation n'est requise.

## Renouvellement d'un certificat

Si un certificat expire, ou doit expirer sous peu, vous pouvez réinitialiser la période de validité. Si une Certificate Authority (autorité de certification ; CA) externe a signé le certificat et que le pare-feu utilise la méthode Online Certificate Status Protocol (protocole de vérification des certificats en ligne ; OCSP) pour vérifier l'état de révocation du certificat, le pare-feu utilisera les informations du répondeur OCSP pour mettre à jour l'état du certificat (reportez-vous à la section Configuration d'un répondeur OCSP). Si le pare-feu est la CA ayant généré le certificat, le pare-feu le remplacera par un nouveau certificat doté d'un numéro de série différent mais des mêmes attributs que l'ancien.

**STEP 1 |** Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**.

**STEP 2 |** Si le pare-feu comporte plusieurs systèmes virtuels (vsys), sélectionnez un **Location (Emplacement)**(vsys ou **Shared (Partagé)**) pour le certificat.

**STEP 3 |** Sélectionnez le certificat à renouveler et cliquez sur **Renew (Renouveler)**.

**STEP 4 |** Saisissez un **New Expiration Interval (Nouveau délai d'expiration)** (en jours).

**STEP 5 |** Cliquez sur **OK**, puis sur **Commit (Valider)**.

# Sécurisation des clés avec un module de sécurité matériel (HSM)

Un Hardware Security Module (module de sécurité matériel - HSM) est un dispositif physique qui gère les clés numériques. Il sert à générer et à stocker des clés numériques en toute sécurité. Il offre une protection à la fois logique et physique de ces équipements matériels contre toute utilisation non autorisée et tout menace potentielle.

Les clients HSM intégrés aux pare-feu Palo Alto Networks et à Panorama activent la sécurité renforcée pour les clés privées utilisées dans le décryptage SSL/TLS (le proxy de transfert SSL, ainsi que l'inspection SSL entrante). Vous pouvez également utiliser le HSM pour crypter les clés principales.

Les rubriques suivantes expliquent comment intégrer un HSM à votre pare-feu ou à Panorama :

- Paramétrage de la connectivité à un module de sécurité matériel (HSM)
- Cryptage d'une clé principale à l'aide d'un HSM
- Enregistrement des clés privées sur un HSM
- Gestion du déploiement du HSM

## Paramétrage de la connectivité à un module de sécurité matériel (HSM)

Les clients HSM sont intégrés aux pare-feu PA-3200 Series, PA-5200 Series, PA-7000 Series et VM-Series et sur le serveur de gestion Panorama (appareils virtuels et M-Series) à utiliser avec les HSM suivants :

- **nCipher nShield Connect** : les versions du client prises en charge dépendent de la version de PAN-OS :
  - PAN-OS 10.1 prend en charge la version client 12.40.2 (rétrocompatible jusqu'à la version client 11.50 pour les anciens appareils).
  - PAN-OS 9.1, 9.0 et 8.1 prennent en charge la version client 12.30.
  - PAN-OS 8.0 et les versions antérieures prennent en charge la version 11.62.
- **SafeNet Network** : Les versions clients compatibles dépendent de la version de PAN-OS :
  - PAN-OS 10.1 prend en charge les versions client 5.4.2 et 7.2.
  - PAN-OS 9.1 et 9.0 prennent en charge les versions client 5.4.2 et 6.3.
  - PAN-OS 8.1 prend en charge les versions client 5.4.2 et 6.2.2.
  - PAN-OS 8.0.2 et les versions ultérieures de PAN-OS 8.0 (ainsi que PAN-OS 7.1.10 et les versions ultérieures de PAN-OS 7.1) prennent en charge les versions client 5.2.1, 5.4.2 et 6.2.2.

La version du serveur HSM doit être compatible avec les versions de ces clients. Reportez-vous à la documentation du fournisseur HSM pour la matrice de compatibilité de la version client/serveur. Sur le pare-feu ou sur Panorama, utilisez la procédure suivante pour sélectionner la version du client SafeNet Network qui est compatible avec votre serveur HSM SafeNet.

*La rétrogradation des serveurs HSM pourrait ne pas être une option après que vous avez procédé à leur mise à niveau.*

- Configuration de la connectivité à un HSM SafeNet Network
- Configuration de la connectivité à un HSM nCipher nShield Connect

- Installez le SafeNet Client RPM Packet Manager (Gestionnaire de paquets RPM du client SafeNet).
  1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **HSM (Module de sécurité matériel)**, puis **Select HSM Client Version (Sélectionnez la version du client HSM)** (paramètres Opérations de sécurité matérielle).
  2. Sélectionnez **Version 5.4.2** (par défaut) ou **7.2**, selon ce qui correspond à la version de votre serveur HSM.
  3. Cliquez sur **OK**.
  4. (Obligatoire uniquement si vous modifiez la version HSM sur le pare-feu) Si le changement de version fonctionne, le pare-feu vous invite à redémarrer pour passer à la nouvelle version HSM. Si vous êtes invité à redémarrer, cliquez sur **Yes (Oui)**.
  5. Si la clé principale ne se trouve pas sur le pare-feu, la mise à niveau de la version du client échouera. **Close (Fermez)** le message et assurez-vous que la clé principale soit locale au pare-feu :
     - Modifiez le Fournisseur du module matériel de sécurité et désactivez (décochez) l'option **Master Key Secured by HSM (Clé principale sécurisée par le module de sécurité matériel)**.
     - Cliquez sur **OK**.
     - Sélectionnez **Device (Périphérique)** > **Master Key and Diagnostics (Clé principale et diagnostics)**, puis modifiez la Master Key (Clé principale).
     - Saisissez la **Current Master Key (Clé principale active)** ; vous pouvez ensuite saisir cette même clé dans les champs **New Master Key (Nouvelle clé principale)** et **Confirm New Master Key (Confirmez la nouvelle clé principale)**.
     - Cliquez sur **OK**.
     - Répétez les quatre premières étapes pour **Select HSM Client Version (Sélectionner la version du client HSM)**, puis redémarrez de nouveau.

## Configuration de la connectivité à un HSM SafeNet Network

Pour configurer la connectivité entre un pare-feu Palo Alto Networks (client HSM) et un serveur SafeNet Network, vous devez définir l'adresse IP de ce serveur, saisir un mot de passe pour authentifier le pare-feu sur le serveur, puis enregistrer le pare-feu avec le serveur. Avant de commencer à configurer votre client HSM, créez une partition pour le pare-feu sur le serveur HSM, puis confirmez que la version du client SafeNet Network sur le pare-feu est compatible avec votre serveur HSM SafeNet Network HSM (reportez-vous à la section Paramétrage de la connectivité à un module de sécurité matériel (HSM)).

Avant que le HSM et le pare-feu puissent se connecter, le HSM doit authentifier le pare-feu grâce à l'adresse IP du pare-feu. Ainsi, lorsque vous configurez le pare-feu, celui-ci doit avoir une adresse IP statique, et non une adresse dynamique attribuée par un serveur DHCP. Les opérations sur le HSM cessent de fonctionner si l'adresse IP du pare-feu vient à changer pendant leur exécution.

*Les configurations HSM ne sont pas synchronisées entre les pare-feu homologues High Availability (haute disponibilité ; HD). C'est pourquoi vous devez configurer le HSM individuellement sur chacun des homologues. Dans les configurations HD d'une configuration active/passive, vous devez déclencher un basculement manuel pour configurer et authentifier chaque homologue HD individuellement sur le HSM. Une fois le basculement manuel effectué, l'interaction entre les utilisateurs n'est pas requise pour que le basculement fonctionne correctement.*

**STEP 1 |** Saisissez les paramètres de connexion pour chaque HSM SafeNet Network.

1. Connectez-vous à l'interface Web du pare-feu et sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **HSM**.
2. Modifiez les paramètres de Fournisseur de module de sécurité matériel et sélectionnez **Safenet Network HSM (HSM SafeNet Network)** comme **Provider Configured (Fournisseur configuré)**.
3. **Add (Ajoutez)** chaque serveur HSM comme suit. Les configurations HSM HD (Haute disponibilité) nécessitent au moins deux serveurs. Votre nœud peut contenir un maximum de 16 serveurs HSM. Tous les serveurs HSM du nœud peuvent exécuter la même version de SafeNet et doivent s'authentifier distinctement. Vous devriez utiliser un nœud SafeNet uniquement lorsque vous souhaitez répliquer les clés à l'échelle du nœud. Vous pouvez également ajouter un maximum de 16 serveurs HSM SafeNet qui fonctionneront de manière autonome.
   1. Saisissez un **Module Name (Nom de module)** (une chaîne ASCII composée d'un maximum de 31 caractères) à donner au serveur HSM.
   2. Saisissez une adresse IPv4 pour l'**Server Address (Adresse du serveur)** HSM.
4. (HA uniquement) Sélectionnez **High Availability (Haute disponibilité)**, précisez la valeur de **Auto Recovery Retry (Tentative de rétablissement automatique)** (nombre maximal de fois que le client HSM tente de rétablir sa connexion à un serveur HSM avant de basculer vers le serveur HSM homologue HA ; la plage est comprise entre 0 et 500 ; la valeur par défaut est 0), puis saisissez un **High Availability Group Name (Nom du groupe de haute disponibilité)** (une chaîne ASCII composée d'un maximum de 31 caractères).

   *Si vous configurez deux serveurs HSM ou plus, il est recommandé d'activer la **High Availability (Haute Disponibilité)**. Autrement, le pare-feu n'utilise pas les autres serveurs HSM.*
5. Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.

**STEP 2 |** (Facultatif) Configurez un itinéraire de service pour autoriser le pare-feu à se connecter au HSM si vous ne voulez pas qu'il utilise l'interface de gestion (par défaut).

*Si vous configurez un itinéraire de service pour le HSM, le déclenchement de la commande CLI* ***clear session all*** *effacera toutes les sessions existantes du HSM, ce qui provoque la désactivation et l'activation de tous les états du HSM. Pendant les quelques secondes nécessaires au rétablissement du HSM, toutes les opérations SSL/TLS se solderont par un échec.*

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Services** et cliquez sur **Service Route Configuration (Configuration de l'itinéraire de service)**.
2. **Customize (Personnalisez)** un Itinéraire de service. L'onglet **IPv4** est activé par défaut.
3. Cliquez sur **HSM** dans la colonne Service.
4. Sélectionnez une **Source Interface (Interface Source)** pour le HSM.
5. Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.

**STEP 3 |** Configurez le pare-feu pour qu'il s'authentifie sur le HSM.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** et **Setup Hardware Security Module (Configurez le module de sécurité matériel)**.
2. Sélectionnez le **Server Name (Nom du serveur)**.
3. Sélectionnez **Automatic (Automatique)** ou **Manual (Manuel)** pour votre d'authentification et certificat de confiance.
4. Saisissez le **Administrator Password (Mot de passe administrateur)** pour authentifier le pare-feu sur le HSM.
5. Cliquez sur **OK**.

   Le pare-feu tente d'effectuer une authentification auprès du HSM et affiche un message d'état.
6. Cliquez de nouveau sur **OK**.

**STEP 4 |** Enregistrez le pare-feu comme client du HSM sur le serveur HSM et affectez-le à une partition sur le serveur HSM.

*Si le HSM compte un pare-feu avec le même <nom-cl> enregistré, vous devez supprimer le doublon d'enregistrement en exécutant la commande suivante avant la fin de l'enregistrement :* ***client delete-client <nom-cl>****, où <nom-cl> est le nom du client enregistré (pare-feu) que vous souhaitez supprimer.*

1. Connectez-vous au HSM depuis un système distant.
2. Enregistrez le pare-feu à l'aide de la commande de la CLI suivante : **client register -c *<nom-cl>* -ip *<adresse-ip-de-transfert>***, où *<nom-cl>* est un nom que vous affectez au pare-feu à utiliser sur le HSM et *<adresse-ip-de-transfert>* est l'adresse IP du pare-feu.
3. Affectez une partition au pare-feu à l'aide de la commande de la CLI suivante : **client assignpartition -c *<nom-cl>* -p *<nom-de-la-partition>*** où *<nom-cl>* est le nom affecté au pare-feu dans la commande **client register** et *<nom-de-la-*

*partition>* est le nom d'une partition configurée précédemment que vous souhaitez affecter au pare-feu.

**STEP 5 |** Configurez le pare-feu pour qu'il se connecte à la partition du HSM.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **HSM** et actualisez ( ) l'affichage.
2. Sélectionnez **Setup HSM Partition (Configurer la partition du HSM)** (paramètres Opérations de sécurité matérielle).
3. Saisissez le **Partition Password (Mot de passe de la partition)** pour authentifier le pare-feu sur la partition du HSM.
4. Cliquez sur **OK**.

**STEP 6 |** (Configuration HD uniquement) Répétez les étapes précédentes d'authentification, d'enregistrement et de connexion à une partition pour ajouter un nouveau HSM au groupe HD existant.

*Si vous enlevez une configuration HSM, répétez les étapes précédentes de connexion à une partition pour enlever un HSM supprimé du groupe HD.*

**STEP 7 |** Vérifiez la connexion du pare-feu avec le HSM ainsi que l'authentification.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **HSM** et vérifiez l'état de la connexion :
   - **Vert** : le pare-feu est authentifié et connecté avec succès au HSM.
   - **Rouge** : le pare-feu n'a pas été authentifié ou la connectivité réseau au HSM est en panne.
2. Consultez les colonnes suivantes dans l'État du module de sécurité matériel pour déterminer l'état d'authentification :
   - **Serial Number (Numéro de série)** : le numéro de série de la partition du HSM si le pare-feu été authentifié avec succès.
   - **Partition** : Le nom de la partition du module de sécurité matériel qui a été affectée sur le pare-feu.
   - **Module State (État du module)** : état actuel de la connexion HSM. Cette valeur est toujours `Authenticated(Authentifié)` si l'État du module de sécurité matériel affiche le HSM.

## Configuration de la connectivité à un HSM nCipher nShield Connect

Vous devez obligatoirement configurer un Remote File System (système de fichiers distants ; RFS) à utiliser en tant que concentrateur afin de synchroniser les données de clés pour tous les pare-feux (clients HSM) de votre organisation qui utilisent le HSM nCipher nShield Connect. Afin de vous assurer que la version client de nShield Connect sur vos pare-feu est compatible avec votre serveur nShield Connect, reportez-vous à la section Configuration de la connectivité à un HSM.

Avant que le HSM et les pare-feu puissent se connecter, le HSM doit authentifier les pare-feu grâce à leur adresse IP. Ainsi, lorsque vous configurez les pare-feu, ceux-ci doivent avoir une adresse IP statique, et non une adresse dynamique attribuée par un serveur DHCP. (Les opérations sur le HSM cessent de fonctionner si l'adresse IP du pare-feu vient à changer pendant leur exécution.)

*Les configurations HSM ne sont pas synchronisées entre les pare-feu homologues High Availability (haute disponibilité ; HD). C'est pourquoi vous devez configurer le HSM individuellement sur chacun des homologues. Dans les configurations HD d'une configuration active/passive, vous devez déclencher un basculement manuel pour configurer et authentifier chaque homologue HD individuellement sur le HSM. Une fois le basculement manuel effectué, l'interaction entre les utilisateurs n'est pas requise pour que le basculement fonctionne correctement.*

**STEP 1 |** Saisissez les paramètres de connexion pour chaque HSM nCipher nShield Connect.

1. Connectez-vous à l'interface Web du pare-feu et sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **HSM**.
2. Modifiez les paramètres du Fournisseur de module de sécurité matériel et sélectionnez **nShield Connect** comme **Provider Configured (Fournisseur configuré)**.
3. **Add (Ajoutez)** chaque serveur HSM comme suit. Les configurations HSM HD nécessitent deux serveurs.
   1. Saisissez un **Module Name (Nom de Module)** pour le serveur HSM. Il peut s'agir de n'importe quelle chaîne ASCII de 31 caractères maximum.
   2. Saisissez une adresse IPv4 pour l'**Server Address (Adresse du serveur)** HSM.
4. Saisissez une adresse IPv4 pour l'**Remote Filesystem Address (Adresse du système de fichiers distants)**.
5. Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.

**STEP 2 |** (Facultatif) Configurez un itinéraire de service pour autoriser le pare-feu à se connecter au HSM si vous ne voulez pas qu'il utilise l'interface de gestion (par défaut).

*Si vous configurez un itinéraire de service pour le HSM, le déclenchement de la commande CLI* ***`clear session all`*** *effacera toutes les sessions existantes du HSM, ce qui provoque la désactivation et l'activation de tous les états du HSM. Pendant les quelques secondes nécessaires au rétablissement du HSM, toutes les opérations SSL/TLS se solderont par un échec.*

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Services** et cliquez sur **Service Route Configuration (Configuration de l'itinéraire de service)**.
2. **Customize (Personnalisez)** un Itinéraire de service. L'onglet **IPv4** est activé par défaut.
3. Cliquez sur **HSM** dans la colonne Service.
4. Sélectionnez une **Source Interface (Interface Source)** pour le HSM.
5. Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.

**STEP 3 |** Enregistrez le pare-feu comme le client du HSM avec le serveur HSM.

Cette étape décrit sommairement la procédure à suivre pour utiliser l'interface de la façade du HSM nShield Connect. Pour obtenir plus d'informations, consultez la documentation sur nCipher.

1. Connectez-vous à l'affichage du panneau frontal du HSM nCipher nShield Connect.
2. Utilisez le bouton de navigation droit pour sélectionner **System (Système)** > **System Configuration (Configuration du système)** > **Client Config (Configuration du client)** > **New Client (Nouveau client)**.
3. Saisissez l'adresse IP du pare-feu.
4. Sélectionnez **System (Système)** > **System Configuration (Configuration du système)** > **Client config (Configuration du client)** > **Remote file system (Système de fichiers à distance)** et saisissez l'adresse IP de l'ordinateur client sur lequel vous avez paramétré le système de fichiers distant.

**STEP 4 |** Configurez le RFS afin qu'il accepte des connexions depuis le pare-feu.

1. Connectez-vous au système de fichiers distant (RFS) depuis un client Linux.
2. Obtenez le numéro de série électronique (ESN) et le hachage de la clé $K_{NETI}$, qui authentifie le HSM auprès de clients, en exécutant la commande de la CLI **anonkneti *<ip-address>*** , où *<ip-address>* est l'adresse IP du HSM.

   Par exemple :

   ```
   anonkneti 192.0.2.1
   ```

   ```
   B1E2-2D4C-E6A2 5a2e5107e70d525615a903f6391ad72b1c03352c
   ```

   Dans cet exemple, `B1E2-2D4C-E6A2` est le numéro de série électronique (ESN) et `5a2e5107e70d525615a903f6391ad72b1c03352c` est le hachage de la clé $K_{NETI}$.
3. Saisissez la commande suivante depuis un compte super utilisateur pour configurer le système de fichiers distants :

   ```
   rfs-setup --force <ip-address> <ESN> <hash-Kneti-key>
   ```

   *<adresse-IP>* est l'adresse IP du HSM, *<ESN>* est le numéro de série électronique, et *<hachage-clé-Kneti>* est le hachage de la clé $K_{NETI}$.

   L'exemple suivant utilise les valeurs obtenues dans cette procédure :

   ```
   rfs-setup --force 192.0.2.1 B1E2-2D4C-E6A2
    5a2e5107e70d525615a903f6391ad72b1c03352c
   ```
4. Exécutez la commande suivante pour autoriser un client HSM à envoyer des fichiers sur le système de fichiers distants :

   ```
   rfs-setup --gang-client --write-noauth <FW-IPaddress>
   ```

   où *<FW-IPaddress>* est l'adresse IP du pare-feu.

**STEP 5 |** Authentifiez le pare-feu sur le HSM.

1. Dans l'interface Web du pare-feu, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **HSM** et **Setup Hardware Security Module (Configurer le module de sécurité matériel)**.
2. Cliquez sur **OK**.

   Le pare-feu tente d'effectuer une authentification auprès du HSM et affiche un message d'état.
3. Cliquez sur **OK**.

**STEP 6 |** Synchronisez le pare-feu avec le RFS en sélectionnant **Device (Périphérique)** > **Setup (Configuration)** > **HSM** et **Synchronize with Remote Filesystem (Synchroniser avec Système de fichiers distants)**.

**STEP 7 |** Vérifiez la connexion du pare-feu avec le HSM ainsi que l'authentification.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **HSM** et vérifiez l'état de la connexion :
   - **Vert** : le pare-feu est authentifié et connecté avec succès au HSM.
   - **Rouge** : le pare-feu n'a pas été authentifié ou la connectivité réseau au HSM est en panne.
2. Consultez l'état du module de sécurité matériel pour déterminer l'état d'authentification.
   - **Name (Nom)** – Le nom du module de sécurité matériel.
   - **IP Address (Adresse IP)** – L'adresse IP du HSM.
   - **Module State (État du module)** : état actuel de la connexion HSM : `Authenticated (Authentifié)` ou `NotAuthenticated (Non authentifié)`.

## Cryptage d'une clé principale à l'aide d'un HSM

Un clé principale chiffre toutes les clés privées et mots de passe du pare-feu et de Panorama. Si vous avez des exigences de sécurité pour stocker vos clés privées dans un emplacement sécurisé, vous pouvez crypter la clé principale à l'aide d'une clé de cryptage qui est enregistrée sur un HSM. Le pare-feu ou Panorama demande ensuite au HSM de déchiffrer la clé principale chaque fois qu'un mot de passe ou une clé privée doit être décrypté(e) sur le pare-feu. Normalement, le HSM est situé dans un emplacement hautement sécurisé qui est indépendant du pare-feu ou de Panorama pour une sécurité accrue.

Le HSM crypte la clé principale à l'aide d'une clé d'encapsulation. Pour maintenir la sécurité, vous devez occasionnellement changer (rafraîchir) cette clé d'encapsulation.

*Les pare-feu configurés en mode FIPS-CC ne prennent pas en charge le chiffrement des clés principales au moyen d'un HSM.*

Les rubriques suivantes expliquent comment chiffrer initialement la clé principale, puis comment actualiser son cryptage :

- Cryptage de la clé principale
- Actualiser le cryptage de la clé principale

### Cryptage de la clé principale

Si vous n'avez pas précédemment crypté la clé principale sur un équipement, utilisez la procédure suivante. Suivez cette procédure lorsque vous cryptez une clé pour la première fois ou si vous définissez une nouvelle clé principale et que vous souhaitez la crypter. Pour actualiser le cryptage sur une clé précédemment cryptée, reportez-vous à la section Actualisation du cryptage de la clé principale.

**STEP 1 |** Sélectionnez **Device (Périphérique)** > **Master Key and Diagnostics (Clé principale et diagnostics)**.

**STEP 2 |** Indiquez la clé actuellement utilisée pour crypter toutes les clés privées et tous les mots de passe sur le pare-feu dans le champ **Master Key (Clé principale)**.

**STEP 3 |** Si vous devez changer la clé principale, saisissez la nouvelle clé principale et confirmez-la.

**STEP 4 |** Cochez la case **HSM (Module de sécurité matériel)**.

- **Life Time (Durée de vie)** : nombre de jours et d'heures au bout desquel(le)s la clé principale arrive à expiration (période de 1 à 730 jours).
- **Time for Reminder (Heure de rappel)** : nombre de jours et d'heures avant l'expiration lorsque l'utilisateur est informé de l'expiration imminente (période de 1 à 365 jours).

**STEP 5 |** Cliquez sur **OK**.

### Actualiser le cryptage de la clé principale

Il est recommandé d'actualiser régulièrement le cryptage de la clé principale en procédant à la rotation de la clé d'encapsulation. La fréquence de cette rotation dépend de votre application. La clé d'encapsulation se trouve dans votre HSM. Cette commande est la même pour les deux types de HSM, SafeNet Network et nCipher nShield Connect.

**STEP 1 |** Connectez-vous à l'ILC du pare-feu.

**STEP 2 |** Saisissez la commande CLI suivante pour effectuer la rotation de la clé d'encapsulation pour la clé principale d'un HSM :

```
> request hsm mkey-wrapping-key-rotation
```

Si la clé principale est cryptée sur le HSM, la commande CLI générera une nouvelle clé d'encapsulation sur le HSM et cryptera la clé principale avec la nouvelle clé d'encapsulation.

Si la clé principale n'est pas cryptée sur le HSM, la commande CLI générera une nouvelle clé d'encapsulation sur le HSM pour une prochaine utilisation.

L'ancienne clé d'encapsulation n'est pas supprimée par cette commande.

## Enregistrement des clés privées sur un HSM

Pour une sécurité accrue, vous pouvez utiliser un HSM pour sécuriser les clés privées utilisées dans le décryptage SSL/TLS pour :

- Proxy de transfert SSL : la clé privée du certificat d'approbation de transfert qui est utilisée pour signer les certificats dans les opérations du proxy de transfert SSL/TLS peut être enregistrée sur le HSM. Le pare-feu enverra ensuite les certificats qu'il génère pendant ces opérations au HSM pour signature avant de les transférer au client.
- Inspection SSL entrante : les clés privées des serveurs internes pour lesquels vous effectuez l'inspection SSL/TLS entrante peuvent être enregistrées sur le HSM.

Si vous utilisez les algorithmes d'échange de clés DHE ou ECDHE pour activer la Prise en charge de Perfect Forward Secrecy (Confidentialité de transmission parfaite ; PFS) pour le décryptage SSL, vous pouvez utiliser un hardware security module (module de sécurité matérielle ; HSM) pour stocker les clés privées pour l'inspection SSL entrante. Vous pouvez également utiliser un HSM pour stocker les clés ECDSA utilisées pour le décryptage de proxy de transfert SSL ou d'inspection SSL entrante, sauf si vous utilisez TLSv1.3. Pour le trafic TLSv1.3, PAN-OS prend en charge les HSM uniquement pour le proxy de transfert SSL. Il ne prend pas en charge les HSM pour l'inspection SSL entrante.

**STEP 1 |** Sur le HSM, importez ou générez le certificat et la clé privée utilisés dans vos déploiements de décryptage.

Pour plus d'informations sur l'importation ou la génération de certificat et de clé privée sur le HSM, reportez-vous à la documentation fournie par votre fournisseur HSM.

**STEP 2 |** (nCipher nShield Connect uniquement) Synchronisez les données de clés provenant du système de fichiers distants de nCipher nShield avec le pare-feu.

*La synchronisation avec le HSM de SafeNet Network se fait automatiquement.*

1. Accédez à l'interface Web du pare-feu et sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **HSM**.
2. Sélectionnez **Synchronize with Remote Filesystem** (Synchroniser avec le système de fichiers distants) dans les paramètres Opérations de sécurité matérielle.

**STEP 3 |** Importez le certificat correspondant à la clé provenant du HSM.

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, puis cliquez sur **Import (Importer)**.
2. Saisissez le **Certificate Name (nom du certificat)**.
3. **Browse (Naviguez)** jusqu'au **Certificate File (Fichier du certificat)** sur le HSM.
4. Sélectionnez un **File Format (Format de fichier)**.
5. Sélectionnez **Private Key resides on Hardware Security Module (La clé privée se trouve sur le module de sécurité matériel)**.
6. Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.

**STEP 4 |** (Certificats d'approbation de transfert uniquement) Activez le certificat à utiliser dans le proxy de transfert SSL/TLS.

1. Ouvrez le certificat que vous avez importé à l'étape 3 pour le modifier.
2. Sélectionnez **Forward Trust Certificate (Certificat d'approbation de transfert)**.
3. Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.

**STEP 5 |** Vérifiez que vous avez correctement importé le certificat sur le pare-feu.

Identifiez le certificat que vous avez importé à l'étape 3 et vérifiez si une icône est affichée dans la colonne Key (Clé) :

- **Icône Verrou** : la clé privée du certificat se trouve sur le HSM.
- **Icône Erreur** : la clé privée ne se trouve pas sur le HSM ou le HSM n'a pas été correctement authentifié ou connecté.

## Gestion du déploiement du HSM

Vous pouvez effectuer les tâches suivantes pour gérer votre déploiement HSM :

- Affichez les paramètres de configuration du HSM.

  Sélectionnez **Device (périphérique)** > **Setup (Configuration)** > **HSM**.

- Consultez les informations détaillées concernant le HSM.

  Sélectionnez **Show Detailed Information (Afficher les informations détaillées)** dans la section Hardware Security Operations (Opérations de sécurité matérielle).

  Les informations concernant les serveurs du HSM, l'état HA du HSM et le matériel du HSM s'affichent.

- Exportez le fichier de support.

  Sélectionnez **Export Support File (Exporter le fichier de support)** dans la section Hardware Security Operations (Opérations de sécurité matérielle).

  Un fichier de test est créé pour aider le service clientèle à résoudre un problème lié à la configuration du HSM sur le pare-feu.

- Réinitialisez la configuration du HSM.

  Sélectionnez **Reset HSM Configuration (Réinitialiser la configuration du HSM)** dans la section Hardware Security Operations (Opérations de sécurité matérielle).

  L'activation de cette option supprime toutes les connexions au HSM. Toutes les procédures d'authentification doivent être répétées après avoir utilisé cette option.

# Haute disponibilité

La High Availability (haute disponibilité ; HA) est un déploiement dans laquelle deux pare-feu sont placés dans un groupe ou jusqu'à 16 pare-feu sont placés dans un cluster HA et où leur configuration est synchronisée afin d'éviter tout point de défaillance unique sur votre réseau. Une connexion de pulsation entre les pare-feu homologues garantit un basculement transparent en cas d'arrêt d'un homologue. Le paramétrage HA fournit une redondance et vous permet d'assurer la continuité de l'activité.

# Présentation de la HA

Vous pouvez configurer deux pare-feu Palo Alto Networks en tant que paire HA ou configurer jusqu'à 16 pare-feu en tant que membres homologues d'un cluster HA. Les homologues dans le cluster peuvent être des paires HA ou des pare-feux autonomes. HA vous permet de minimiser les temps d'arrêt en vous assurant qu'un autre pare-feu est disponible en cas de défaillance d'un pare-feu homologue. Les pare-feu d'une paire ou d'un cluster HA utilisent des ports HA dédiés ou en bande sur le pare-feu pour synchroniser les configurations de réseau de données, d'objets et de politiques, et pour maintenir les informations d'état. La configuration spécifique à un pare-feu, comme l'adresse IP d'une interface de gestion ou des profils administrateur, une configuration spécifique à la HA, des données de journaux, et les informations de l'Application Command Center (centre de commande des applications - ACC), n'est pas partagée entre les périphériques.

Pour obtenir une vue consolidée des applications et des journaux sur une paire HA, vous devez utiliser Panorama, le système de gestion centralisée de Palo Alto Networks. Reportez-vous à la section Changement de contexte : Pare-feu ou Panorama du Guide de l'administrateur Panorama. Consultez Configuration requise pour la HA active/passive et Prérequis pour HA actif/actif. Il est fortement recommandé d'utiliser Panorama pour mettre à disposition les membres du cluster HA. Consultez Bonnes pratiques et approvisionnement de la mise en cluster HA.

Lorsqu'une défaillance se produit sur un pare-feu dans une paire HA ou un cluster HA et qu'un pare-feu homologue prend en charge la tâche de sécuriser le trafic, l'événement est appelé basculement. Les conditions déclenchant un basculement sont :

- Échec d'une ou de plusieurs des interfaces surveillées. (Surveillance des liaisons)
- Impossibilité d'atteindre une ou plusieurs des destinations spécifiées sur le pare-feu. (Surveillance des chemins)
- Pas de réponse du pare-feu à l'analyse des pulsations. (Sondage de pulsation et messages Hello)
- Échec d'un microprocesseur ou d'un composant logiciel, c'est-à-dire le contrôle de fonctionnement du chemin que doit emprunter un paquet.

Les pare-feu Palo Alto Networks prennent en charge la haute disponibilité à inspection d'état active/passive ou active/active avec synchronisation de la session et de la configuration avec quelques exceptions :

- Le pare-feu VM-Series sur Azure et le pare-feu VM-Series sur AWS prennent en charge la HA active/passive uniquement.

  Sur AWS, lorsque vous déployez le pare-feu avec Amazon Elastic Load Balancing (ELB), il ne prend pas en charge la HA (dans ce cas, le service ELB fournit les capacités de basculement).
- Le pare-feu VM-Series dans Google Cloud Platform ne prend pas en charge la HA.

Commencez par comprendre les concepts HA et le Présentation de la mise en cluster HA si vous voulez configurer la mise en cluster HA.

# Concepts de la HA

Les rubriques suivantes fournissent des informations conceptuelles sur le fonctionnement de la HA sur un pare-feu Palo Alto Networks :

- Modes HD
- Liaisons HA et liaisons de secours
- Priorité et préemption des périphériques
- Basculement
- Prénégociation LACP et LLDP pour la HA active/passive
- Adresse IP flottante et adresse MAC virtuelle
- Partage de charge ARP
- Redondance de routage
- Minuteurs HA
- Propriétaire de session
- Configuration de la session
- NAT en mode HA active/active
- ECMP en mode HA active/active

## Modes HD

Vous pouvez configurer les pare-feu d'une paire de HA selon l'un des deux modes suivants :

- **Actif/Passif** : un pare-feu gère activement le trafic pendant que l'autre est synchronisé et prêt à passer à l'état actif en cas d'échec. Dans ce mode, les deux pare-feu partagent les mêmes paramètres de configuration et un seul gère activement le trafic jusqu'à ce que l'échec d'un chemin, d'une liaison, d'un système ou d'un réseau se produise. Lorsque le pare-feu actif échoue, le pare-feu passif passe à l'état actif, prend systématiquement le relais et applique les mêmes politiques pour gérer la sécurité du réseau. La HA active/passive est prise en charge dans les déploiements de câble virtuel, de Couche 2 ou de Couche 3.
- **Active/active** : les deux pare-feu d'une paire sont actifs, traitent le trafic et travaillent de façon synchrone pour gérer la configuration et la propriété d'une session. Les deux pare-feu gèrent des tables de session et des tables de routage et sont synchronisés l'un à l'autre. La HA active/active est prise en charge dans les déploiements de câble virtuel et de Couche 3.

  En mode HA active/active, le client ne prend pas en charge le client DHCP. De plus, seul le pare-feu actif/passif peut faire office d'agent de relais DHCP. Si le pare-feu actif-secondaire reçoit les paquets de diffusion DHCP, il les abandonne.

  ***Une configuration active/active n'équilibre pas la charge du trafic. Bien qu'il puisse partager la charge en envoyant le trafic vers l'homologue, aucun équilibrage de charge ne se produit. Pour partager la charge des sessions entre les deux pare-feu, vous pouvez, notamment, utiliser ECMP, plusieurs ISP et des équilibreurs de charge.***

Lorsque vient le temps de décider s'il faut utiliser le mode actif/passif ou actif/actifs, tenez compte des différences suivantes :

- Le mode actif/passif se distingue par la simplicité de sa conception ; la résolution de problèmes liés au routage et au flux de trafic est beaucoup plus facile en mode actif/passif. Le mode actif/passif prend en charge le déploiement de Couche 2 ; pas le mode actif/actif.
- Le mode actif/actif repose sur des concepts de conception avancés qui peuvent se traduire par des réseaux plus complexes. Selon votre implémentation de la HD active/active, vous pourriez devoir effectuer des configurations supplémentaires, par exemple, l'activation des protocoles de réseautage sur les deux pare-feu, la réplication de pools NAT et le déploiement d'adresses IP flottantes pour procurer un basculement efficace. Puisque les deux pare-feu traite activement le trafic, les pare-feu utilisent des concepts supplémentaires de propriété de session et de paramétrage de session pour effectuer l'inspection du contenu de Couche 7. Il est recommandé d'utiliser le mode actif/actif si chaque pare-feu doit posséder ses propres instances de routage et que vous devez compter sur une redondance complète en temps réel des deux pare-feu en tout temps. En mode actif/actif, le basculement est plus rapide et les flux de trafic de pointe sont mieux gérés qu'en mode actif/passif, car les deux pare-feu traitent activement le trafic.

  ***En mode actif/actif, la paire HD peut être utilisée pour traiter temporairement une plus grande quantité de trafic que ce qu'un seul pare-feu peut généralement gérer. Cette façon de procéder ne devrait toutefois pas être la norme, puisque l'échec d'un pare-feu entraîne le réacheminement du trafic à l'autre pare-feu de la paire HD. Votre conception doit permettre à l'autre pare-feu de traiter la capacité maximale de vos charges de trafic avec l'inspection du contenu permise. Si la conception dépasse la capacité de l'autre pare-feu, une latence élevée et/ou un échec de l'application peuvent se produire.***

Pour plus d'informations sur la configuration de vos pare-feu dans un mode actif/passif, reportez-vous à la section Configuration de la HA active/passive. Pour plus d'informations sur la configuration de vos pare-feu dans un mode actif/actif, reportez-vous à la section Configuration de la HA active/actif.

Dans un cluster HA, tous les membres sont considérés comme actifs ; il n'y a pas de concept de pare-feu passif, sauf pour les paires HA dans les clusters, qui peuvent conserver leur relation active/passive après que vous les ayez ajoutés à un cluster HA.

## Liaisons HA et liaisons de secours

Les pare-feu d'une paire HA utilisent des liaisons HA pour synchroniser des données et gérer des informations d'état. Certains modèles de pare-feu disposent de ports HA dédiés, liaison de contrôle (HA1) et liaison de données (HA2), alors que d'autres exigent que vous utilisiez des ports sur bande comme liaison HA.

- Dans le cas de pare-feu possédant des ports HA dédiés, utilisez ces ports pour gérer la communication et la synchronisation entre les pare-feu. Pour plus d'informations, reportez-vous à la section Ports HA sur les pare-feu Palo Alto Networks.
- Pour les pare-feu ne disposant pas de ports HA dédiés, comme les pare-feu PA-220 et PA-220R, il est recommandé d'utiliser le port de gestion pour le port HA1 et d'utiliser le port du plan de données pour le secours de HA1.

  ***Pour les pare-feux sans ports dédiés HA, décidez quel port utiliser pour HA1 et HA1 backup en fonction de votre environnement et compréhension de ce qui est le moins utilisé et moins congestionné Assignez HA1 à la meilleure interface et HA1 backup et à l'autre***

Les homologues HA dans un groupe HA peuvent être une combinaison de membres autonomes et de paires HA. Les membres du cluster HA utilisent un lien HA4 et un lien de secours HA4 pour effectuer la synchronisation des états de session. HA1 (lien de contrôle), HA2 (lien de données) et HA3 (lien de transfert de paquets) ne sont pas pris en charge entre les membres du cluster qui ne sont pas des paires HA.

| Liaisons HA et liaisons de secours | Description |
|---|---|
| Liaison de contrôle | la liaison HA1 permet d'échanger des messages Hello, des pulsations et des informations d'état HA, ainsi que des synchronisations de plans de gestion pour le routage et des informations sur User-ID. Les pare-feu utilisent également cette liaison pour synchroniser les modifications de configuration avec cet homologue. La liaison HA1 est une liaison de Couche 3 et exige une adresse IP.<br><br>ICMP est utilisé pour l'échange de messages de pulsation entre les homologues HA.<br><br>Ports utilisés pour la HA1 : port TCP 28769 et 28260 pour les communications en texte clair ; le port 28 pour les communications cryptées (SSH sur TCP).<br><br>Si vous activez le chiffrement sur la liaison HA1, vous pouvez également Actualisation des clés SSH HA1 et configuration des options des clés. |
| Liaison de données | la liaison HA2 permet de synchroniser des sessions, des tables de transfert, des associations de sécurité IPSec et des tables ARP entre les pare-feu d'une paire HA. Le flux de données de la liaison HA2 est toujours unidirectionnel (sauf pour la persistance HA2), du périphérique actif vers le périphérique passif. La liaison HA2 est une liaison de Couche 2 et utilise l'EtherType 0x7261 par défaut.<br><br>Ports utilisés pour la HA2 : la liaison de données HA peut être configurée pour utiliser IP (numéro de protocole 99) ou UDP (port 29281) comme protocole de transport et permet donc à la liaison de données HA d'étendre les sous-réseaux. |
| Liens de secours HA1 et HA2 | fournissent une redondance pour les liaisons HA1 et HA2. Les ports sur bande peuvent être utilisés pour les liaisons de secours pour les connexions HA1 et HA2 lorsque les liaisons de secours dédiées ne sont pas disponibles. Tenez compte des directives suivantes lors de la configuration de liaisons HA de secours :<br><br>• Les adresses IP des liaisons HA principales et de secours ne doivent pas se chevaucher.<br>• Les liaisons HA de secours doivent figurer sur un autre sous-réseau par rapport aux liaisons HA principales.<br>• Les ports HA1 de secours et HA2 de secours doivent être configurés sur des ports physiques distincts. La liaison HA1 de secours utilise les ports 28770 et 28260. |

| Liaisons HA et liaisons de secours | Description |
|---|---|
| | • Les pare-feu PA-3200 Series ne prennent pas en charge l'adresse IPv6 pour la liaison de secours HA1 ; utilisez une adresse IPv4.<br><br>***Palo Alto Networks recommande d'activer la sauvegarde des pulsations (port 28771 sur l'interface MGT) si vous utilisez un port sur bande pour les liaisons HA1 ou HA1 de secours.*** |
| Liaison de transfert des paquets | En plus des liaisons HA1 et HA2, un déploiement actif/actif exige également une liaison HD3 dédié. Les pare-feu se servent de cette liaison pour transférer des paquets à l'homologue lors de la configuration de la session et les flux de trafic asymétriques. La liaison HA3 est une liaison de Couche 2 qui utilise l'encapsulation MAC-in-MAC. Elle ne prend pas en charge l'adressage ou le cryptage de Couche 3. Les pare-feu PA-7000 Series synchronisent les sessions individuellement sur les NPC. Sur les pare-feu PA-800 Series, PA-3200 Series, PA-5200 Series et PA-5200, vous pouvez configurer des interfaces agrégées en tant que liaison HA3. Les interfaces agrégées peuvent également fournir une redondance pour la liaison HA3 ; vous ne pouvez configurer de liaisons de secours pour la liaison HA3. Sur les pare-feu PA-3200 Series, PA-5200 et PA-7000 Series, les ports HSCI dédiés prennent en charge la liaison HA3. Le pare-feu ajoute un en-tête de paquet exclusif aux paquets qui traversent la liaison HD3 ; la MTU sur cette liaison doit être supérieure à la longueur maximale des paquets transmis. |
| Lien HA4 et lien de secours HA4 | Le lien HA4 et le lien de secours HA4 assurent la synchronisation du cache de session entre tous les membres du cluster HA ayant le même ID de cluster. Le lien HA4 entre les membres du cluster détecte les défaillances de connectivité entre les membres du cluster en envoyant et en recevant des messages de maintien de la couche 2. Consultez l'état des liens de secours HA4 et HA4 sur le tableau de bord du pare-feu. |

## Ports HA sur les pare-feu Palo Alto Networks

Lorsque vous connectez deux pare-feu Palo Alto Networks® dans une configuration High Availability (haute disponibilité ; HA), nous vous recommandons d'utiliser les ports HA dédiés pour les liaisons HA et les liaisons de secours. Voici certains de ces ports dédiés : les ports HA1 étiquetés HA1, HA1-A et HA1-B utilisés pour le contrôle HA et la synchronisation du trafic; et les ports HA2 et High Speed Chassis Interconnect (interconnexion de châssis haute vitesse ; HSCI) utilisés pour le trafic de paramétrage de session HA. Les pare-feu PA-5200 Series possèdent des ports auxiliaires multiusages étiquetés AUX-1 et AUX-2 que vous pouvez configurer pour le trafic HA1.

Vous pouvez également configurer le port HSCI pour la HA3, qui est utilisée pour le transfert des paquets vers le pare-feu homologue dans le flux de trafic asymétrique et de paramétrage de session (HA active/active uniquement). Le port HSCI peut être utilisé pour le trafic HA2, le trafic HA3, ou les deux.

*Les liaisons HA1 et AUX permettent de synchroniser les fonctions présentes sur le plan de gestion. L'utilisation des interfaces HA dédiées sur le plan de gestion est plus efficace que l'utilisation des ports sur bande car il n'est alors plus nécessaire de transmettre les paquets de synchronisation via le plan de données.*

Si votre pare-feu ne dispose pas de ports HA dédiés, vous pouvez configurer les ports de données en tant qu'interfaces HA. Si votre pare-feu dispose de ports HA dédiés, mais qu'il ne possède pas de port de secours HA dédié, vous pouvez également configurer les ports de données en tant ports de secours pour les ports HA dédiés.

*Lorsque possible, connectez les ports HA directement entre les deux pare-feu de la paire HA (et non pas par l'intermédiaire d'un commutateur ou d'un routeur) afin d'éviter que des problèmes de communications ou de liaisons HA ne se produisent en cas de problème de réseau.*

Utilisez le tableau suivant pour en apprendre davantage sur les ports HA dédiés et sur la manière de connecter les Liaisons HA et les liaisons de secours :

| Modèle | Ports dédiés du panneau frontal |
|---|---|
| Pare-feu PA-800 Series | • **HA1 et HA2** : ports Ethernet 10 Mbits/s,100 Mbits/s, 1000 Mbits/s utilisés pour la HA1 et la HA2 dans les deux Modes HA.<br>  • **Pour le trafic HA1** : connectez directement le port HA1 du premier pare-feu au port HA1 du second pare-feu de la paire, ou connectez ces ports à l'aide d'un commutateur ou d'un routeur.<br>  • **Pour le trafic HA2** : connectez directement le port HA2 du premier pare-feu au port HA2 du second pare-feu de la paire, ou connectez ces ports à l'aide d'un commutateur ou d'un routeur. |
| Pare-feu PA-3200 Series | • **HA1-A et HA1-B** : ports Ethernet 10 Mbits/s, 100 Mbits/s, 1000 Mbits/s utilisés pour le trafic HA1 dans les deux Modes HD.<br>  • **Pour le trafic HA1** : connectez directement le port HA1-A du premier pare-feu au port HA1-A du second pare-feu de la paire, ou connectez-les à l'aide d'un commutateur ou d'un routeur.<br>  • **Pour un port de secours pour la connexion HA1-A** : connectez directement le port HA1-B du premier pare-feu au port HA1- |

| Modèle | Ports dédiés du panneau frontal |
|---|---|
| | B du second pare-feu de la paire, ou connectez-les à l'aide d'un commutateur ou d'un routeur.<br><br>*Si le plan de données du pare-feu redémarre en raison d'un échec ou d'un redémarrage manuel, la liaison HA1-B redémarre également. Si cette situation se produit et que la liaison HA1-A n'est pas connectée ni configurée, une condition de « split brain » se produit alors. Nous vous recommandons donc de connecter et de configurer les ports HA1-A et les ports HA1-B afin de procurer la redondance et d'éviter les problèmes de « split brain ».*<br><br>*Vous pouvez redéfinir les ports SFP du pare-feu en tant que ports HA1-A et HA1-B via PAN-OS ou Panorama.*<br><br>• **HSCI** : le port HSCI est une interface SFP+ de couche 1 qui connecte deux pare-feu PA-3200 dans une configuration HA. Utilisez ce port pour une connexion HA2 ou HA3, ou les deux.<br><br>Le trafic acheminé sur les ports HSCI est du trafic de couche 1 brut, qui n'est ni acheminable ni commutable. Vous devez donc connecter les ports HSCI directement les uns aux autres (du port HSCI du premier pare-feu au port HSC du second pare-feu). |
| Pare-feu PA-5200 Series | • **HA1-A et HA1-B** : ports Ethernet 10 Mbits/s, 100 Mbits/s, 1000 Mbits/s utilisés pour le trafic HA1 dans les deux Modes HD.<br>  • **Pour le trafic HA1** : connectez directement le port HA1-A du premier pare-feu au port HA1-A du second pare-feu de la paire, ou connectez-les à l'aide d'un commutateur ou d'un routeur.<br>  • **Pour un port de secours pour la connexion HA1-A** : connectez directement le port HA1-B du premier pare-feu au port HA1-B du second pare-feu de la paire, ou connectez-les à l'aide d'un commutateur ou d'un routeur.<br>• **HSCI** : le port HSCI est une interface de couche 1 qui connecte deux pare-feu PA-5200 dans une configuration HA. Utilisez ce port pour une connexion HA2 ou HA3, ou les deux.<br><br>*Le port HSCI sur le pare-feu PA-5220 est un port QSFP + et le port HSCI sur les pare-feu PA-5250, PA-5260 et PA-5280 est un port QSFP28.*<br><br>Le trafic acheminé sur le port HSCI est du trafic de couche 1 brut, qui n'est ni acheminable ni commutable. Vous devez donc connecter les ports HSCI directement les uns aux autres (du port HSCI du premier pare-feu au port HSC du second pare-feu). |

| Modèle | Ports dédiés du panneau frontal |
|---|---|
| Pare-feu PA-5200 Series (Suite) | • **AUX-1 et AUX-2** : les ports SFP+ auxiliaires sont des ports multiusages que vous pouvez configurer pour la HA1, les fonctions de gestion ou le transfert des journaux vers Panorama. Utilisez ces ports lorsque vous avez besoin d'un connexion en fibre pour l'une de ces options.<br>  • **Pour le trafic HA1** : connectez directement le port AUX-1 du premier pare-feu au port AUX-1 du second pare-feu de la paire, ou connectez-les à l'aide d'un commutateur ou d'un routeur.<br>  • **Pour un port de secours pour la connexion AUX-1** : connectez directement le port AUX-2 du premier pare-feu au port AUX-2 du second pare-feu de la paire, ou connectez-les à l'aide d'un commutateur ou d'un routeur. |
| Pare-feu PA-7000 Series | • **HA1-A et HA1-B** : ports Ethernet 10 Mbits/s, 100 Mbits/s, 1000 Mbits/s utilisés pour le trafic HA1 dans les deux Modes HD.<br>  • **Pour le trafic HA1** : connectez directement le port HA1-A du premier pare-feu au port HA1-A du second pare-feu de la paire, ou connectez-les à l'aide d'un commutateur ou d'un routeur.<br>  • **Pour un port de secours pour la connexion HA1-A** : connectez directement le port HA1-B du premier pare-feu au port HA1-B du second pare-feu de la paire, ou connectez-les à l'aide d'un commutateur ou d'un routeur.<br>  *Vous ne pouvez configurer une connexion HA1 sur les ports de données NPC ou sur le port de gestion (MGT).*<br>• **HSCI-A et HSCI-B** : les ports HSCI sont des interfaces QSFP+ de couche 1 qui connectent deux pare-feu PA-7000 dans une configuration HA. Utilisez ces ports pour une connexion HA2 ou HA3, ou les deux.<br>  Le trafic acheminé sur les ports HSCI est du trafic de couche 1 brut, qui n'est ni acheminable ni commutable. Vous devez donc connecter ces ports comme suit :<br>  • **Pour le trafic HA2 et HA3** : connectez le port HSCI-A du premier pare-feu au port HSCI-A du second pare-feu.<br>  *Pour le trafic HA2 ou HA2/HA3, les pare-feu PA-7000 Series synchronisent les sessions individuellement sur les NPC.*<br>  • **Pour un port de secours pour la connexion HSCI-A** : connectez directement le port HSCI-B du premier pare-feu au port HSCI-B du second pare-feu. |

| Modèle | Ports dédiés du panneau frontal |
| --- | --- |
| | *Les liens HA2 et HA2 de secours peuvent être configurés pour utiliser une interface de plan de données au lieu des ports HSCI. Cependant, s'ils sont configurés de cette manière, les liens HA2 et HA2 de secours doivent utiliser des interfaces de plan de données. La combinaison d'un port de plan de données et d'un port HSCI pour HA2 ou HA2 de secours entraînera un échec de la validation. Cela s'applique au PA-7050-SMC, au PA-7080-SMC, au PA-7050-SMC-B et au PA-7080-SMC-B.* |

## Priorité et préemption des périphériques

Les pare-feu d'une paire HA active/passive peuvent se voir affecter une valeur de ***priorité du périphérique*** afin d'indiquer une préférence pour laquelle un pare-feu doit assumer un rôle actif ou actif-principal. Si vous devez utiliser un pare-feu spécifique de la paire HA pour la sécurisation active du trafic, vous devez activer le comportement préemptif sur les deux pare-feu et affecter une valeur de priorité pour chaque pare-feu. Le pare-feu affichant la valeur numérique la plus basse et, par conséquent, ***la priorité la plus élevée***, est désigné comme étant actif. L'autre pare-feu est le pare-feu passif.

Il en va de même pour une paire HA active/active ; cependant, l'***ID de périphérique*** sert à attribuer une valeur de priorité du périphérique. De même, la valeur numérique la plus faible de l'ID du périphérique correspond à une priorité élevée. Le pare-feu ayant la priorité la plus élevée devient actif-principal, et le pare-feu qui lui est associé devient actif-secondaire.

Par défaut, la préemption est désactivée sur les pare-feu et doit être activée sur les deux pare-feu. Lorsqu'il est activé, le comportement préemptif permet au pare-feu affichant ***la priorité la plus élevée*** (valeur numérique la plus basse) de reprendre l'état actif après avoir récupéré d'un échec. En cas de préemption, l'événement est consigné dans les journaux système.

## Basculement

Lorsqu'une défaillance se produit sur un pare-feu et que l'homologue dans la paire HA (ou un homologue dans le cluster HA) prend en charge la tâche de sécurisation du trafic, l'événement est appelé ***basculement*** . Un basculement est déclenché, par exemple, lorsqu'une des mesures surveillées sur un pare-feu d'une paire HD échoue. Les mesures que le pare-feu surveille pour détecter une défaillance du pare-feu sont les suivantes :

- **Sondage de pulsation et messages Hello**

  Les pare-feu utilisent les messages hello et les pulsations pour vérifier que le pare-feu homologue est réactif et opérationnel. Les messages Hello sont envoyés d'un homologue à l'autre pendant l'***intervalle Hello*** configuré pour vérifier l'état de l'autre pare-feu. La pulsation est une requête ping ICMP envoyée à l'homologue HA sur la liaison de contrôle et l'homologue y répond pour indiquer que les pare-feu sont connectés et réactifs. Par défaut, l'intervalle d'une pulsation est de 1 000 millisecondes. Une requête ping est envoyée aux 1 000 millisecondes, et un basculement se produit si trois pulsations consécutives sont perdues. Pour plus d'informations sur les minuteurs HA qui déclenchent un basculement, reportez-vous à la section Minuteurs HA.

- **Surveillance des liaisons**

  Vous pouvez spécifier un groupe d'interfaces physiques que le pare-feu surveillera (un groupe de liens) et le pare-feu surveille l'état de chaque lien dans le groupe (lien actif ou lien inactif). Vous pouvez déterminer la condition d'échec pour groupe de liens : **Any (Un quelconque)** lien inactif ou **All (Tous)** les liens inactifs dans le groupe constitue une défaillance du groupe de liens (mais pas nécessairement un basculement).

  Vous pouvez créer plusieurs groupes de liens. Par conséquent, vous déterminez également l'état de défaillance de l'ensemble des groupes de liens : **Any (Un quelconque)** groupe de liens échoue ou **All (Tous)** les groupes de liens échouent, ce qui détermine quand un basculement est déclenché. Le comportement par défaut est que la défaillance de **Any (Un quelconque)** lien dans **Any (Un quelconque)** groupe de liens fait que le pare-feu change l'état HA en non fonctionnel (ou en état provisoire en mode actif/actif) pour indiquer une défaillance d'un objet surveillé.

- **Surveillance des chemins**

  Vous pouvez spécifier un groupe d'adresses IP de destination que le pare-feu surveillera. Le pare-feu surveille le chemin complet à travers le réseau vers les adresses IP critiques en utilisant des pings ICMP pour vérifier l'accessibilité de l'adresse IP. L'intervalle par défaut des requêtes ping est de 200 ms. Une adresse IP est considérée comme injoignable lorsque 10 pings consécutifs (la valeur par défaut) échouent. Vous spécifiez la condition de défaillance pour les adresses IP dans un groupe d'adresses IP de destination : **Any (Une quelconque)** adresse IP injoignable ou **All (Toutes)** les adresses IP injoignables dans le groupe. Vous pouvez spécifier plusieurs groupes d'IP de destination pour un groupe de chemins pour un câble virtuel, un VLAN ou un routeur virtuel ; vous spécifiez la condition de défaillance des groupes d'IP de destination dans un groupe de chemins : **Any (Un quelconque)** ou **All (Tous)**, ce qui constitue un échec du groupe de chemins. Vous pouvez configurer plusieurs groupes de chemins de câbles virtuels, groupes de chemins VLAN et groupes de chemins de routeurs virtuels.

  Vous déterminez également la condition de défaillance globale : **Any (Un quelconque)** groupe de chemins échoue ou **All (Tous)** les groupes de chemins échouent, ce qui détermine quand un basculement est déclenché. Le comportement par défaut est que si **Any (Une quelconque)** des adresses IP devient injoignable dans **Any (Un quelconque)** groupe d'adresses IP de destination dans **Any (Un quelconque)** groupe de chemins de câble virtuel, de VLAN ou de routeur virtuel, le pare-feu modifie l'état HA en état non fonctionnel (ou en état provisoire en mode actif/actif) pour indiquer une défaillance d'un objet surveillé.

Outre les déclenchements de basculement répertoriés ci-dessus, un basculement se produit également lorsque l'administrateur suspend le pare-feu ou en cas de préemption.

Sur les pare-feu PA-3200 Series, PA-5200 Series et PA-7000 Series, un basculement peut se produire lors de l'échec d'une vérification de l'état interne. Cette vérification n'est pas configurable et est activée afin de surveiller les composants essentiels, comme les FPGA et les processeurs. De plus, les vérifications générales se produisent sur toutes les plateformes, ce qui entraîne un basculement.

Ce qui suit décrit ce qui se passe en cas de défaillance d'une carte de traitement réseau (NPC) sur un pare-feu de la série PA-7000 qui est membre d'un cluster HA :

- Si la NPC qui est utilisée pour tenir le cache des sessions de la mise en cluster HA (une copie des sessions des autres membres) tombe en panne, le pare-feu devient non fonctionnel. Lorsque cela se produit, le dispositif de distribution de session (tel qu'un équilibreur de charge) doit détecter que le pare-feu est hors service et distribuer la charge de session aux autres membres du cluster.

- Si la NPC d'un membre du cluster tombe en panne et qu'aucune surveillance de lien ou de chemin n'a été activée sur cette NPC, le membre du pare-feu de la série PA-7000 restera en place, mais avec une capacité inférieure parce qu'une NPC est en panne.
- Si la NPC d'un membre du cluster tombe en panne et que la surveillance des liens ou des chemins a été activée sur cette NPC, le pare-feu de la série PA-7000 deviendra non fonctionnel et le dispositif de distribution de session (tel qu'un équilibreur de charge) doit détecter que le pare-feu est en panne et distribuer la charge de session aux autres membres du cluster.

## Prénégociation LACP et LLDP pour la HA active/passive

Si un pare-feu utilise LACP ou LLDP, la négociation de ces protocoles en cas de basculement empêche le basculement en dessous d'une seconde. Toutefois, vous pouvez activer une interface sur un pare-feu passif pour négocier LACP et LLDP avant le basculement. Ainsi, un pare-feu en état HA passif ou non fonctionnel peut communiquer avec des dispositifs voisins en utilisant LACP ou LLDP. Une telle pré-négociation accélère le basculement.

Tous les modèles de pare-feu, sauf les modèles de pare-feu VM-Series prennent en charge une configuration de pré-négociation selon que l'interface Ethernet ou AE se trouve dans un déploiement de couche 2, de couche 3 ou de câble virtuel. Un pare-feu passif HA gère les paquets LACP et LLDP de deux manières:

- **Actif** : Le pare-feu a LACP ou LLDP configuré sur l'interface et participe activement à la pré-négociation LACP ou LLDP, respectivement.
- **Passif** : LACP ou LLDP n'est pas configuré sur l'interface et le pare-feu ne participe pas au protocole, mais permet aux homologues de chaque côté du pare-feu de pré-négocier LACP ou LLDP, respectivement.

Le tableau suivant indique quels sont les déploiements pris en charge par Aggregate Ethernet (AE) et les interfaces Ethernet.

| Déploiement d'interface | Interface AE | Interface Ethernet |
|---|---|---|
| LACP en couche 2 | Actif | Pas pris en charge |
| LACP en couche 3 | Actif | Pas pris en charge |
| LACP en câble virtuel | Pas pris en charge | Passif |
| LLDP en couche 2 | Actif | Actif |
| LLDP en couche 3 | Actif | Actif |
| LLDP en câble virtuel | Actif | • Active si LLDP lui-même est configuré.<br>• Passive si LLDP lui-même n'est pas configuré. |

La pré-négociation n'est pas prise en charge sur les sous-interfaces ou les interfaces de tunnel.

Pour configurer la pré-négociation LACP ou LLDP, reportez-vous à l'étape (Facultatif) Activer la Prénégociation LACP et LLDP pour la HA active/passive pour un basculement plus rapide si votre réseau utilise LACP ou LLDP.

## Adresse IP flottante et adresse MAC virtuelle

Dans un déploiement de Couche 3 du mode HD active/active, vous pouvez assigner des adresses IP flottantes, qui passent d'un pare-feu HD à l'autre en cas d'échec d'une liaison ou d'un pare-feu. L'interface sur le pare-feu qui dispose de l'adresse IP flottante répond aux requêtes ARP à l'aide d'une adresse MAC virtuelle.

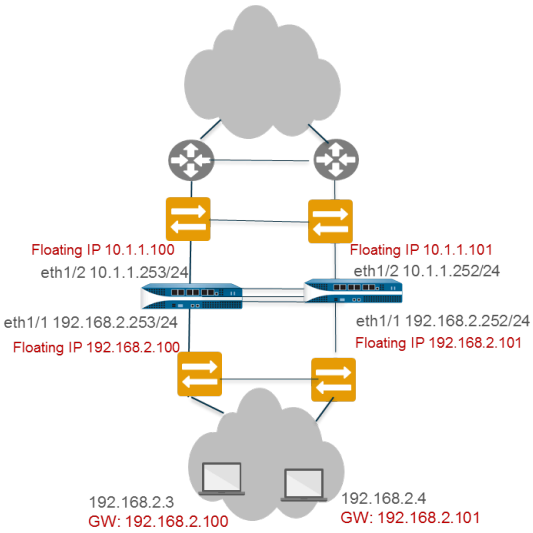
Il est recommandé de recourir à des adresses IP flottantes lorsque vous devez disposer d'une fonction comme le protocole Virtual Router Redundancy Protocol (protocole de redondance de routeur virtuel ; VRRP). Les adresses IP flottantes peuvent également servir à mettre en œuvre les VPN et la traduction NAT source, ce qui permet de poursuivre les connexions en cas d'échec du pare-feu proposant ces services.

Comme le montre la figure suivante, chaque interface de pare-feu HD possède sa propre adresse IP et sa propre adresse IP flottante. L'adresse IP de l'interface se trouve localement sur le pare-feu, mais l'adresse IP flottante passe d'un pare-feu à l'autre lors de l'échec d'un pare-feu. Vous configurez les hôtes finaux pour qu'ils utilisent une adresse IP flottante comme passerelle par défaut, ce qui vous permet d'équilibrer la charge du trafic entre les deux homologues HD. Vous pouvez également utiliser des équilibreurs de charge externe pour équilibrer la charge du trafic.

En cas d'échec d'une liaison ou d'un pare-feu ou si un événement de surveillance des chemins entraîne un basculement, l'adresse IP flottante et l'adresse MAC virtuelle sont transférées au pare-feu actif. (Dans la figure ci-dessus, chaque pare-feu possède deux adresses IP flottantes et adresses MAC virtuelles ; elles sont toutes transférées en cas d'échec du pare-feu.) Le pare-feu actif envoie un message ARP gratuit pour mettre à jour les tables MAC des commutateurs connectés pour les informer de la modification de propriété des adresses IP flottantes et MAC afin de réacheminer le trafic vers lui.

Après la récupération du pare-feu suite à un échec, l'adresse IP flottante et l'adresse MAC virtuelle retournent par défaut au pare-feu ayant l'ID de périphérique [0 ou 1] auquel l'adresse IP flottante est liée. Plus particulièrement, après la récupération du pare-feu suite à un échec, il devient disponible. Le pare-feu actuellement actif détermine que le pare-feu a redémarré et vérifie si l'adresse IP flottante qu'il gère lui appartient de manière native ou si elle appartient à l'autre pare-feu. Si l'adresse IP flottante était initialement liée à l'autre périphérique, le pare-feu la retourne automatiquement. (Pour connaître une variante à ce comportement par défaut, reportez-vous à la section Cas pratique : Configuration de la HD actif/actif avec des adresses IP flottantes liées à un pare-feu principal actif.)




Chaque pare-feu d'une paire HD crée une adresse MAC virtuelle pour chacune de ses interfaces qui disposent d'une adresse IP flottante ou d'une adresse IP de partage de charge ARP.

Le format de l'adresse MAC virtuelle (sur les pare-feu autres que les pare-feu PA-7000 Series, PA-5200 et PA-3200 Series) est le suivant : 00-1B-17-00-xx-yy, dans lequel 00-1B-17 correspond à l'ID constructeur (soit Palo Alto Networks dans le cas présent), 00 est fixe, xx indique l'ID de périphérique et l'ID de groupe, comme l'illustre la figure suivante, et yy est l'ID de l'interface :

| 7 | 6 | 543210 | 76543210 |
|---|---|---|---|
| ID du périphérique | 0 | ID du groupe | ID de l'interface |

Le format de l'adresse MAC virtuelle sur les pare-feu PA-7000, PA-5200 et PA-3200 Series est le suivant : B4-0C-25-xx-xx-xx, dans lequel B4-0C-25 correspond à l'ID constructeur (soit Palo Alto Networks dans le cas présent), les 24 bits suivants indiquent l'ID de périphérique, l'ID de groupe et l'ID de l'interface, comme suit :

| 765 | 4 | 321076 | 5432 | 1076543210 |
|---|---|---|---|---|
| 111 | ID du périphérique | ID du groupe | 0000 | ID de l'interface |

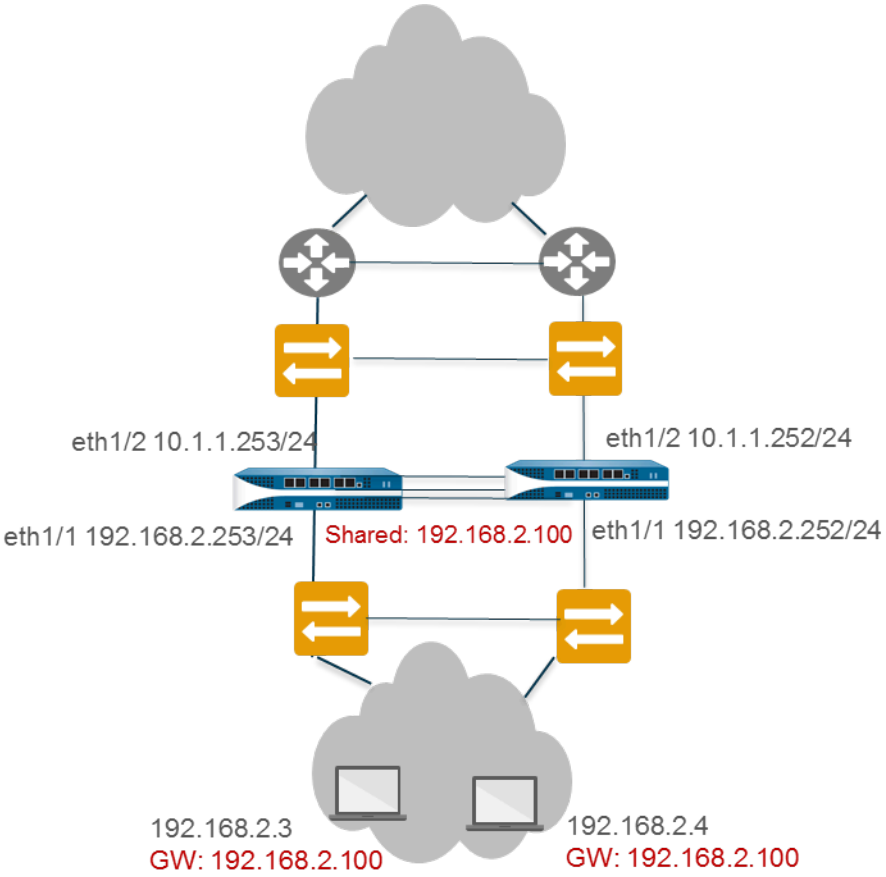
Lorsqu'un nouveau pare-feu actif prend le relais, celui-ci envoie des messages ARP gratuits par chacune de ses interfaces connectées afin d'informer les commutateurs de Couche 2 connectés du nouvel emplacement de l'adresse MAC virtuelle. Pour configurer les adresses IP flottantes, reportez-vous à la section Cas pratique : Configuration de la HA active/active avec des adresses IP flottantes.

## Partage de charge ARP

Dans un déploiement d'interface de couche 3 et une configuration HA active/active, le partage de charge ARP permet aux pare-feu de partager une adresse IP et de fournir des services de passerelle. Utilisez le partage de charge ARP uniquement lorsqu'aucun périphérique de Couche 3 n'existe entre

le pare-feu et les hôtes finaux, c'est-à-dire lorsque les hôtes finaux utilisent le pare-feu en tant que passerelle par défaut.



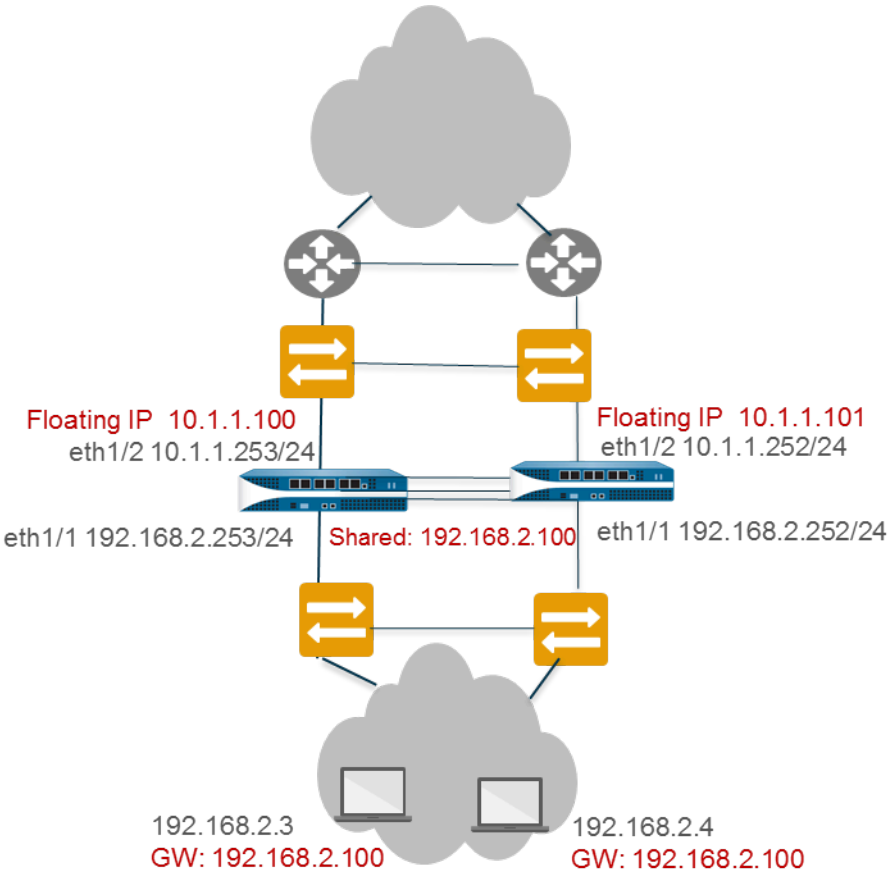

Dans un tel scénario, tous les hôtes sont configurés avec une adresse IP de passerelle unique. L'un des pare-feu répond aux requêtes ARP d'adresse IP de passerelle en transmettant son adresse MAC virtuelle. Une adresse MAC virtuelle unique à chaque pare-feu est générée pour l'adresse IP partagée. L'algorithme de partage de charge qui contrôle le pare-feu qui répondra aux requêtes ARP est configurable ; il est déterminé en calculant le hachage ou le modulo de l'adresse IP source de la requête ARP.

Lorsque l'hôte final a reçu la réponse à la requête ARP de la part de la passerelle, il met l'adresse MAC en cache, et tout le trafic qui part de l'hôte est acheminé via le pare-feu qui a transmis l'adresse MAC pour la durée du cache ARP. La durée de vie du cache ARP dépend du système d'exploitation installé sur l'hôte final.

En cas d'échec d'une liaison ou d'un pare-feu, l'adresse IP flottante et l'adresse MAC virtuelle sont transmises au pare-feu qui est opérationnel. Le pare-feu actif envoie des messages ARP gratuits pour mettre à jour la table MAC des commutateurs connectés afin de réacheminer le trafic provenant du pare-feu ayant subi un échec vers lui-même. Reportez-vous à la section Cas d'utilisation : Configuration de la HA active/active avec le partage de charge ARP.

Vous pouvez configurer des interfaces du côté WAN des pare-feu HD avec des adresses IP flottantes et configurer des interfaces du côté LAN des pare-feu HD avec une adresse IP partagée pour le partage de charge ARP. Par exemple, la figure présentée ci-dessous illustre les adresses IP flottantes des routeurs périphériques WAN en amont et une adresse de partage de charge ARP pour les hôtes du segment LAN.

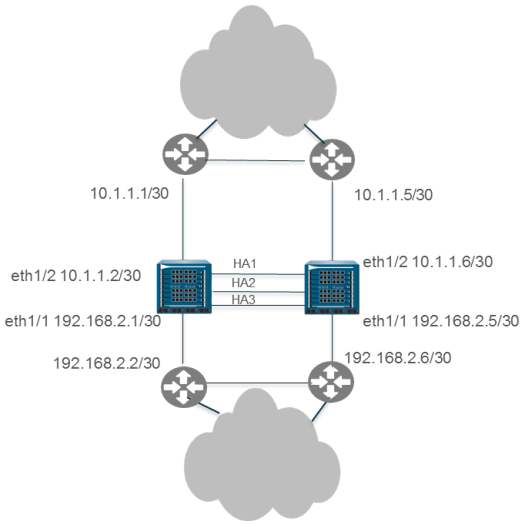
 




## Redondance de routage

Dans un déploiement d'interface de couche 3 et dans une configuration HD active/active, les pare-feux sont connectés à des routeurs plutôt qu'à des commutateurs. Les pare-feux utilisent des protocoles de routage dynamique pour déterminer le meilleur chemin (routage asymétrique) et pour équilibrer la charge entre la paire HD. Dans un tel scénario, aucune adresse IP flottante n'est nécessaire. En cas d'échec d'une liaison, d'un chemin surveillé ou d'un pare-feu, ou si la détection de transmission bidirectionnelle (BFD) détecte l'échec d'une liaison, le protocole de routage (RIP, OSPF ou BGP) s'occupe de réacheminer le trafic vers le pare-feu actif. Vous configurez chaque interface de pare-feu en lui attribuant une adresse IP unique. Les adresses IP se trouvent localement sur le pare-feu sur lequel elles sont configurées ; elles ne passent pas d'un périphérique à l'autre en cas d'échec d'un pare-feu. Reportez-vous à la section Cas d'utilisation : Configuration de la HD active/active avec redondance de routage.




# Minuteurs HA

Les minuteurs High Availability (haute disponibilité ; HA) permettent à un pare-feu de détecter une défaillance du pare-feu et de déclencher un basculement. Pour réduire la complexité de configuration des minuteurs pour une paire HA, vous pouvez sélectionner l'un des trois profils suivants : **Recommended (Recommandé)**, **Aggressive (Aggressif)** et **Advanced (Avancé)**. Ces profils renseignent automatiquement les valeurs optimales des minuteurs HA pour une plate-forme de pare-feu spécifique afin de permettre un déploiement HA accéléré.

Utilisez le profil **Recommended (Recommandé)** si vous souhaitez des paramètres de minuteur de basculement types ou le profil **Aggressive (Agressif)** si vous préférez des paramètres de minuteur de basculement plus rapides. Le profil **Advanced (Avancé)** vous permet de personnaliser les valeurs des minuteurs pour répondre à vos besoins en matière de réseau.

Le tableau suivant décrit chaque minuteur inclus dans les profils et les valeurs actuellement prédéfinies (recommandées/agressives) sur les différents modèles matériels ; ces valeurs ne sont données qu'à titre indicatif et peuvent changer dans une version ultérieure.

*Les minuteurs qui affectent les membres d'un cluster HA sont décrits dans* Configuration de la mise en cluster HA.

| Minuteurs | Description | PA-7000 Series<br>PA-5200 Series<br>PA-3200 Series | PA-800 Series<br>PA-220<br>VM-Series | Appareil virtuel Panorama<br>M-Series Panorama |
|---|---|---|---|---|
| Temps d'attente actif après l'échec de la surveillance (ms) | Intervalle pendant lequel le pare-feu reste actif après un échec de surveillance des chemins ou des liaisons. Ce paramètre est recommandé pour empêcher un | 0/0 | 0/0 | 0/0 |

| Minuteurs | Description | PA-7000 Series<br>PA-5200 Series<br>PA-3200 Series | PA-800 Series<br>PA-220<br>VM-Series | Appareil virtuel Panorama<br>M-Series Panorama |
|---|---|---|---|---|
| | basculement HA dû au battement occasionnel de périphériques à proximité. | | | |
| Délai de maintien de préemption (min) | Temps d'attente du pare-feu passif ou actif-secondaire avant de prendre le relais en tant que pare-feu actif ou actif-principal. | 1/1 | 1/1 | 1/1 |
| Intervalle de pulsation (ms) | Fréquence à laquelle les homologues HA échangent des messages de pulsation sous la forme d'une requête ping ICMP. | 1000/1000 | 2000/1000 | 2000/1000 |
| Délai de maintien de promotion (ms) | Temps d'attente du pare-feu passif (en mode actif/passif) ou du pare-feu actif-secondaire (en mode actif/actif) avant de prendre le relais en tant que pare-feu actif ou actif-principal après la perte de la communication avec l'homologue HA. Ce délai de maintien démarre après la déclaration de l'échec de l'homologue uniquement. | 2000/500 | 2000/500 | 2000/500 |
| Temps d'attente actif principal supplémentaire (ms) | Temps d'intervalle en millisecondes appliqué au même événement que le Temps d'attente actif après l'échec de la surveillance (plage de 0 à 60 000, par | 500/500 | 500/500 | 7000/5000 |

| Minuteurs | Description | PA-7000 Series<br>PA-5200 Series<br>PA-3200 Series | PA-800 Series<br>PA-220<br>VM-Series | Appareil virtuel Panorama<br>M-Series Panorama |
|---|---|---|---|---|
| | défaut 500). Cette durée supplémentaire s'applique uniquement au pare-feu actif en mode actif/passif et au pare-feu actif-principal en mode actif/actif. Ce délai est recommandé pour empêcher un basculement lorsque les deux pare-feu rencontrent le même échec de surveillance des liaisons/chemins simultanément. | | | |
| Intervalle Hello (ms) | Intervalle en millisecondes entre l'envoi des paquets hello et la vérification que la fonctionnalité HA sur l'autre pare-feu est opérationnelle (plage de 8 000 à 60 000 ; par défaut 8 000). | 8000/8000 | 8000/8000 | 8000/8000 |
| Battement Max | Un battement est calculé lorsque l'une des situations suivantes se produit :<br>• Un pare-feu préemptif quitte l'état actif 20 minutes après être devenu actif.<br>• Après être devenu actif, une liaison ou un chemin ne peut rester actif pendant 10 minutes.<br>Cette valeur indique le nombre maximum de battements autorisés | 3/3 | 3/3 | Non applicable |

| Minuteurs | Description | PA-7000 Series<br>PA-5200 Series<br>PA-3200 Series | PA-800 Series<br>PA-220<br>VM-Series | Appareil virtuel Panorama<br>M-Series Panorama |
|---|---|---|---|---|
| | avant que le pare-feu ne soit considéré comme suspendu et que le pare-feu passif ne prenne le relais (plage de 0 à 16, par défaut 3). | | | |

## Propriétaire de session

Dans une configuration HD actif/actif, les deux pare-feux sont actifs simultanément, ce qui signifie que les paquets peuvent être distribués entre eux. Une telle distribution suppose que les pare-feux doivent remplir deux fonctions, soit la propriété et le paramétrage de la session. Généralement, chaque pare-feu qui compose la paire remplit l'une de ces fonctions, ce qui permet d'empêcher des situations de course possibles dans les environnements acheminés de manière asymétrique.

Vous configurez le propriétaire des sessions de sorte qu'il s'agisse du pare-feu qui reçoit le premier paquet d'une nouvelle session de la part de l'hôte final ou du pare-feu qui se trouve à l'état actif principal (le périphérique principal). Si le périphérique principal est configuré, mais que le pare-feu qui reçoit le premier paquet n'est pas à l'état actif principal, le pare-feu transmet le paquet au pare-feu homologue (le propriétaire de la session) via la liaison HD3.

Le propriétaire de la session effectue le traitement de Couche 7, par exemple, App-ID, Content-ID et l'analyse des menaces, applicable à la session. Le propriétaire de la session génère également tous les journaux du trafic de la session.

En cas d'échec du propriétaire de la session, le pare-feu homologue devient le propriétaire de la session. Les sessions existantes basculent vers le pare-feu actif et aucun traitement de Couche 7 n'est disponible pour ces sessions. Lorsqu'un pare-feu récupère d'un échec, toutes les sessions qui lui appartenaient avant l'échec reviennent au pare-feu d'origine ; le traitement de Couche 7 ne reprend pas.

Si vous configurez la propriété de session pour qu'elle corresponde au périphérique principal, le paramétrage de session est également défini par défaut sur Périphérique principal.

*Palo Alto Networks recommande de définir le Propriétaire de session sur Premier paquet et le Paramétrage de session sur Modulo IP, sauf indication contraire dans un cas pratique particulier. En définissant le propriétaire de session sur le premier paquet réduit le trafic sur l'ensemble de la liaison HA3 et permet de distribuer la charge des plans de données sur l'ensemble des homologues.*

*La définition du Propriétaire de la session et du Paramétrage de la session sur Périphérique principal fait en sorte que le pare-feu actif principal traite tout le trafic. Vous pouvez procéder à cette configuration pour l'une des raisons suivantes :*

- *Vous capturez des journaux et des captures de paquets et résolvez des problèmes connexes, afin que le traitement des paquets ne soit pas réparti entre les pare-feu.*
- *Vous voulez obliger la paire HD actif/actif à fonctionner comme une paire HD actif/passif. Reportez-vous à la section* Cas d'utilisation : Configuration de la HA active/active avec des adresses IP flottantes liées a un pare-feu actif principal.

## Configuration de la session

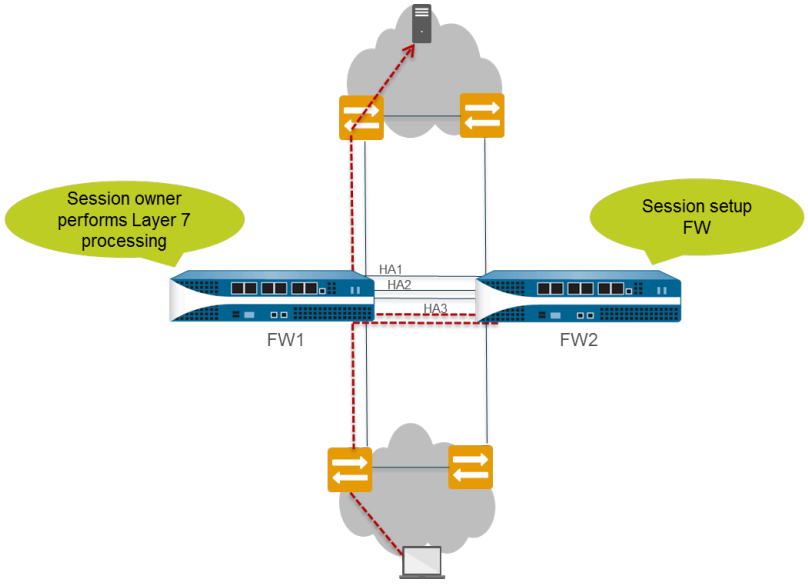
Le pare-feu configuré pour la session effectue le traitement de la Couche 2 à la Couche 4 qui est nécessaire pour configurer une session. Le pare-feu configuré pour la session effectue également les opérations de NAT à l'aide du pool NAT du propriétaire de la session. Vous déterminez le pare-feu configuré pour la session d'une configuration actif/actif en sélectionnant l'une des options de partage de charge du paramétrage de session.

| Option de Configuration de la session | Description |
|---|---|
| **Modulo IP** | Le pare-feu distribue la charge du paramétrage de session en fonction de la parité de l'adresse IP source. C'est une méthode déterministe de partage du paramétrage de session. |
| **Hachage IP** | Le pare-feu utilise un hachage des adresses IP source et de destination pour transférer les responsabilités de paramétrage de la session. |
| **Périphérique principal** | Le pare-feu actif principal configure toujours la session ; un seul pare-feu effectue toutes les responsabilités de paramétrage de la session. |
| **Premier paquet** | Le pare-feu qui reçoit le premier paquet d'une session effectue le paramétrage de la session. |

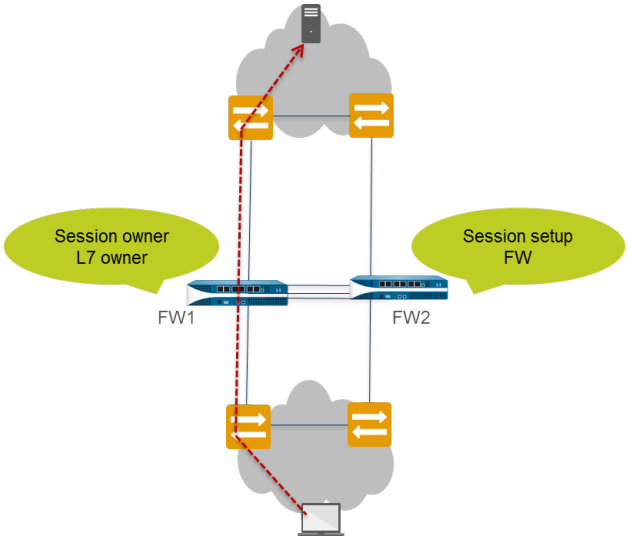
- *Si vous souhaitez partager la charge des responsabilités du propriétaire de session et du paramétrage de session, définissez le propriétaire de session sur Premier paquet et le paramètre de session sur Modulo IP. Ce sont les paramètres recommandés.*
- *Si vous souhaitez capturer des journaux ou des captures de paquets ou résoudre des problèmes connexes, ou si vous voulez qu'une paire HD actif/actif fonctionne comme une paire HD actif/passif, définissez le propriétaire de session et le paramétrage de session sur Périphérique principal afin que le périphérique actif principal effectue le traitement de l'ensemble du trafic. Reportez-vous à la section* Cas d'utilisation : Configuration de la HD actif/actif avec des adresses IP flottantes liées à un pare-feu principal actif.

Le pare-feu utilise la liaison HD3 pour envoyer les paquets à son homologue pour le paramétrage de la session, au besoin. La figure et le texte suivants décrivent le chemin parcouru par un paquet que le pare-feu FW1 reçoit pour initier une nouvelle session. Les lignes pointillées rouges indiquent le transfert du paquet par FW1 à FW2 et le retour du paquet par FW2 à FW1 via la liaison HD3.




- L'hôte final envoie un paquet à FW1.
- FW1 examine le contenu du paquet pour le faire correspondre à une session existante. S'il n'y a aucune concordance de session, FW1 détermine qu'il a reçu le premier paquet d'une nouvelle session et, par conséquent, devient le propriétaire de la session (en supposant que la **Sélection du propriétaire de la session** est définie sur **Premier paquet**).
- FW1 utilise l'option de partage de charge du paramétrage de session configurée pour identifier le pare-feu configuré pour la session. Dans cet exemple, FW2 est configuré pour effectuer le paramétrage de la session.
- FW1 utilise la liaison HD3 pour envoyer le premier paquet à FW2.
- FW2 configure la session et retourne le paquet à FW1 pour le traitement de Couche 7, le cas échéant.
- FW1 transfère alors le paquet à la destination via l'interface de sortie.

La figure et le texte suivants décrivent le chemin parcouru par un paquet qui correspond à une session existante :




- L'hôte final envoie un paquet à FW1.
- FW1 examine le contenu du paquet pour le faire correspondre à une session existante. Si la session correspond à une session existante, FW1 traite le paquet et l'envoie à la destination via l'interface de sortie.

## NAT en mode HA active/active

Dans une configuration HA active / active :

- Vous devez lier chaque règle NAT Dynamic IP (IP dynamique ; DIP) et la règle NAT Dynamic IP and Port (Port et adresse IP dynamiques ; DIPP) à l'ID de périphérique 0 ou à l'ID de périphérique 1.
- Vous devez lier chaque règle NAT statique à l'ID de périphérique 0, à l'ID de périphérique 1, aux deux ID de périphérique ou au pare-feu à l'état actif-principal.

Ainsi, lorsque l'un des pare-feux crée une nouvelle session, la liaison de l'ID du périphérique **0** ou ID du périphérique **1** détermine quelles règles NAT correspondent au pare-feu. La liaison de périphérique doit inclure le pare-feu du propriétaire de session pour produire une correspondance.

Le pare-feu d'installation de session effectue la correspondance de la règle NAT, mais les règles NAT sont évaluées en fonction du propriétaire de la session. La session est traduite en fonction des règles NAT associées au pare-feu propriétaire de la session. Lors de l'exécution de la correspondance de stratégie NAT, un pare-feu ignore toutes les règles NAT qui ne sont pas liées au pare-feu du propriétaire de la session.

Par exemple, supposons que le pare-feu ayant le périphérique 1 est le propriétaire de la session et le pare-feu configuré pour la session. Lorsque le périphérique 1 tente de mettre en correspondance une session et une règle NAT, il saute toutes les règles liées au périphérique ID 0. Le pare-feu n'effectue la traduction NAT que si le propriétaire de la session et l'ID de périphérique dans la règle NAT correspondent.

Vous allez généralement créer des règles NAT spécifiques aux périphériques lorsque les pare-feux homologues utilisent des adresses IP différentes pour la traduction.

Si l'un des pare-feu homologue tombe en panne, le pare-feu actif continue de traiter le trafic pour les sessions synchronisées à partir du pare-feu défaillant, y compris le trafic NAT. Dans une configuration NAT source, lorsqu'un pare-feu échoue :

- L'adresse IP flottante utilisée comme adresse IP traduite de la règle NAT est transférée vers le pare-feu restant. Par conséquent, les sessions existantes qui basculent utiliseront toujours cette adresse IP.
- Toutes les nouvelles sessions utiliseront les règles NAT spécifiques au périphérique que le pare-feu survivant possède naturellement. Autrement dit, le pare-feu survivant traduit les nouvelles sessions en utilisant uniquement les règles NAT qui correspondent à son ID de périphérique; il ignore les règles NAT liées à l'ID de périphérique en échec.

Pour des exemples de HA Active/Active avec NAT, voir :

- Cas d'utilisation : Configuration de la HA active/active avec la NAT DIPP source à l'aide d'adresses IP flottantes
- Cas d'utilisation : Configuration de pools d'adresses IP NAT source séparés pour des pare-feu HA actifs/actifs
- Cas d'utilisation : Configuration de la HA active/active avec le partage de charge ARP avec la NAT de destination
- Cas d'utilisation : Configuration de la HA active/active avec le partage de charge ARP avec la NAT de destination dans la Couche 3

## ECMP en mode HA active/active

En cas d'échec d'un homologue HD actif/actif, ses sessions sont transférées au nouveau pare-feu actif principal, qui tente d'utiliser la même interface de sortie que le pare-feu ayant échoué utilisait. Si le pare-feu trouve cette interface parmi les chemins ECMP, les sessions transférées disposent alors du même chemin et de la même interface de sortie. Ce comportement se produit quel que soit l'algorithme ECMP utilisé ; il est recommandé d'utiliser la même interface.

Le pare-feu actif-principal sélectionne un nouveau chemin ECMP uniquement si aucun chemin ECMP ne correspond à l'interface de sortie d'origine.

Si vous n'avez pas configuré les mêmes interfaces sur les homologues actifs/actifs, lorsqu'un basculement se produit, le pare-feu actif principal sélectionne le meilleur chemin suivant dans la table FIB. Par conséquent, il se peut que les sessions existantes ne soient pas réparties en fonction de l'algorithme ECMP.

# Configuration de la HD active/passive



## Configuration requise pour la HA active/passive

Pour configurer la haute disponibilité sur vos pare-feu Palo Alto Networks, vous avez besoin d'une paire de pare-feu répondant aux exigences suivantes :

- **Modèle identique** : les deux pare-feu de la paire doivent être du même modèle matériel ou du même modèle de machine virtuelle.
- **Version PAN-OS identique** : les deux pare-feu doivent exécuter la même version de PAN-OS et doivent chacun être à jour dans les bases de données d'applications, d'URL et de menaces.
- Les mêmes fonctions de systèmes virtuels multiples : Les **fonctions de systèmes virtuels multiples** doivent être activées ou désactivées sur les deux pare-feu. Lorsqu'elles sont activées, chaque pare-feu doit avoir ses propres licences de systèmes virtuels multiples.
- **Types d'interfaces identiques** : des liaisons HA dédiées ou la combinaison d'un port de gestion à des ports sur bande qui sont définis sur le ***type d'interface*** HA.
  - Déterminez l'adresse IP de la connexion HA1 (contrôle) entre les homologues HA. L'adresse IP HA1 des deux homologues doit apparaître sur le même sous-réseau s'ils sont directement connectés ou s'ils sont connectés au même commutateur.

    Pour les pare-feu ne disposant pas de ports HA dédiés, vous pouvez utiliser le port de gestion pour la connexion de contrôle. L'utilisation de ce port fournit une liaison de communication directe entre les plans de gestion sur les deux pare-feu. Toutefois, étant donné que les ports de gestion ne seront pas directement câblés entre les homologues, vérifiez que vous disposez d'un itinéraire qui connecte ces deux interfaces dans votre réseau.
  - Si vous utilisez la Couche 3 comme mode de transport pour la connexion HA2 (données), déterminez l'adresse IP de la liaison HA2. Utilisez la Couche 3 uniquement si la connexion HA2 doit communiquer sur un réseau routé. Le sous-réseau IP des liaisons HA2 ne doit pas chevaucher sur celui des liaisons HA1 ou sur aucun des autres sous-réseaux affectés aux ports de données sur le pare-feu.
- **Ensemble de licences identiques** : les licences sont uniques pour chaque pare-feu et ne peuvent pas être partagées entre plusieurs pare-feu. Par conséquent, vous devez attribuer des licences identiques aux deux pare-feu. Si ces derniers ne disposent pas d'un ensemble de licences

identiques, ils ne peuvent pas synchroniser les informations de configuration et gérer la parité pour un basculement transparent.

***Si vous disposez déjà d'un pare-feu et que vous souhaitez ajouter un nouveau pare-feu à des fins de HD et que le nouveau pare-feu a une configuration existante, un*** Rétablissement des paramètres d'usine par défaut du pare-feu ***est recommandé sur le nouveau pare-feu. Ainsi, le nouveau pare-feu a une configuration propre. Une fois la HD configurée, vous devez synchroniser la configuration du pare-feu principal avec celle du nouveau pare-feu.***

## Directives de configuration de la HA active/passive

Pour configurer une paire active (HomologueA)/passive (HomologueB) en HA, vous devez configurer à l'identique certaines options sur les deux pare-feu et d'autres indépendamment (non correspondantes) sur chaque pare-feu. Ces paramètres HA ne sont pas synchronisés entre les pare-feu. Pour plus d'informations sur ce qui est synchronisé ou pas, reportez-vous à la section Référence : Synchronisation de Haute Disponibilité.

La liste de contrôle suivante présente les paramètres que vous devez configurer à l'identique sur les deux pare-feu :

- Vous devez activer la HA sur les deux pare-feu.
- Vous devez configurer la même valeur ID de groupe sur les deux pare-feu. Le pare-feu se sert de la valeur ID de groupe pour créer une adresse MAC virtuelle pour l'ensemble des interfaces configurées. Reportez-vous à la section Adresse IP flottante et adresse MAC virtuelle pour obtenir de plus amples informations sur les adresses MAC virtuelles. Lorsqu'un nouveau pare-feu actif prend le relais, il envoie des messages ARP gratuits à partir de chacune de ses interfaces connectées afin d'informer les commutateurs de Couche 2 connectés du nouvel emplacement de l'adresse MAC virtuelle.
- Si vous utilisez des ports sur bande comme liaison HA, vous devez définir les interfaces des liaisons HA1 et HA2 sur le type de HA.
- Définissez le mode HA sur Actif/Passif sur les deux pare-feu.
- Au besoin, activez la préemption sur les deux pare-feu. Toutefois, la valeur de priorité du périphérique ne doit pas être identique.
- Au besoin, configurez le chiffrement de la liaison HA1 (pour les communications entre des homologues HA) sur les deux pare-feu.

- Selon la combinaison des ports HA1 et HA1 de secours que vous utilisez, suivez les recommandations suivantes pour déterminer si vous devez activer la sauvegarde des pulsations :

  > ***La fonctionnalité HA (HA1 et HA1 de secours) n'est pas prise en charge sur l'interface de gestion si l'adressage DHCP y est configuré (IP Type (Type d'adresse IP) défini sur DHCP Client (Client DHCP)). Les exceptions sont AWS et Azure, où l'interface de gestion est configurée en tant que client DHCP et prend en charge les liaisons HA1 et HA1 de secours.***

  - HA1 : Port HA1 dédié

    HA1 de secours : Port HA1 dédié

    **Recommandation :** activer la sauvegarde des pulsations
  - HA1 : Port HA1 dédié

    HA1 de secours : Port sur bande

    **Recommandation :** activer la sauvegarde des pulsations
  - HA1 : Port HA1 dédié

    HA1 de secours : port de gestion

    **Recommandation :** ne pas activer la sauvegarde des pulsations
  - HA1 : Port sur bande

    HA1 de secours : Port sur bande

    **Recommandation :** activer la sauvegarde des pulsations
  - HA1 : port de gestion

    HA1 de secours : Port sur bande

    **Recommandation :** ne pas activer la sauvegarde des pulsations

Le tableau suivant répertorie les paramètres HA que vous devez configurer indépendamment sur chaque pare-feu. Consultez la section Référence : Synchronisation de Haute Disponibilité pour obtenir de plus amples renseignements sur les autres paramètres de configuration qui ne sont pas automatiquement synchronisés entre des homologues.

| Paramètres de configuration indépendants | HomologueA | HomologueB |
|---|---|---|
| Liaison de contrôle | Adresse IP de la liaison HA1 configurée sur ce pare-feu (HomologueA). | Adresse IP de la liaison HA1 configurée sur ce pare-feu (HomologueB). |
| | Pour les pare-feu ne disposant pas de ports HA dédiés, utilisez l'adresse IP du port de gestion de la liaison de contrôle. | |
| Liaison de données | Par défaut, la liaison HA2 utilise Ethernet/Couche 2. | Par défaut, la liaison HA2 utilise Ethernet/Couche 2. |

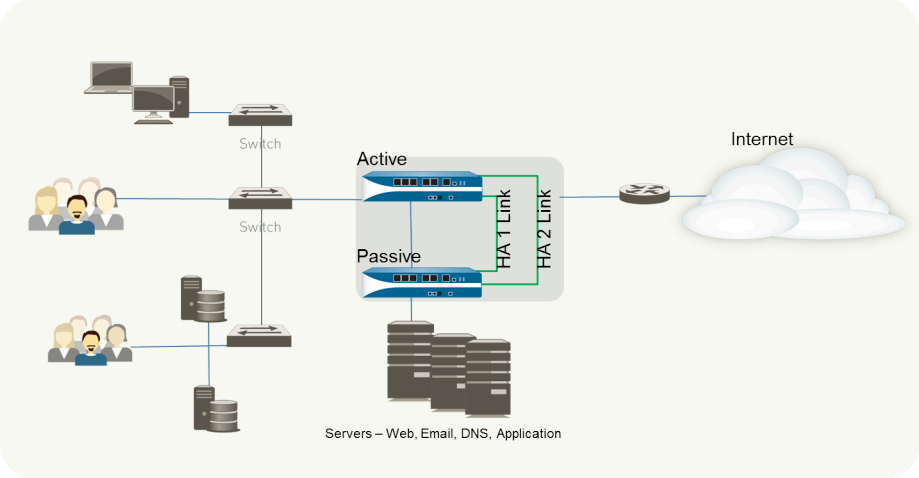
| Paramètres de configuration indépendants | HomologueA | HomologueB |
|---|---|---|
| Les informations de liaison des données sont synchronisées entre les pare-feu une fois que la HA est activée et que la liaison de contrôle est établie entre les pare-feu. | Si une connexion de Couche 3 est utilisée, configurez l'adresse IP de la liaison de données sur ce pare-feu (HomologueA). | Si une connexion de Couche 3 est utilisée, configurez l'adresse IP de la liaison de données sur ce pare-feu (HomologueB). |
| Priorité des périphériques (obligatoire, à condition que la préemption soit activée) | Le pare-feu que vous prévoyez d'activer doit afficher une valeur numérique inférieure à celle de son homologue. Par conséquent, si HomologueA doit fonctionner en tant que pare-feu actif, conservez la valeur 100 par défaut et augmentez la valeur de HomologueB.<br>Si les deux pare-feu affichent une valeur de priorité du périphérique identique, ils utilisent l'adresse MAC de leur HD1 pour briser l'égalité. | Si HomologueB est passif, définissez la valeur de priorité du périphérique sur un nombre supérieur à celui de HomologueA. Par exemple, définissez la valeur sur 110. |
| Surveillance des liaisons : surveillez une ou plusieurs interfaces physiques gérant le trafic vital de ce pare-feu et définissez la condition d'échec. | Sélectionnez les interfaces physiques sur le pare-feu que vous voulez surveiller et définissez la condition d'échec (toutes ou n'importe laquelle) pour déclencher un basculement. | Sélectionnez un ensemble d'interfaces physiques similaires que vous voulez surveiller sur ce pare-feu et définissez la condition d'échec (toutes ou n'importe laquelle) pour déclencher un basculement. |
| Surveillance des chemins : surveillez une ou plusieurs adresses IP de destination que le pare-feu peut utiliser pour envoyer des requêtes ping ICMP afin | Définissez la condition d'échec (toutes ou n'importe laquelle), l'intervalle des requêtes ping et le nombre de requêtes ping. Ceci est particulièrement utile pour surveiller la disponibilité des autres périphériques réseau interconnectés. Par exemple, surveillez la disponibilité d'un routeur qui se connecte à un serveur, la connectivité au serveur même ou un autre équipement vital qui fait partie du flux du trafic. | Sélectionnez un ensemble de périphériques ou d'adresses IP de destination similaires pouvant être surveillés afin de déterminer le déclencheur de basculement pour HomologueB. Définissez la condition d'échec (toutes ou n'importe laquelle), l'intervalle des requêtes ping et le nombre de requêtes ping. |

| Paramètres de configuration indépendants | HomologueA | HomologueB |
|---|---|---|
| de vérifier la réactivité. | Vérifiez que le nœud/le périphérique que vous surveillez n'a pas tendance à être non réactif, surtout lors de son chargement, car ceci pourrait entraîner un échec de surveillance des chemins et déclencher un basculement. | |

## Configuration de la HA active/passive

La procédure suivante explique comment configurer une paire de pare-feu dans un déploiement actif/passif comme décrit dans l'exemple de topologie suivant.




Pour configurer une paire HA active/passive, vous devez d'abord suivre le flux de travail suivant sur le premier pare-feu, puis répétez les étapes sur le second pare-feu.

**STEP 1 |** Connectez les ports HA afin de configurer une connexion physique entre les pare-feu.

- Pour les pare-feu dotés de ports HA dédiés, utilisez un câble Ethernet pour connecter les ports HA1 dédiés et les ports HA2 sur les homologues. Utilisez un câble croisé si les pare-feu sont directement connectés les uns aux autres.
- Pour les pare-feu ne disposant pas de ports HA dédiés, sélectionnez deux interfaces de données pour la liaison HA2 et la liaison HA1 de secours. Utilisez ensuite un câble Ethernet pour connecter ces interfaces HA sur bande aux deux pare-feu.

Utilisez le port de gestion pour la liaison HA1 et vérifiez que les ports de gestion peuvent se connecter les uns aux autres dans votre réseau.

**STEP 2 |** Activez une requête ping sur le port de gestion.

Son activation permet au port de gestion d'échanger des informations sur la sauvegarde des pulsations.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Management Interface Settings (Paramètres de l'interface de gestion).
2. Sélectionnez **Ping (Ping)** en tant que service autorisé sur l'interface.

**STEP 3 |** Si le pare-feu ne dispose pas de ports HA dédiés, configurez les ports de données pour qu'ils fonctionnent en tant que ports HA.

Pour les pare-feu dotés de ports HA dédiés, passez à l'étape suivante.

1. Sélectionnez **Network (Réseau)** > **Interfaces**.
2. Vérifiez que la liaison est active sur les ports que vous voulez utiliser.
3. Sélectionnez l'interface et définissez l'option **Interface Type (Type d'interface)** sur **HA (HA)**.
4. Définissez les paramètres **Link Speed (Vitesse de liaison)** et **Link Duplex (Duplex de la liaison)**, selon le cas.

**STEP 4 |** Définissez le mode HA et l'ID de groupe.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, puis modifiez la section Setup (Configuration).
2. Définissez un **Group ID (ID de groupe)** et saisissez éventuellement une **Description (Description)** de la paire. L'ID de groupe identifie de façon unique chaque paire sur votre réseau. Si vous disposez de plusieurs paires HD qui partagent le même domaine de diffusion, vous devez définir un ID de groupe unique pour chaque paire.
3. Définissez le mode sur **Active Passive (Actif/passif)**.

**STEP 5 |** Configurez la connexion de la liaison de contrôle.

Cet exemple montre un port sur bande défini sur le type d'interface HA.

Pour les pare-feu utilisant le port de gestion en tant que liaison de contrôle, les informations concernant l'adresse IP sont automatiquement prérenseignées.

1. Dans **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, modifiez la section Control Link (HA1) (Liaison de contrôle (HA1)).
2. Sélectionnez le **Port (Port)** que vous avez câblé afin de l'utiliser en tant que liaison HA1.
3. Définissez les options **IPv4/IPv6 Address (Adresse IPv4/IPv6)** et **Netmask (Masque réseau)**.

   Si les interfaces HA1 se trouvent sur des sous-réseaux distincts, saisissez l'adresse IP de la **Gateway (Passerelle)**. N'ajoutez pas d'adresse de passerelle si les pare-feu sont directement connectés ou s'ils se trouvent sur le même VLAN.

**STEP 6 |** (Facultatif) Activez le chiffrement de la connexion de la liaison de contrôle.

Il permet généralement de sécuriser la liaison si les deux pare-feu ne sont pas directement connectés, c'est-à-dire lorsque les ports sont connectés à un commutateur ou à un routeur.

1. Exportez la clé HA d'un pare-feu et importez-la sur le pare-feu homologue.
   1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**.
   2. Sélectionnez **Export HD key (Exporter la clé HD)**. Enregistrez la clé HA sur un emplacement réseau auquel l'homologue peut accéder.
   3. Sur le pare-feu homologue, sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**, puis **Import HA key (Importer la clé HA)** pour accéder à l'emplacement dans lequel vous avez sauvegardé la clé et l'importer sur l'homologue.
   4. Répétez ce processus sur le second pare-feu pour échanger les clés HA sur les deux périphériques.
2. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, modifiez la section Control Link (HA1) (Liaison de contrôle (HA1)).
3. Sélectionnez **Encryption Enabled (Chiffrement activé)**.

   *Si vous activez le chiffrement, une fois que vous avez fini de configurer les pare-feu HA, vous pouvez* Actualisation des clés SSH HA1 et configuration des options des clés.

**STEP 7 |** Configurez la connexion de la liaison de contrôle de secours.

1. Dans **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, modifiez la section Control Link (HA1 Backup) (Liaison de contrôle (HA1 de secours)).
2. Sélectionnez l'interface HA1 de secours, puis définissez les options **IPv4/IPv6 Address (Adresse IPv4/IPv6)** et **Netmask (Masque réseau)**.

   *Les pare-feu PA-3200 Series ne prennent pas en charge l'adresse IPv6 pour la liaison de contrôle HA1 de secours ; utilisez une adresse IPv4.*

**STEP 8 |** Configurez la connexion de la liaison de données (HA2) et la connexion HA2 de secours entre les pare-feu.

1. Dans **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, modifiez la section Data Link (HA2) (Liaison de données (HA2)).
2. Sélectionnez le **Port (Port)** à utiliser pour la connexion de la liaison de données.
3. Sélectionnez la méthode de **Transport (Transport)**. La valeur par défaut est **ethernet (ethernet)** et sera utilisée lorsque la paire HD sera connectée directement ou via un

commutateur. Si vous devez acheminer le trafic de la liaison de données via le réseau, sélectionnez **IP (IP)** ou **UDP (UDP)** comme mode de transport.

4. Si vous utilisez IP ou UDP comme mode de transport, définissez les options **IPv4/IPv6 Address (Adresse IPv4/IPv6)** et **Netmask (Masque réseau)**.
5. Vérifiez que l'option **Enable Session Synchronization (Activer la synchronisation de la session)** est sélectionnée.
6. Sélectionnez **HA2 Keep-alive (Persistance HA2)** pour activer la surveillance sur la liaison de données HD2 entre les homologues HD. Si un échec se produit en fonction du seuil défini (la valeur par défaut étant 10 000 ms), l'action définie va s'exécuter. Pour la configuration active/passive, un message critique du journal système est généré en cas d'échec de la persistance HA2.

   *Vous pouvez configurer l'option Persistance HA2 sur les deux pare-feu ou sur un seul pare-feu de la paire HA. Si l'option n'est activée que sur un seul pare-feu, il sera le seul à envoyer des messages de persistance. L'autre pare-feu sera informé en cas d'échec.*
7. Modifiez la section **Data Link (HA2 Backup) (Liaison de données (HA2 de secours))**, sélectionnez l'interface, puis définissez les options **IPv4/IPv6 Address (Adresse IPv4/IPv6)** et **Netmask (Masque réseau)**.

**STEP 9 |** Activez la sauvegarde des pulsations si votre liaison de contrôle utilise un port HA dédié ou un port sur bande.

Vous n'avez pas besoin d'activer la sauvegarde des pulsations si vous utilisez le port de gestion pour la liaison de contrôle.

1. Dans **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, modifiez la section Election Settings (Paramètres de sélection).
2. Sélectionnez **Heartbeat Backup (Sauvegarde des pulsations)**.

   Pour permettre la transmission des pulsations entre les pare-feu, vous devez vérifier que le port de gestion des deux homologues peut acheminer les pulsations vers l'un comme vers l'autre.

   *L'activation de la sauvegarde des pulsations vous permet également d'empêcher une situation de « split brain ». Un « split brain » se produit lorsque la liaison HA1 s'arrête, le pare-feu manquant ainsi des pulsations, et ce alors qu'il fonctionne toujours. Dans une telle situation, chaque homologue pense que l'autre est arrêté et tente de démarrer des services déjà exécutés, entraînant ainsi un « split brain ». Lorsque la liaison de sauvegarde des pulsations est activée, le « split brain » est empêché car des pulsations redondantes et des messages hello sont transmis sur le port de gestion.*

**STEP 10 |** Définissez la priorité des périphériques et activez la préemption.

Ce paramètre est uniquement requis si vous voulez vous assurer qu'un pare-feu spécifique est le pare-feu actif favori. Pour plus d'informations, reportez-vous à la section Priorité et préemption des périphériques.

1. Dans **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, modifiez la section Election Settings (Paramètres de sélection).
2. Définissez la valeur numérique dans **Device Priority (Priorité du périphérique)**. Veillez à définir une valeur numérique inférieure sur le pare-feu auquel vous voulez affecter une priorité supérieure.

   *Si les deux pare-feu affichent une valeur de priorité du périphérique identique, le pare-feu disposant de l'adresse MAC la plus basse sur la liaison de contrôle HA1 va devenir le pare-feu actif.*
3. Sélectionnez **Preemptive (Préemptif)**.

   Vous devez activer l'option Préemptif sur les pare-feu actif et passif.

**STEP 11 |** (Facultatif) Modifiez les minuteurs HA.

Par défaut, le profil de minuteur HA est défini sur **Recommended (Recommandé)** et est adapté à la plupart des déploiements HA.

1. Dans **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, modifiez la section Election Settings (Paramètres de sélection).
2. Sélectionnez le profil **Aggressive (Agressif)** pour déclencher le basculement de manière plus rapide ; sélectionnez **Advanced (Avancé)** pour définir des valeurs personnalisées déclenchant le basculement dans votre configuration.

   *Pour afficher la valeur prédéfinie d'un minuteur inclus dans un profil, sélectionnez **Advanced (Avancé)** et cliquez sur **Load Recommended (Charger le profil recommandé)** ou **Load Aggressive (Charger le profil agressif)**. Les valeurs prédéfinies de votre modèle matériel s'affichent alors à l'écran.*

**STEP 12 |** (Facultatif) Modifiez l'état de la liaison des ports HD sur le pare-feu passif.

*L'état de la liaison passive affiche **shutdown (arrêté)**, par défaut. Une fois la HA activée, l'état de la liaison des ports HA sur le pare-feu actif s'affichera en vert et ceux du pare-feu passif seront inactifs et s'afficheront en rouge.*

Le paramètre **Auto (Auto)** de l'état de la liaison permet de réduire le délai nécessaire au pare-feu passif pour prendre le relais en cas de basculement et vous permet de surveiller l'état de la liaison.

Pour activer l'état de la liaison sur le pare-feu passif afin qu'elle reste active et reflète l'état du câblage sur l'interface physique :

1. Dans **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, modifiez la section Active Passive Settings (Paramètres du mode actif/passif).
2. Définissez **Passive Link State (État de la liaison passive)** sur **Auto (Auto)**.

   L'option Auto réduit le délai nécessaire au pare-feu passif pour prendre le relais en cas de basculement.

   *Bien que l'interface s'affiche en vert (câblée et active), elle continue à supprimer tout trafic jusqu'à ce qu'un basculement soit déclenché.*

   Lorsque vous modifiez l'état de la liaison passive, vérifiez que les périphériques adjacents ne transfèrent pas le trafic vers le pare-feu passif en se basant uniquement sur l'état de la liaison du pare-feu.

**STEP 13 |** Activez la HA.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, puis modifiez la section Setup (Configuration).
2. Sélectionnez **Enable HD (Activer la HD)**.
3. Sélectionnez **Enable Config Sync (Activer la synchronisation de la configuration)**. Ce paramètre permet la synchronisation des paramètres de configuration entre les pare-feu actif et passif.
4. Saisissez l'adresse IP affectée à la liaison de contrôle de l'homologue dans **Peer HA1 IP Address (Adresse IP de l'homologue HD1)**.

   Pour les pare-feu ne disposant pas de ports HA dédiés, si l'homologue utilise le port de gestion pour la liaison HA1, saisissez l'adresse IP du port de gestion de l'homologue.
5. Définissez l'option **Backup HA1 IP Address (Adresse IP HA1 de secours)**.

**STEP 14 |** (Facultatif) Activez la prénégociation LACP et LLDP pour la HA active/passive pour un basculement plus rapide si votre réseau utilise LACP ou LLDP.

*Activez LACP et LLDP avant de configurer la prénégociation HD du protocole si vous voulez que la prénégociation fonctionne en mode actif.*

1. À l'étape 12, assurez-vous de définir l'état de liaison sur **Auto (Auto)**.
2. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**.
3. Pour activer la prénégociation LACP active :
   1. Sélectionnez une interface Ethernet agrégée dans un déploiement de Couche 2 ou de Couche 3.
   2. Sélectionnez l'onglet **LACP (LACP)**.
   3. Sélectionnez **Enable in HA Passive State (Activation à l'état HA passif)**.
   4. Cliquez sur **OK**.

   *Vous ne pouvez plus sélectionner l'option **Same System MAC Address for Active-Passive HA (Adresse MAC système identique pour la HD active/passive)**, étant donné que la prénégociation exige la présence d'adresses MAC d'interface uniques sur les pare-feu actif et passif.*
4. Pour activer la prénégociation LACP passive :
   1. Sélectionnez une interface Ethernet dans un déploiement de câble virtuel.
   2. Sélectionnez l'onglet **Advanced (Avancé)**.
   3. Sélectionnez l'onglet **LACP (LACP)**.
   4. Sélectionnez **Enable in HA Passive State (Activation à l'état HA passif)**.
   5. Cliquez sur **OK**.
5. Pour activer la prénégociation LLDP active :
   1. Sélectionnez une interface Ethernet dans un déploiement de Couche 2, de Couche 3 ou de câble virtuel.
   2. Sélectionnez l'onglet **Advanced (Avancé)**.
   3. Sélectionnez l'onglet **LLDP (LLDP)**.
   4. Sélectionnez **Enable in HA Passive State (Activation à l'état HA passif)**.
   5. Cliquez sur **OK**.

   *Si vous souhaitez autoriser la prénégociation LLDP passive pour un déploiement de câble virtuel, effectuez l'étape 14.e, mais n'activez pas LLDP.*

**STEP 15 |** Enregistrez les modifications de configuration.

Cliquez sur **Commit (Valider)**.

**STEP 16 |** Une fois les deux pare-feu configurés, vérifiez qu'ils sont appariés en mode HA active/passive.

1. Accédez au **Dashboard (Tableau de bord)** sur les deux pare-feu et affichez le widget High Availability (Haute disponibilité).
2. Sur le pare-feu actif, cliquez sur le lien **Sync to peer** (Synchroniser avec l'homologue).
3. Vérifiez que les pare-feu sont appariés et synchronisés comme indiqué ci-dessous :
   - Sur le pare-feu passif : l'état du pare-feu local doit afficher **passive (passif)** et la configuration active doit être **synchronized (synchronisée)**.
   - Sur le pare-feu actif : l'état du pare-feu local doit afficher **active (actif)** et la configuration active doit être **synchronized (synchronisée)**.

## Définition des conditions de basculement HA

Effectuez la tâche suivante pour utiliser la surveillance des liens ou des chemins pour définir les conditions Basculement et ainsi établir ce qui provoquera le basculement d'un pare-feu dans une paire HA, un événement où la tâche de sécurisation du trafic passe du pare-feu précédemment actif à son homologue HA. La section Présentation de la HA décrit les conditions qui entraînent un basculement.

Vous pouvez surveiller plusieurs groupes de chemins IP par routeur virtuel, VLAN ou câble virtuel. Vous pouvez activer chaque groupe de chemins avec une ou plusieurs adresses IP et donner à chacun ses propres conditions d'échec. En outre, vous pouvez définir ces conditions d'échec à la fois au niveau du groupe de cheminement et au niveau plus large du routeur virtuel ou du VLAN ou du groupe de filtrage virtuel en utilisant « any » (un quelconque) ou « all » (tous) les contrôles d'échec pour déterminer l'état du pare-feu actif.

Lorsque vous passez à PAN-OS 10.0, le pare-feu transfère automatiquement vos adresses IP de destination actuellement surveillées à un groupe de destination nouvellement créé et donne à ce groupe un nom de surveillance des chemins par défaut. Le nouveau groupe de destination conserve votre condition de basculement précédente au niveau du groupe de chemins.

***Assurez-vous de supprimer toutes les configurations de surveillance des chemins VLAN dans le HA actif/actif avant de passer à PAN-OS 10.1, car la surveillance des chemins VLAN n'est pas compatible avec l'appariement HA actif/actif dans PAN-OS 10.0 ; le fait de conserver une configuration HA actif/actif antérieure entraîne un échec de la validation automatique.***

Avant d'activer la surveillance des chemins, vous devez configurer vos routeurs virtuels, VLAN, ou câbles virtuels ou une combinaison de ces composants logiques de réseau. La surveillance des chemins dans les routeurs virtuels et les câbles virtuels est compatible avec les déploiements HA actifs/actifs et actifs/passifs ; cependant, la surveillance des chemins dans les VLAN n'est prise en charge que sur les paires actives/passives.

Avant d'activer la surveillance des chemins, vous devez également :

- Vérifier l'accessibilité des groupes d'IP de destination dans vos routeurs virtuels.
- Vous assurer que les VLAN (pour lesquels vous avez l'intention d'activer la surveillance des chemins) comprennent des interfaces configurées.
- Obtenir l'adresse IP source que vous utiliserez pour recevoir des pings à partir de l'adresse IP de destination appropriée.

*Si vous utilisez SNMPv3 pour surveiller les pare-feu, notez que l'ID de moteur SNMPv3 est unique pour chaque pare-feu ; l'ID de moteur n'est pas synchronisé dans la paire HA et vous permet ainsi de surveiller indépendamment chaque pare-feu de la paire HA. Pour plus d'informations sur le paramétrage de SNMP, reportez-vous à la section* Transférer des pièges à un gestionnaire SNMP*. L'ID de moteur étant généré à l'aide du numéro de série du pare-feu, vous devez appliquer une licence valide sur le pare-feu VM-Series afin d'obtenir un ID de moteur unique pour chaque pare-feu.*

**STEP 1 |** Pour configurer la surveillance des liens HA, il faut spécifier un groupe d'interfaces physiques que le pare-feu doit surveiller (lien vers le haut ou vers le bas).

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **Link and Path Monitoring (Surveillance des liens et des chemins)**.
2. Dans la section Link Monitoring (Surveillance des liens), **Add (Ajoutez)** un groupe de liens par **Name (Nom)**.
3. Sélectionnez **Enabled (Activé)** pour activer le groupe de liens.
4. Sélectionnez la **Failure Condition (Condition d'échec)** pour les interfaces dans le groupe de liens : **Any (Une quelconque)** (par défaut) ou **All (Toutes)**.
5. **Add (Ajoutez)** la ou les **Interface**s à surveiller.
6. Cliquez sur **OK**.

**STEP 2 |** (Facultatif) Modifiez la condition d'échec des groupes de liens configurés sur le pare-feu.

Par défaut, le pare-feu déclenche un basculement lors de l'échec d'un groupe de liens surveillé quelconque.

1. Modifiez la section **Link Monitoring (Surveillance des liens)**.
2. Réglez la **Failure Condition (Condition d'échec)** sur **Any (Une quelconque)** ou **All (Toutes)**.
3. Cliquez sur **OK**.

**STEP 3 |** Pour configurer la surveillance du chemin d'accès HA pour un câble virtuel, un VLAN ou un routeur virtuel, spécifiez les adresses IP de destination que le pare-feu testera par ping pour vérifier la connectivité du réseau.

1. Dans la section Path Monitoring (Surveillance des chemins), sélectionnez **Add Virtual Wire Path (Ajouter un chemin de câble virtuel)**, **Add VLAN Path (Ajouter un chemin VLAN)** ou **Add Virtual Router Path (Ajouter un chemin de routeur virtuel)**.
2. Saisissez un **Name (Nom)** pour le groupe de chemins de câble virtuel, VLAN ou routeur virtuel.
3. (Chemin de câble virtuel ou chemin VLAN uniquement) Saisissez l'adresse **IP source** à utiliser pour envoyer un ping à l'adresse IP de destination via le câble virtuel ou le VLAN.
4. Sélectionnez **Enabled (Activé)** pour activer le groupe de chemins.
5. Sélectionnez la **Failure Condition (Condition d'échec)** qui se traduit par un échec pour ce groupe de chemins : **Any (Une quelconque)** (par défaut) pour émettre un échec lorsqu'un ou plusieurs groupes d'IP de destination de ce groupe de chemins échouent ou **All (Toutes)**

pour émettre un échec lorsque tous les groupes d'IP de destination dans le groupe de chemins échouent.

6. Entrez le **Ping Interval (Intervalle de ping)** en millisecondes ; l'intervalle entre les messages ICMP envoyés à l'adresse IP de destination (plage de 200 à 60 000 ; la valeur par défaut est 200).
7. Saisissez le **Ping Count (Nombre de requêtes ping)** des requêtes ping devant échoué avant de déclarer un échec (plage de 3 à 10 ; la valeur par défaut est 10).
8. **Add (Ajoutez)** et saisissez un nom de **Destination IP Group (Groupe d'IP de destination)**.
9. **Add (Ajoutez)** une ou plusieurs adresses **IP de destination** auxquelles envoyer le ping.
10. Sélectionnez **Enabled (Activé)** pour activer la surveillance des chemins pour le groupe d'IP de destination.
11. Sélectionnez la **Failure Condition (Condition d'échec)** qui se traduit par un échec pour ce groupe d'IP de destination : **Any (Une quelconque)** (par défaut) pour émettre un échec lorsqu'une ou plusieurs adresses IP indiquées sont injoignables ou **All (Toutes)** pour émettre un échec lorsque toutes les adresses IP indiquées sont injoignables.
12. Cliquez deux fois sur **OK**.
13. (Panorama uniquement) Sélectionnez le modèle Panorama approprié pour pousser la configuration de surveillance des chemins vers votre appareil.

> *Vous pouvez transmettre la surveillance du chemin HA pour un câble virtuel, un VLAN ou un routeur virtuel uniquement vers des pare-feu exécutant PAN-OS 10.1 ou une version ultérieure. Si vous essayez de transmettre la configuration vers des pare-feu exécutant une version antérieure à PAN-OS 10.1 (comme 9.1.x ou 9.0.x), la validation peut échouer ou la validation peut supprimer les adresses IP de destination du groupe de chemins.*

**STEP 4 |** (Facultatif) Modifiez la condition d'échec de tous les groupes de chemins configurés sur le pare-feu.

Par défaut, le pare-feu déclenche un basculement lors de l'échec d'un groupe de chemins surveillé quelconque.

1. Modifiez la section **Path Monitoring (Surveillance des chemins)**.
2. Sélectionnez **Enabled (Activé)** pour activer la surveillance des chemins sur l'appareil.
3. Réglez la **Failure Condition (Condition d'échec)** sur **Any (Une quelconque)** (par défaut) pour émettre un échec pour ce pare-feu lorsqu'un ou plusieurs des routeurs virtuels, VLAN ou câbles virtuels sont en hors service. Sélectionnez **All (Toutes)** pour émettre un échec pour ce pare-feu lorsque tous les routeurs virtuels, VLAN ou câbles virtuels surveillés sont hors service.
4. Cliquez sur **OK**.

**STEP 5 |** **Commit** (Valider).

## Vérification d'un basculement

Pour tester le bon fonctionnement de votre configuration HA, déclenchez un basculement manuel et vérifiez que les pare-feu passent correctement d'un état à un autre.

**STEP 1 |** Suspendez le pare-feu actif.

Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **Operational Commands (Commandes opérationnelles)**, puis cliquez sur le lien **Suspend local device (Suspendre le périphérique local)**.

**STEP 2 |** Vérifiez que le pare-feu passif est passé à l'état actif.

Sur le **Dashboard (Tableau de bord)**, vérifiez que l'état du pare-feu passif passe à **Active (Actif)** dans le widget Haute disponibilité.

**STEP 3 |** Rétablissez l'état fonctionnel du pare-feu suspendu. Patientez quelques minutes, puis vérifiez que la préemption s'est produite, si le mode **Preemptive (Préemptif)** a été activé.

1. Sur le pare-feu précédemment suspendu, sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **Operational Commands (Commandes opérationnelles)**, puis cliquez sur le lien **Make local device functional (Rendre le périphérique local fonctionnel)**.
2. Dans le widget Haute disponibilité du **Dashboard (Tableau de bord)**, vérifiez que le pare-feu a pris le relais en tant que pare-feu actif et que l'homologue affiche désormais un état passif.

# Configuration de la HD active/passive



## Prérequis pour HA actif/actif

Pour configurer le HA actif/actif sur vos pare-feu, vous avez besoin d'une paire de pare-feu répondant aux exigences suivantes :

- **Modèle identique** : Les pare-feu de la paire doivent être du même modèle matériel.
- **Version PAN-OS identique**: les pare-feu doivent exécuter la même version de PAN-OS et doivent chacun être à jour dans les bases de données d'applications, d'URL et de menaces.
- **Les mêmes fonctions de systèmes virtuels multiples** : Les **Multi Virtual System Capability (fonctions de systèmes virtuels multiples)** doivent être activées ou désactivées sur les deux pare-feu. Lorsqu'elles sont activées, chaque pare-feu doit avoir ses propres licences de systèmes virtuels multiples.
- **Types d'interfaces identiques** : des liaisons HA dédiées ou la combinaison d'un port de gestion à des ports sur bande qui sont définis sur le ***type d'interface*** HA.
  - Les interfaces HD doivent être configurées avec des adresses IP statiques uniquement, et non pas avec des adresses IP obtenues de DHCP (à l'exception de AWS qui peut utiliser les adresses DHCP). Déterminez l'adresse IP de la connexion HA1 (contrôle) entre les homologues HA. L'adresse IP HD1 des homologues doit apparaître sur le même sous-réseau s'ils sont directement connectés ou s'ils sont connectés au même commutateur.

    Pour les pare-feu ne disposant pas de ports HA dédiés, vous pouvez utiliser le port de gestion pour la connexion de contrôle. L'utilisation de ce port fournit une liaison de communication directe entre les plans de gestion sur les deux pare-feu. Toutefois, étant donné que les ports de gestion ne seront pas directement câblés entre les homologues, vérifiez que vous disposez d'un itinéraire qui connecte ces deux interfaces dans votre réseau.
  - Si vous utilisez la Couche 3 comme mode de transport pour la connexion HA2 (données), déterminez l'adresse IP de la liaison HA2. Utilisez la Couche 3 uniquement si la connexion HA2 doit communiquer sur un réseau routé. Le sous-réseau IP des liaisons HA2 ne doit pas chevaucher sur celui des liaisons HA1 ou sur aucun des autres sous-réseaux affectés aux ports de données sur le pare-feu.
  - Chaque pare-feu nécessite une interface dédiée pour la liaison HD3. Les pare-feu PA-7000 Series utilisent le port HSCI pour la HA3. Les pare-feu PA-5200 Series peuvent utiliser le port HSCI pour la HA3, ou vous pouvez configurer les interfaces agrégées sur les ports des plans de données pour la HA3 aux fins de la redondance. Sur les autres plateformes, vous pouvez configurer des interfaces agrégées sur les ports des plans de données en tant que liaison HD3 pour la redondance.
- **Ensemble de licences identiques** : les licences sont uniques pour chaque pare-feu et ne peuvent pas être partagées entre plusieurs pare-feu. Par conséquent, vous devez attribuer des licences identiques aux deux pare-feu. Si ces derniers ne disposent pas d'un ensemble de licences

identiques, ils ne peuvent pas synchroniser les informations de configuration et gérer la parité pour un basculement transparent.

*Si vous disposez déjà d'un pare-feu et que vous souhaitez ajouter un nouveau-pare-feu à des fins de HD et que le nouveau pare-feu a une configuration existante, il est recommandé de procéder au* Rétablissement des paramètres d'usine par défaut du pare-feu *du nouveau pare-feu. Ainsi, le nouveau pare-feu aura une configuration propre. Une fois la HA configurée, vous devez synchroniser la configuration du pare-feu principal avec celle du nouveau pare-feu. Vous devrez également configurer les adresses IP locales.*

## Configuration de la HA active/active

La procédure suivante décrit le flux de travail de base à suivre pour configurer vos pare-feu dans une configuration active/active. Toutefois, avant de commencer, déterminez votre cas pratique actif/actif pour examiner des exemples de configuration qui sont mieux adaptés à votre environnement réseau particulier.

*Si vous disposez d'un commutateur entre vos pare-feu HA, les ports des commutateurs qui connectent la liaison HD3 doivent prendre en charge les trames Jumbo pour gérer la charge associée à l'encapsulation MAC-in-MAC sur la liaison HD3.*

Pour une configuration active/active, vous devez d'abord effectuer les étapes suivantes sur l'un des homologues avant de les appliquer au second homologue tout en vous assurant de définir l'ID du périphérique de chaque homologue sur des valeurs différentes (0 ou 1).

**STEP 1 |** Connectez les ports HA afin de configurer une connexion physique entre les pare-feu.

*Pour chaque cas pratique, il peut s'agir de pare-feu de tout modèle matériel ; sélectionnez l'étape HA3 qui correspond à votre modèle.*

- Pour les pare-feu dotés de ports HA dédiés, utilisez un câble Ethernet pour connecter les ports HA1 dédiés et les ports HA2 sur les homologues. Utilisez un câble croisé si les pare-feu sont directement connectés les uns aux autres.
- Pour les pare-feu ne disposant pas de ports HA dédiés, sélectionnez deux interfaces de données pour la liaison HA2 et la liaison HA1 de secours. Utilisez ensuite un câble Ethernet pour connecter ces interfaces HA sur bande aux deux pare-feu. Utilisez le port de gestion pour la liaison HA1 et vérifiez que les ports de gestion peuvent se connecter les uns aux autres dans votre réseau.
- Pour la HA3 :
  - Sur les pare-feu PA-7000 Series, connectez le High Speed Chassis Interconnect (interconnexion de châssis haute vitesse ; HSCI-A) sur le premier châssis directement à HSCI-A sur le second châssis, et HSCI-B sur le premier châssis à HSCI-B sur le second châssis.
  - Sur des pare-feu PA-5200 Series (qui possèdent un port HSCI), connectez le port HSCI sur le premier châssis au port HSCI sur le second châssis. Vous pouvez également utiliser les ports de données HA3 sur les pare-feu PA-5200 Series.

- Sur des pare-feu PA-3200 Series (qui possèdent un port HSCI), connectez le port HSCI sur le premier châssis au port HSCI sur le second châssis.
- Sur tout autre modèle de matériel, utilisez les interfaces de plan de données pour la HA3.

**STEP 2 |** Activez une requête ping sur le port de gestion.

Son activation permet au port de gestion d'échanger des informations sur la sauvegarde des pulsations.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Management Interface Settings (Paramètres de l'interface de gestion).
2. Sélectionnez **Ping (Ping)** en tant que service autorisé sur l'interface.

**STEP 3 |** Si le pare-feu ne dispose pas de ports HA dédiés, configurez les ports de données pour qu'ils fonctionnent en tant que ports HA.

Pour les pare-feu dotés de ports HA dédiés, passez à l'étape suivante.

1. Sélectionnez **Network (Réseau)** > **Interfaces**.
2. Vérifiez que la liaison est active sur les ports que vous voulez utiliser.
3. Sélectionnez l'interface et définissez l'option **Interface Type (Type d'interface)** sur **HA (HA)**.
4. Définissez les paramètres **Link Speed (Vitesse de liaison)** et **Link Duplex (Duplex de la liaison)**, selon le cas.

**STEP 4 |** Activez la HA active/active et définissez l'ID de groupe.

1. Dans **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, modifiez la configuration.
2. Sélectionnez **Enable HD (Activer la HD)**.
3. Saisissez un **Group ID (ID de groupe)**, qui doit être le même pour les deux pare-feu. Le pare-feu utilise un ID de groupe pour calculer l'adresse MAC virtuelle (la plage est de 1 à 63).
4. (Facultatif) Saisissez une **Description (Description)**.
5. Pour **Mode (Mode)**, sélectionnez **Active Active (Active Active)**.

**STEP 5 |** Définissez l'ID du périphérique, activez la synchronisation et identifiez la liaison de contrôle sur le pare-feu homologue.

1. Dans **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, modifiez la configuration.
2. Sélectionnez **Device ID (ID du périphérique)** comme suit :
   - Lorsque vous configurez le premier homologue, définissez le **Device ID (ID du périphérique)** sur **0**.
   - Lorsque vous configurez le second homologue, définissez le **Device ID (ID du périphérique)** sur **1**.
3. Sélectionnez **Enable Config Sync (Activer la synchronisation de la configuration)**. Ce paramètre est requis pour synchroniser les deux configurations de pare-feu (activé par défaut).
4. Saisissez la **Peer HA1 IP Address (Adresse IP de l'homologue HA1)**, à savoir l'adresse IP de la liaison de contrôle HA1 sur le pare-feu homologue.
5. (Facultatif) Saisissez la valeur pour **Backup Peer HA1 IP Address (Adresse IP de l'homologue HA1 de sauvegarde)**, à savoir l'adresse IP de la liaison de contrôle de sauvegarde du pare-feu de l'homologue.
6. Cliquez sur **OK**.

**STEP 6 |** Déterminez si le pare-feu ayant l'ID de périphérique le plus faible remplace le pare-feu actif principal après une récupération suite à un échec.

1. Dans **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, modifiez la section Election Settings (Paramètres de sélection).
2. Sélectionnez le **Preemptive (Mode préemptif)** pour forcer le pare-feu ayant l'ID de périphérique le plus faible à reprendre automatiquement l'activité active principale après que le pare-feu récupère d'un échec. Le **Preemptive (Mode préemptif)** doit être activé sur les deux pare-feu pour que la préemption se produise.

   Laissez la case **Preemptive (Mode préemptif)** décochée si vous souhaitez que le rôle actif principal reste associé au pare-feu actuel jusqu'à que vous redonniez manuellement ce rôle au pare-feu actif principal ayant récupéré.

**STEP 7 |** Activez la sauvegarde des pulsations si votre liaison de contrôle utilise un port HA dédié ou un port sur bande.

Vous n'avez pas besoin d'activer la sauvegarde des pulsations si vous utilisez le port de gestion pour la liaison de contrôle.

1. Dans **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, modifiez la section Election Settings (Paramètres de sélection).
2. Sélectionnez **Heartbeat Backup (Sauvegarde des pulsations)**.

   Pour permettre la transmission des pulsations entre les pare-feu, vous devez vérifier que le port de gestion des deux homologues peut acheminer les pulsations vers l'un comme vers l'autre.

   *L'activation de la sauvegarde des pulsations vous permet d'empêcher une situation de « split brain ». Un « split brain » se produit lorsque la liaison HA1 s'arrête, le pare-feu manquant ainsi des pulsations, et ce, alors qu'il fonctionne toujours. Dans une telle situation, chaque homologue pense que l'autre est arrêté et tente de démarrer des services déjà exécutés, entraînant ainsi un « split brain ». L'activation de la liaison de sauvegarde des pulsations empêche le « split brain », car des pulsations redondantes et des messages hello sont transmis sur le port de gestion.*

**STEP 8 |** (Facultatif) Modifiez les minuteurs HA.

Par défaut, le profil de minuteur HA est défini sur **Recommended (Recommandé)** et est adapté à la plupart des déploiements HA.

1. Dans **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, modifiez la section Election Settings (Paramètres de sélection).
2. Sélectionnez **Aggressive (Agressif)** pour déclencher le basculement de manière plus rapide. Sélectionnez **Advanced (Avancé)** pour définir des valeurs personnalisées déclenchant le basculement dans votre configuration.

   *Pour afficher la valeur prédéfinie d'un minuteur inclus dans un profil, sélectionnez **Advanced (Avancé)** et cliquez sur **Load Recommended (Charger le profil recommandé)** ou **Load Aggressive (Charger le profil agressif)**. Les valeurs prédéfinies de votre modèle matériel s'affichent alors à l'écran.*

**STEP 9 |** Configurez la connexion de la liaison de contrôle.

Cet exemple utilise un port sur bande défini sur le type d'interface HA.

Pour les pare-feu utilisant le port de gestion en tant que liaison de contrôle, les informations concernant l'adresse IP sont automatiquement prérenseignées.

1. Dans **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, modifiez la section Control Link (HA1) (Liaison de contrôle (HA1)).
2. Sélectionnez le **Port (Port)** que vous avez câblé afin de l'utiliser en tant que liaison HA1.
3. Définissez les options **IPv4/IPv6 Address (Adresse IPv4/IPv6)** et **Netmask (Masque réseau)**.

   Si les interfaces HA1 se trouvent sur des sous-réseaux distincts, saisissez l'adresse IP de la **Gateway (Passerelle)**. N'ajoutez pas d'adresse de passerelle si les pare-feu sont directement connectés.

**STEP 10 |** (Facultatif) Activez le chiffrement de la connexion de la liaison de contrôle.

Il permet généralement de sécuriser la liaison si les deux pare-feu ne sont pas directement connectés, c'est-à-dire lorsque les ports sont connectés à un commutateur ou à un routeur.

1. Exportez la clé HA d'un pare-feu et importez-la sur le pare-feu homologue.
   1. Sélectionnez **Device (Appareil)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**.
   2. Sélectionnez **Export HD key (Exporter la clé HD)**. Enregistrez la clé HA sur un emplacement réseau auquel l'homologue peut accéder.
   3. Sur le pare-feu homologue, sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**, puis **Import HA key (Importer la clé HA)** pour accéder à l'emplacement dans lequel vous avez sauvegardé la clé et l'importer sur l'homologue.
2. Dans **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, modifiez la section Control Link (HA1) (Liaison de contrôle (HA1)).
3. Sélectionnez **Encryption Enabled (Chiffrement activé)**.

   *Si vous activez le chiffrement, une fois que vous avez fini de configurer les pare-feu HA, vous pouvez* Actualisation des clés SSH HA1 et configuration des options des clés.

**STEP 11 |** Configurez la connexion de la liaison de contrôle de secours.

1. Dans **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, modifiez la section Control Link (HA1 Backup) (Liaison de contrôle (HA1 de secours)).
2. Sélectionnez l'interface HA1 de secours, puis définissez les options **IPv4/IPv6 Address (Adresse IPv4/IPv6)** et **Netmask (Masque réseau)**.

   *Les pare-feu PA-3200 Series ne prennent pas en charge l'adresse IPv6 pour la liaison de contrôle HA1 de secours ; utilisez une adresse IPv4.*

**STEP 12 |** Configurez la connexion de la liaison de données (HA2) et la connexion HA2 de secours entre les pare-feu.

1. Dans **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, modifiez la Liaison de données (HA2).
2. Sélectionnez le **Port (Port)** à utiliser pour la connexion de la liaison de données.
3. Sélectionnez la méthode de **Transport (Transport)**. La valeur par défaut est **ethernet (ethernet)** et sera utilisée lorsque la paire HD sera connectée directement ou via un commutateur. Si vous devez acheminer le trafic de la liaison de données via le réseau, sélectionnez **IP (IP)** ou **UDP (UDP)** comme mode de transport.
4. Si vous utilisez IP ou UDP comme mode de transport, définissez les options **IPv4/IPv6 Address (Adresse IPv4/IPv6)** et **Netmask (Masque réseau)**.
5. Vérifiez que l'option **Enable Session Synchronization (Activer la synchronisation de la session)** est sélectionnée.
6. Sélectionnez **HA2 Keep-alive (Persistance HA2)** pour activer la surveillance sur la liaison de données HD2 entre les homologues HD. Si un échec se produit en fonction du seuil défini (la valeur par défaut étant 10 000 ms), l'action définie va s'exécuter. en cas d'échec de la persistance HA2, le système génère un message critique du journal système ou entraîne un plan de données divisé, selon votre configuration.

   *Vous pouvez configurer l'option Persistance HA2 sur les deux pare-feu ou sur un seul pare-feu de la paire HA. Si l'option n'est activée que sur un seul pare-feu, il est le seul à envoyer des messages de persistance. L'autre pare-feu est informé en cas d'échec.*

   *Un plan de données divisé entraîne les plans de données des deux homologues à fonctionner indépendamment tout en laissant l'état de haute disponibilité en tant qu'actif-principal et actif-secondaire. Si un seul pare-feu est configuré pour diviser le plan de données, le plan de données divisé s'applique alors à l'autre périphérique également.*
7. Modifiez la section **Data Link (HA2 Backup) (Liaison de données (HA2 de secours))**, sélectionnez l'interface, puis définissez les options **IPv4/IPv6 Address (Adresse IPv4/IPv6)** et **Netmask (Masque réseau)**.
8. Cliquez sur **OK**.

**STEP 13 |** Configurez la liaison HA3 pour le transfert de paquets.

1. Dans **Device (Équipement)** > **High Availability (Haute disponibilité)** > **Active/Active Config (Configuration active/active)**, modifiez la section Packet Forwarding (Transfert des paquets).
2. Sous **HA3 Interface (Interface HA3)**, sélectionnez l'interface que vous souhaitez utiliser pour transférer des paquets entre les homologues HA actifs/actifs. Il doit s'agir d'une interface dédiée capable de prendre en charge le transport de Couche 2 et définie sur **Interface Type HA (Type d'interface HA)**.
3. Sélectionnez **VR Sync (Synchronisation du routeur virtuel)** pour forcer la synchronisation de tous les routeurs virtuels configurés sur les homologues HA. Sélectionnez cette option lorsque le routeur virtuel n'est pas configuré pour fonctionner avec des protocoles de routage dynamique. Les deux homologues doivent être connectés au même routeur de saut suivant via un réseau commuté et utiliser uniquement un routage statique.

4. Sélectionnez **QoS Sync (Synchronisation de la QoS)** pour synchroniser la sélection du profil QoS sur toutes les interfaces physiques. Sélectionnez cette option lorsque les deux homologues disposent de vitesses de liaison similaires et que les mêmes profils QoS sont requis sur toutes les interfaces physiques. Ce paramètre s'applique à la synchronisation des paramètres de QoS de l'onglet **Network (Réseau)**. La politique de QoS est synchronisée, quel que soit ce paramètre.

**STEP 14 |** (Facultatif) Modifiez le temps d'attente provisoire.

1. Dans **Device (Équipement)** > **High Availability (Haute disponibilité)** > **Active/Active Config (Configuration active/active)**, modifiez la section Packet Forwarding (Transfert des paquets).
2. Sous **Tentative Hold Time (sec) (Temps d'attente provisoire (s))**, saisissez le nombre de secondes pendant lesquelles un pare-feu reste à l'état provisoire après qu'il récupère après un échec (plage de 10 à 600 ; la valeur par défaut est 60).

**STEP 15 |** Configurez le propriétaire de la session et la configuration de la session.

1. Dans **Device (Équipement)** > **High Availability (Haute disponibilité)** > **Active/Active Config (Configuration active/active)**, modifiez la section Packet Forwarding (Transfert des paquets).
2. Sous **Session Owner Selection (Sélection du propriétaire de la session)**, sélectionnez l'une des options suivantes :
   - **First Packet (Premier paquet)** : le pare-feu qui reçoit le premier paquet d'une nouvelle session est le propriétaire de la session (paramètre recommandé). Ce paramètre minimise le trafic sur la HD3 et équilibre la charge du trafic entre les homologues.
   - **Primary Device (Périphérique principal)** : le pare-feu à l'état actif/principal est le propriétaire de la session.
3. Sous **Session Setup (Paramétrage de la session)**, sélectionnez l'une des options suivantes :
   - **IP Modulo (Modulo IP)** : le pare-feu effectue une opération XOR sur les adresses IP source et de destination à partir du paquet et selon le résultat, le pare-feu choisit l'homologue HA qui configure la session.
   - **Primary Device (Périphérique principal)** : le pare-feu actif principal configure toutes les sessions.
   - **First Packet (Premier paquet)** : le pare-feu qui reçoit le premier paquet d'une nouvelle session configure la session (paramètre recommandé).

     *Commencez avec le premier paquet pour le propriétaire de session, puis, selon la distribution de la charge, vous pouvez passer à l'une des autres options.*
   - **IP Hash (Hachage IP)** : le pare-feu utilise un hachage de l'adresse IP source ou une combinaison des adresses IP source et de destination pour transférer les responsabilités de paramétrage de la session.
4. Cliquez sur **OK**.

**STEP 16 |** Configurez une adresse virtuelle HA.

Vous avez besoin d'une adresse virtuelle pour utiliser une Adresse IP flottante et adresse MAC virtuelle ou le partage de charge ARP.

1. Sous **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **Active/Active Config (Configuration active/active)**, **Add (Ajoutez)** une adresse virtuelle.
2. Saisissez ou sélectionnez une **Interface (Interface)**.
3. Sélectionnez l'onglet **IPv4 (IPv4)** ou l'onglet **IPv6 (IPv6)**, puis cliquez sur **Add (Ajouter)**.
4. Saisissez une **IPv4 Address (Adresse IPv4)** ou **IPv6 Address (Adresse IPv6)**.
5. Sous **Type (Type)** :
   - Sélectionnez **Floating (Flottante)** pour configurer l'adresse IP virtuelle en tant qu'adresse IP flottante.
   - Sélectionnez **ARP Load Sharing (Partage de charge ARP)** pour configurer l'adresse IP virtuelle en tant qu'adresse IP partagée et passez à l'étape Configuration du partage de charge ARP.

**STEP 17 |** Configurez l'adresse IP flottante.

1. Évitez de sélectionner l'option **Floating IP bound to the Active-Primary device (IP flottante liée au périphérique principal actif)**, sauf si vous souhaitez que la paire HD active/active se comporte comme une paire HD active/passive.
2. Pour **Device 0 Priority (Priorité de l'appareil 0)** et **Device 1 Priority (Priorité de l'appareil 1)**, saisissez une priorité pour le pare-feu configuré avec l'ID d'appareil 0 et l'ID d'appareil 1, respectivement. Les priorités relatives déterminent l'homologue possédant l'adresse IP flottante que vous venez de configurer (plage de 0-255). Le pare-feu avec la valeur de priorité la plus basse (priorité la plus élevée) possède l'adresse IP flottante.
3. Sélectionnez **Failover address if link state is down (Adresse de basculement si l'état des liaisons est inactif)** pour que le pare-feu utilise l'adresse de basculement lorsque l'état de la liaison sur l'interface est Inactif.
4. Cliquez sur **OK**.

**STEP 18 |** Configurez le Partage de charge ARP.

L'algorithme de sélection d'appareil détermine le pare-feu HA qui répond aux requêtes ARP pour fournir le partage de charge.

1. Sous **Device Selection Algorithm (Algorithme de sélection des périphériques)**, sélectionnez l'une des options suivantes :
   - **IP Modulo (Modulo IP)** : le pare-feu qui répondra aux requêtes ARP dépend de la parité de l'adresse IP du demandeur ARP.
   - **IP Hash (Hachage IP)** : le pare-feu qui répondra aux requêtes ARP dépend d'un hachage de l'adresse IP du demandeur ARP.
2. Cliquez sur **OK**.

**STEP 19 |** Définition des conditions de basculement HA.

**STEP 20 |** **Commit (Validez)** la configuration.

# Déterminer votre cas pratique actif/actif

Déterminez votre type de cas pratique, puis sélectionnez la procédure correspondante pour configurer la HD active/active.

Si vous utilisez la Redondance de routage, l'Adresse IP flottante et adresse MAC virtuelle ou le Partage de charge ARP, sélectionnez la procédure correspondante :

- Cas d'utilisation : Configuration de la HA active/active avec redondance de routage
- Cas d'utilisation : Configuration de la HA active/active avec des adresses IP flottantes
- Cas d'utilisation : Configuration de la HA active/active avec le partage de charge ARP

Si vous voulez un déploiement HD active/active de Couche 3 qui se comporte comme un déploiement actif/passif, sélectionnez la procédure suivante :

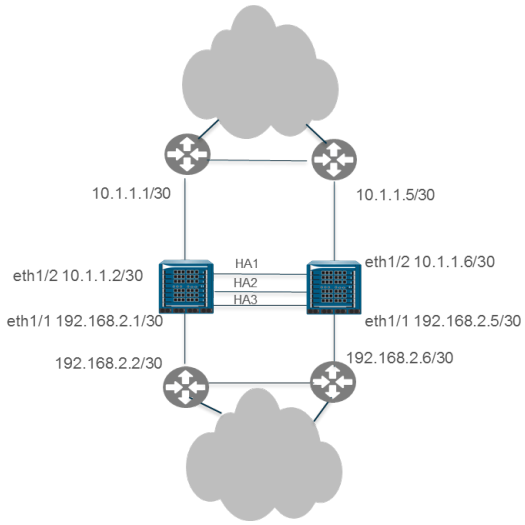
- Cas d'utilisation : Configuration de la HA active/active avec des adresses IP flottantes liées a un pare-feu actif principal

Si vous configurez NAT en mode HA active/active, reportez-vous aux procédures suivantes :

- Cas d'utilisation : Configuration de la HA active/active avec la NAT DIPP source à l'aide d'adresses IP flottantes
- Cas d'utilisation : Configuration de pools d'adresses IP NAT source séparés pour des pare-feu HA actifs/actifs
- Cas d'utilisation : Configuration de la HA active/active avec le partage de charge ARP avec la NAT de destination
- Cas d'utilisation : Configuration de la HA active/active avec le partage de charge ARP avec la NAT de destination dans la Couche 3

## Cas d'utilisation : Configuration de la HA active/active avec redondance de routage

La topologie de Couche 3 suivante illustre deux pare-feu PA-7050 dans un environnement HA actif/actif qui utilise la Route-Based Redundancy (Redondance basée sur le routage). Les pare-feu appartiennent à une zone OSPF. Lorsqu'un pare-feu ou une liaison échoue, OSPF gère la redondance en redirigeant le trafic vers le pare-feu fonctionnel.



**STEP 1 |** Configuration de la HA active/active.

Effectuez les étapes 1 à 15.

**STEP 2 |** Configurez OSPF.

Consultez OSPF.

**STEP 3 |** Définissez les conditions de basculement HA.

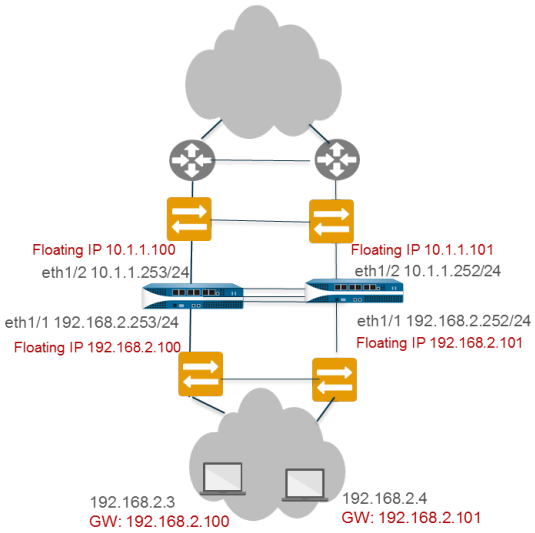
Définition des conditions de basculement HA.

**STEP 4 |** **Commit (Validez)** la configuration.

**STEP 5 |** Configurez le pare-feu homologue de la même façon à l'exception de l'étape 5 : si vous avez sélectionné l'ID de périphérique **0** pour le premier pare-feu, sélectionnez l'ID de périphérique **1** pour le pare-feu homologue.

## Cas d'utilisation : Configuration de la HA active/active avec des adresses IP flottantes

Dans cet exemple d'interface de Couche 3, les pare-feu HA se connectent à des commutateurs et utilisent des adresses IP flottantes pour gérer les échecs de liaison ou de pare-feu. Les hôtes terminaux sont configurés chacun avec une passerelle, qui est l'adresse IP flottante d'un des pare-feu HA. Consultez Adresse IP flottante et adresse MAC virtuelle.




**STEP 1 |** Configuration de la HA active/active.

Effectuez les étapes 1 à 15.

**STEP 2 |** Configurez une adresse virtuelle HA.

Vous aurez besoin d'une adresse virtuelle pour utiliser une Adresse IP flottante et une adresse MAC virtuelle.

1. Sous **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **Active/Active Config (Configuration active/active)**, **Add (Ajoutez)** une adresse virtuelle.
2. Saisissez ou sélectionnez une **Interface (Interface)**.
3. Sélectionnez l'onglet **IPv4 (IPv4)** ou l'onglet **IPv6 (IPv6)**, puis cliquez sur **Add (Ajouter)**.
4. Saisissez une **IPv4 Address (Adresse IPv4)** ou **IPv6 Address (Adresse IPv6)**.
5. Pour le **Type (Type)**, sélectionnez **Floating (Flottante)** pour configurer l'adresse IP virtuelle comme une adresse IP flottante.

**STEP 3 |** Configurez l'adresse IP flottante.

1. Ne sélectionnez pas **Floating IP bound to the Active-Primary device (IP flottante liée à l'appareil principal actif)**.
2. Pour **Device 0 Priority (Priorité de l'appareil 0)** et **Device 1 Priority (Priorité de l'appareil 1)**, saisissez une priorité pour le pare-feu configuré avec l'ID d'appareil 0 et l'ID d'appareil 1, respectivement. Les priorités relatives déterminent l'homologue possédant l'adresse IP flottante que vous venez de configurer (plage de 0 à 255). Le pare-feu avec la valeur de priorité la plus basse (priorité la plus élevée) possède l'adresse IP flottante.
3. Sélectionnez **Failover address if link state is down (Adresse de basculement si l'état des liaisons est inactif)** pour que le pare-feu utilise l'adresse de basculement lorsque l'état de la liaison sur l'interface est Inactif.
4. Cliquez sur **OK**.

**STEP 4 |** Activez les trames jumbo et pare-feu autres que les pare-feu PA-7000 Series.

Effectuez l'étape 19 de Configure Active/Active HA (Configuration de la HA active/active).

**STEP 5 |** Définition des conditions de basculement HA

**STEP 6 |** **Commit (Validez)** la configuration.

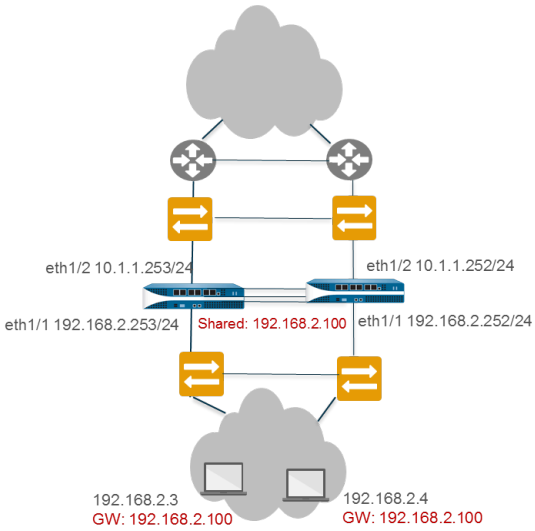
**STEP 7 |** Configurez le pare-feu homologue de la même façon, à l'exception du choix d'un ID d'appareil différent.

Par exemple, si vous avez sélectionné l'ID d'appareil **0** pour le premier pare-feu, sélectionnez **1** pour le pare-feu homologue.

## Cas d'utilisation : Configuration de la HA active/active avec le partage de charge ARP

Dans cet exemple, les hôtes d'un déploiement de Couche 3 ont besoin des services de passerelle des pare-feu HA. Les pare-feu sont configurés avec une seule adresse IP partagée qui autorise le Partage de charge ARP. Les hôtes terminaux sont configurés avec la même passerelle, qui est l'adresse IP partagée des pare-feu HA.




**STEP 1 |** Effectuez les étapes 1 à 15 de Configure Active/Active HA (Configuration de la HA active/active).

**STEP 2 |** Configurez une adresse virtuelle HA.

L'adresse virtuelle est l'adresse IP partagée qui permet le Partage de charge ARP.

1. Sélectionnez **Device (Équipement)** > **High Availability (Haute disponibilité)** > **Active/Active Config (Configuration active/active)** > **Virtual Address (Adresse virtuelle)**, puis cliquez sur **Add (Ajouter)**.
2. Saisissez ou sélectionnez une **Interface (Interface)**.
3. Sélectionnez l'onglet **IPv4 (IPv4)** ou l'onglet **IPv6 (IPv6)**, puis cliquez sur **Add (Ajouter)**.
4. Saisissez une **IPv4 Address (Adresse IPv4)** ou **IPv6 Address (Adresse IPv6)**.
5. Pour **Type (Type)**, sélectionnez **ARP Load Sharing (Partage de charge ARP)**, qui permet aux deux homologues d'utiliser l'adresse IP virtuelle pour le Partage de charge ARP.

**STEP 3 |** Configurez le Partage de charge ARP.

L'algorithme de sélection d'appareil détermine le pare-feu HA qui répond aux requêtes ARP pour fournir le partage de charge.

1. Sous **Device Selection Algorithm (Algorithme de sélection des périphériques)**, sélectionnez l'une des options suivantes :
   - **IP Modulo (Modulo IP)** : le pare-feu qui répondra aux requêtes ARP dépend de la parité de l'adresse IP du demandeur ARP.
   - **IP Hash (Hachage IP)** : le pare-feu qui répondra aux requêtes ARP dépend d'un hachage de l'adresse IP du demandeur ARP.
2. Cliquez sur **OK**.

**STEP 4 |** Activez les trames jumbo et pare-feu autres que les pare-feu PA-7000 Series.

**STEP 5 |** Définition des conditions de basculement HA

**STEP 6 |** **Commit (Validez)** la configuration.

**STEP 7 |** Configurez le pare-feu homologue de la même façon, à l'exception du choix d'un ID d'appareil différent.

Par exemple, si vous avez sélectionné l'ID d'appareil **0** pour le premier pare-feu, sélectionnez **1** pour le pare-feu homologue.

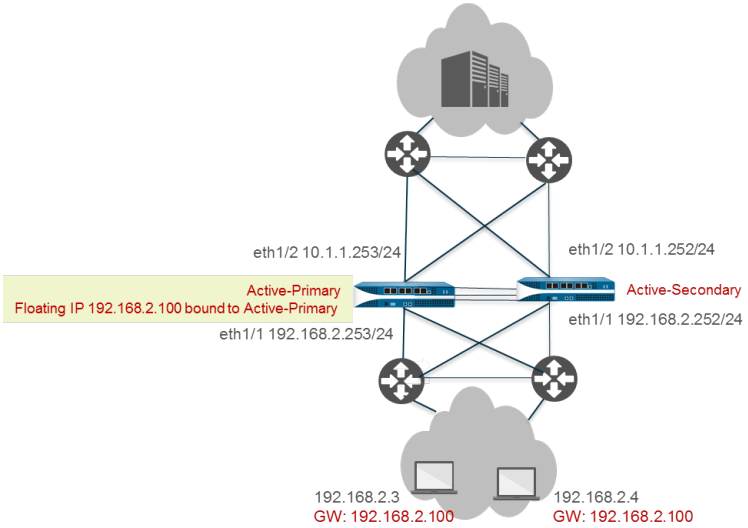
## Cas d'utilisation : Configuration de la HA active/active avec des adresses IP flottantes liées a un pare-feu actif principal

Dans les centres de données stratégiques, vous souhaiterez peut-être que les deux pare-feu HA de Couche 3 participent à la surveillance des chemins pour qu'ils puissent détecter les pannes de chemin en amont. Par ailleurs, vous préférerez contrôler si et quand l'adresse IP flottante revient au pare-feu récupéré une fois ce dernier rétabli, plutôt que faire revenir l'adresse IP flottante à l'ID d'appareil auquel elle est liée. (Ce comportement par défaut est décrit dans Adresse IP flottante et adresse MAC virtuelle.)

Dans ce cas d'usage, vous contrôlez le moment auquel l'adresse IP flottante et donc le rôle actif-principal reviennent à un homologue HA récupéré. Les pare-feu HA actif/actif partagent une adresse IP flottante unique que vous liez au pare-feu qui se trouve en état actif-principal. Avec une seule adresse IP flottante, le trafic réseau circule principalement vers un seul pare-feu. Ainsi, ce déploiement actif/actif fonctionne comme un déploiement actif/passif.

Dans ce cas pratique, les commutateurs Cisco Nexus 7010 avec PortChannel virtuels (vPC) fonctionnant en Couche 3 se connectent aux pare-feu. Vous devez configurer les commutateurs de Couche 3 (routeurs homologues) au nord et au sud des pare-feu avec une préférence d'itinéraire pour l'adresse IP flottante. En d'autres termes, vous devez concevoir votre réseau pour que les tables d'itinéraire des routeurs homologues aient le meilleur chemin d'accès à l'adresse IP flottante. Cet exemple utilise les itinéraires statiques avec les bonnes mesures pour que l'itinéraire vers l'adresse IP flottante utilise une mesure plus basse (l'itinéraire vers l'adresse IP flottante est préférable) et reçoit le trafic. Une solution alternative à l'utilisation d'itinéraires statiques consiste à concevoir le réseau pour redistribuer l'adresse IP flottante dans le protocole de routage OSPF (si vous utilisez OSPF).

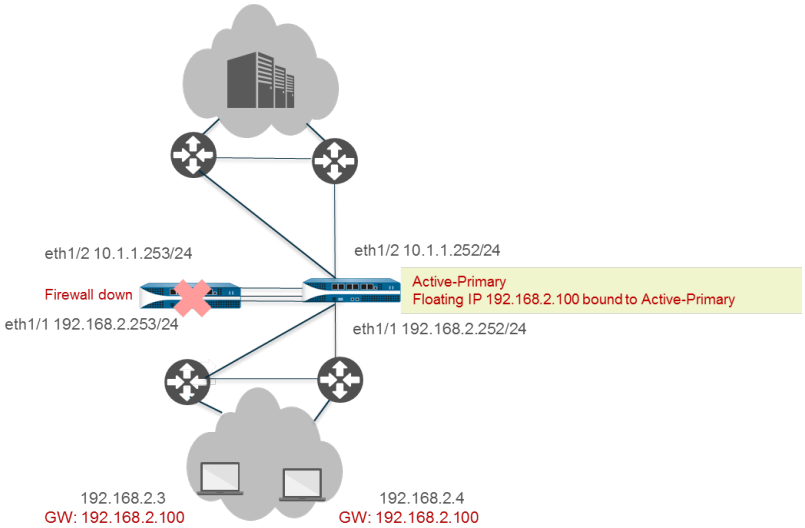
La topologie suivante illustre l'adresse IP flottante liée au pare-feu actif-principal, qui est initialement l'homologue A, le pare-feu sur la gauche.




Lors d'un basculement, lorsque le pare-feu actif-principal (homologue A) est inaccessible et que le pare-feu actif-secondaire (homologue B) prend le rôle de l'homologue actif-principal, l'adresse IP

flottante passe à l'homologue B (comme illustré ci-après). L'homologue B reste le pare-feu actif-principal et le trafic continue à aller à l'homologue B, même quand l'homologue A récupère et devient par la même occasion le pare-feu actif-secondaire. Vous déterminez si et quand l'homologue A devient à nouveau le pare-feu actif-principal.




Lier l'adresse IP flottante au pare-feu actif-principal vous offre plus de contrôle sur la façon dont les pare-feu déterminent la propriété de l'adresse IP flottante lorsque les États de pare-feu HA changent. Les avantages suivants en résultent :

- Vous pouvez avoir une configuration HA active/active pour la surveillance de chemin avec les deux pare-feu, tout en faisant fonctionner les pare-feu comme une configuration HA active/passive, car le trafic dirigé vers l'adresse IP flottante va toujours vers le pare-feu actif-principal.

Lorsque vous désactivez la préemption sur les deux pare-feu, vous avez les avantages supplémentaires suivants :

- L'adresse IP flottante ne se déplace pas constamment entre les pare-feu HA si le pare-feu actif-secondaire change.
- Vous pouvez vérifier la fonctionnalité du pare-feu récupéré et des composants adjacents avant de manuellement acheminer à nouveau le trafic vers ce pare-feu, ce que vous pouvez faire lors d'un temps d'arrêt qui vous convient.
- Vous avez le contrôle sur le pare-feu propriétaire de l'adresse IP flottante. Ainsi, vous gardez tous les flux de sessions nouvelles et existantes sur le pare-feu actif-principal, en minimisant le trafic sur la liaison HA3.

- *Nous vous recommandons fortement de configurer la surveillance de liaison HA sur les interfaces qui prennent en charge les adresses IP flottantes pour permettre à chaque homologue HA de détecter rapidement une défaillance et de basculer sur son homologue. Les deux homologues HA doivent avoir la surveillance de liaison pour que cela fonctionne.*
- *Nous vous recommandons fortement de configurer la surveillance de chemin HA pour informer chaque homologue HA lorsqu'un chemin échoue, pour qu'un pare-feu puisse basculer sur son homologue. L'adresse IP flottante étant toujours liée au pare-feu actif-principal, le pare-feu ne peut pas automatiquement basculer vers l'homologue lorsqu'un chemin devient inaccessible et que la surveillance de chemin n'est pas activée.*

*Vous ne pouvez pas configurer NAT pour une adresse IP flottante qui est liée à un pare-feu actif-principal.*

**STEP 1 |** Effectuez les étapes 1 à 5 de Configure Active/Active HA (Configuration de la HA active/active).

**STEP 2 |** (Facultatif) Désactivez la préemption.

*Désactiver la préemption vous permet d'avoir le contrôle intégral sur le moment auquel le pare-feu récupéré devient le pare-feu actif-principal.*

1. Dans **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, modifiez la section Election Settings (Paramètres de sélection).
2. Décochez **Preemptive (Préemptif)** si l'option est activée.
3. Cliquez sur **OK**.

**STEP 3 |** Effectuez les étapes 7 à 14 de Configure Active/Active HA (Configuration de la HA active/active).

**STEP 4 |** Configurez le propriétaire de la session et la configuration de la session.

1. Dans **Device (Équipement)** > **High Availability (Haute disponibilité)** > **Active/Active Config (Configuration active/active)**, modifiez la section Packet Forwarding (Transfert des paquets).
2. Pour **Session Owner Selection (Sélection du propriétaire de la session)**, nous vous recommandons de sélectionner **Primary Device (Appareil principal)**. Le pare-feu en état actif-principal est le propriétaire de la session.

   Sinon, pour **Session Owner Selection (Sélection du propriétaire de la session)** vous pouvez sélectionner **First Packet (Premier paquet)**, puis, pour **Session Setup (Configuration de la session)**, sélectionner **Primary Device (Appareil principal)** ou **First Packet (Premier paquet)**.
3. Sous **Session Setup (Paramétrage de la session)**, sélectionnez **Primary Device (Périphérique principal)** : le pare-feu actif principal configure toutes les sessions. Il s'agit du paramètre recommandé si vous souhaitez que votre configuration active/active fonctionne comme une configuration active/passive, car elle garde toutes les activités sur le pare-feu actif-principal.

   *Vous devez également concevoir votre réseau de façon à éliminer le risque de trafic asymétrique dirigé vers la paire HA. Si vous ne le faites pas et que du trafic arrive sur le pare-feu actif-secondaire, régler **Session Owner Selection (Sélection du propriétaire de la session)** et **Session Setup (Configuration de la session)** sur **Primary Device (Appareil principal)** oblige le trafic à traverser HA3 pour accéder au pare-feu actif-principal pour la propriété de session et la configuration de la session.*
4. Cliquez sur **OK**.

**STEP 5 |** Configurez une adresse virtuelle HA.

1. Sélectionnez **Device (Équipement)** > **High Availability (Haute disponibilité)** > **Active/Active Config (Configuration active/active)** > **Virtual Address (Adresse virtuelle)**, puis cliquez sur **Add (Ajouter)**.
2. Saisissez ou sélectionnez une **Interface (Interface)**.
3. Sélectionnez l'onglet **IPv4 (IPv4)** ou **IPv6 (IPv6)** et **Add (Ajoutez)** une **IPv4 Address (Adresse IPv4)** ou une **IPv6 Address (Adresse IPv6)**.
4. Pour le **Type (Type)**, sélectionnez **Floating (Flottante)**, ce qui configure l'adresse IP virtuelle comme une adresse IP flottante.
5. Cliquez sur **OK**.

**STEP 6 |** Liez l'adresse IP flottante au pare-feu actif-principal.

1. Sélectionnez **Floating IP bound to the Active-Primary device (IP flottante liée à l'appareil actif-principal)**.
2. Sélectionnez **Failover address if link state is down (Adresse de basculement si l'état des liaisons est inactif)** pour que le pare-feu utilise l'adresse de basculement lorsque l'état de la liaison sur l'interface est Inactif.
3. Cliquez sur **OK**.

**STEP 7 |** Activez les trames jumbo et pare-feu autres que les pare-feu PA-7000 Series.

**STEP 8 |** **Commit (Validez)** la configuration.

**STEP 9 |** Configurez le pare-feu homologue de la même façon, à l'exception du choix d'un ID d'appareil différent.

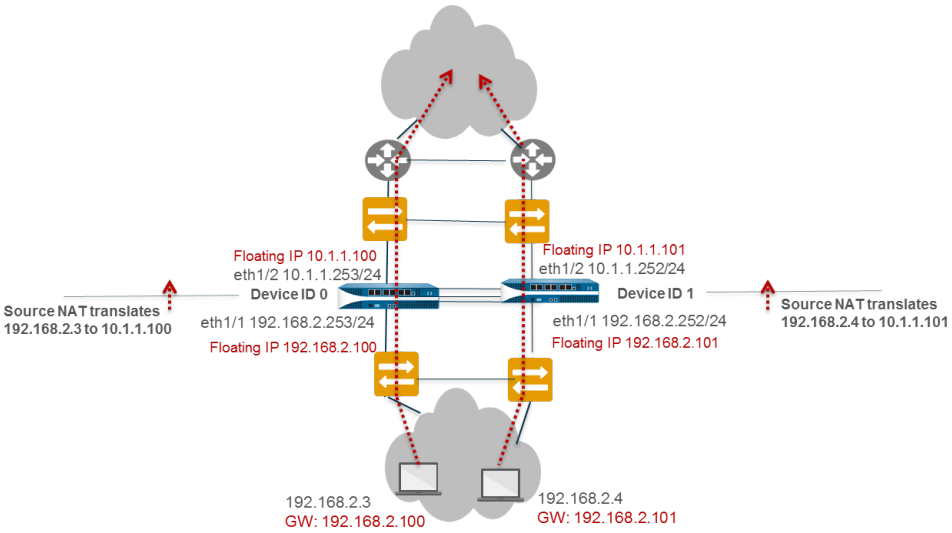
Par exemple, si vous avez sélectionné l'ID d'appareil **0** pour le premier pare-feu, sélectionnez **1** pour le pare-feu homologue.

## Cas d'utilisation : Configuration de la HA active/active avec la NAT DIPP source à l'aide d'adresses IP flottantes

L'interface de Couche 3 utilise la NAT source en mode HA actif/actif. Les commutateurs de Couche 2 créent des domaines de diffusion pour permettre aux utilisateurs d'accéder à tout ce qui se trouve au nord et au sud des pare-feu.

PA-3050-1 a l'ID d'appareil 0 et son homologue HA, PA-3050-2, l'ID d'appareil 1. Dans ce cas pratique, NAT traduit l'adresse IP source et le numéro de port sur l'adresse IP flottante configurée sur l'interface de sortie. Chaque hôte est configuré avec une adresse de passerelle par défaut, qui est l'adresse IP flottante sur Ethernet1/1 sur chaque pare-feu. Cette configuration nécessite deux règles NAT source, une liée à chaque ID d'appareil, bien que vous configurez les deux règles NAT sur un seul pare-feu et qu'elles sont synchronisées sur le pare-feu homologue.




**STEP 1 |** Sur PA-3050-2 (ID de périphérique 1), effectuez les étapes 1 à 3 de Configure Active/Active HA (Configuration de la HA active/active).

**STEP 2 |** Activez la HA active/active.

1. Dans **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, modifiez la configuration.
2. Sélectionnez **Enable HD (Activer la HD)**.
3. Saisissez un **Group ID (ID de groupe)**, qui doit être le même pour les deux pare-feu. Le pare-feu utilise un ID de groupe pour calculer l'adresse MAC virtuelle (la plage est de 1 à 63).
4. Pour **Mode (Mode)**, sélectionnez **Active Active (Active Active)**.
5. Définissez le **Device ID (ID d'appareil)** sur **1**.
6. Sélectionnez **Enable Config Sync (Activer la synchronisation de la configuration)**. Ce paramètre est requis pour synchroniser les deux configurations de pare-feu (activé par défaut).
7. Saisissez la **Peer HA1 IP Address (Adresse IP de l'homologue HA1)**, à savoir l'adresse IP de la liaison de contrôle HA1 sur le pare-feu homologue.
8. (Facultatif) Saisissez la valeur pour **Backup Peer HA1 IP Address (Adresse IP de l'homologue HA1 de sauvegarde)**, à savoir l'adresse IP de la liaison de contrôle de sauvegarde du pare-feu de l'homologue.
9. Cliquez sur **OK**.

**STEP 3 |** Configuration de la HA active/active.

Effectuez les étapes 6 à 14.

**STEP 4 |** Configurez le propriétaire de la session et la configuration de la session.

1. Dans **Device (Équipement)** > **High Availability (Haute disponibilité)** > **Active/Active Config (Configuration active/active)**, modifiez la section Packet Forwarding (Transfert des paquets).
2. Pour **Session Owner Selection (Sélection du propriétaire de la session)**, sélectionnez **First Packet (Premier paquet)** : le pare-feu qui reçoit le premier paquet d'une nouvelle session devient le propriétaire de la session.
3. Pour **Session Setup (Configuration de la session)**, sélectionnez **IP Modulo (Modulo IP)** : Cela distribue la charge de configuration de la session en fonction de la parité de l'adresse IP source.
4. Cliquez sur **OK**.

**STEP 5 |** Configurez une adresse virtuelle HA.

1. Sélectionnez **Device (périphérique)** > **High Availability (Haute disponibilité)** > **Active/Active Config (Configuration active/active)** > **Virtual Address (Adresse virtuelle)**, puis cliquez sur **Add (Ajouter)**.
2. Sélectionnez l'**Interface (Interface)** eth1/1.
3. Sélectionnez **IPv4 (IPv4)** et **Add (Ajoutez)** une **IPv4 Address (adresse IPv4)** de 10.1.1.101.
4. Pour le **Type (Type)**, sélectionnez **Floating (Flottante)**, ce qui configure l'adresse IP virtuelle comme une adresse IP flottante.

**STEP 6 |** Configurez l'adresse IP flottante.

1. Ne sélectionnez pas **Floating IP bound to the Active-Primary device (IP flottante liée à l'appareil principal actif)**.
2. Sélectionnez **Failover address if link state is down (Adresse de basculement si l'état des liaisons est inactif)** pour que le pare-feu utilise l'adresse de basculement lorsque l'état de la liaison sur l'interface est Inactif.
3. Cliquez sur **OK**.

**STEP 7 |** Enable jumbo frames on firewalls other than the PA-7000 Series. (Activez les trames jumbo et pare-feu autres que les pare-feux PA-7000 Series.)

**STEP 8 |** Définition des conditions de basculement HA.

**STEP 9 |** **Commit (Validez)** la configuration.

**STEP 10 |** Configurez le pare-feu homologue, PA-3050-1 avec les mêmes paramètres, en dehors des modifications suivantes :

- Sélectionnez **Device ID 0 (ID d'appareil 0)**.
- Configurez une adresse virtuelle HA, 10.1.1.100.
- Pour **Device 1 Priority (Priorité de l'appareil 1)**, saisissez 255. Pour **Device 0 Priority (Priorité de l'appareil 0)**, saisissez 0.

Dans cet exemple, l'ID d'appareil 0 a une valeur de priorité plus faible, et donc une priorité plus élevée. Ainsi, le pare-feu avec l'ID d'appareil 0 (PA-3050-1) est propriétaire de l'adresse IP flottante 10.1.1.100.

**STEP 11 |** Toujours sur le PA-3050-1, créez la règle NAT source pour l'ID d'appareil 0.

1. Sélectionnez **Policies (Politiques)** > **NAT (NAT)**, puis cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name (Nom)** pour la règle qui, dans cet exemple, l'identifie comme la règle NAT source pour l'ID d'appareil 0.
3. Pour **NAT Type (Type de NAT)**, sélectionnez **ipv4** (paramètre par défaut).
4. Sur **Original Packet (Paquet d'origine)**, dans **Source Zone (Zone source)**, sélectionnez **Any (N'importe laquelle)**.
5. Pour **Destination Zone (Zone de destination)**, sélectionnez la zone que vous avez créée pour le réseau externe.
6. Laissez **Destination Interface (Interface de destination)**, **Service (Service)**, **Source Address (Adresse source)** et **Destination Address (Adresse de destination)** sur **Any (Tout)**.
7. Pour **Translated Packet (Paquet traduit)**, sélectionnez **Dynamic IP And Port (IP et port dynamiques)** pour **Translation Type (Type de traduction)**.
8. Pour **Address Type (Type d'adresse)**, sélectionnez **Interface Address (Adresse de l'interface)**, auquel cas l'adresse traduite sera l'adresse IP de l'interface. Sélectionnez une **Interface (Interface)** (eth1/1 dans cet exemple) et une **IP Address (Adresse IP)** de l'adresse IP flottante 10.1.1.100.
9. Dans l'onglet **Active/Active HA Binding (Liaison HA Active/Active)**, pour **Active/Active HA Binding (Liaison HA Active/Active)** sélectionnez **0** pour lier la règle NAT à l'ID d'appareil 0.
10. Cliquez sur **OK**.

**STEP 12 |** Créez la règle NAT source pour l'ID d'appareil 1.

1. Sélectionnez **Policies (Politiques)** > **NAT (NAT)**, puis cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name (Nom)** pour la règle de politique qui, dans cet exemple, contribue à l'identifier comme la règle NAT source pour l'ID d'appareil 1.
3. Pour **NAT Type (Type de NAT)**, sélectionnez **ipv4** (paramètre par défaut).
4. Sur **Original Packet (Paquet d'origine)**, dans **Source Zone (Zone source)**, sélectionnez **Any (N'importe laquelle)**. Pour **Destination Zone (Zone de destination)**, sélectionnez la zone que vous avez créée pour le réseau externe.
5. Laissez **Destination Interface (Interface de destination)**, **Service (Service)**, **Source Address (Adresse source)** et **Destination Address (Adresse de destination)** sur **Any (Tout)**.
6. Pour **Translated Packet (Paquet traduit)**, sélectionnez **Dynamic IP And Port (IP et port dynamiques)** pour **Translation Type (Type de traduction)**.
7. Pour **Address Type (Type d'adresse)**, sélectionnez **Interface Address (Adresse de l'interface)**, auquel cas l'adresse traduite sera l'adresse IP de l'interface. Sélectionnez une **Interface** (eth1/1 dans cet exemple) et une **IP Address (Adresse IP)** de l'adresse IP flottante 10.1.1.101.
8. Dans l'onglet **Active/Active HA Binding (Liaison HA Active/Active)**, pour **Active/Active HA Binding (Liaison HA Active/Active)** sélectionnez **1** pour lier la règle NAT à l'ID d'appareil 1.
9. Cliquez sur **OK**.

**STEP 13 |** **Commit (Validez)** la configuration.

## Cas d'utilisation : Configuration de pools d'adresses IP NAT source séparés pour des pare-feu HA actifs/actifs

Si vous souhaitez utiliser des pools d'adresses IP pour la source NAT en mode HA active/active, chaque pare-feu doit avoir son propre pool, que vous liez ensuite à un ID d'appareil dans une règle NAT.

Les objets d'adresse et règles NAT sont synchronisés (en mode actif/passif et en mode actif/actif), vous devez donc les configurer sur un seul des pare-feu de la paire HA.

Cet exemple configure un objet d'adresse nommé Dyn-IP-Pool-dev0 contenant le pool d'adresses IP 10.1.1.140-10.1.1.150. Il configure également un objet d'adresse nommé Dyn-IP-Pool-dev1 contenant le pool d'adresses IP 10.1.1.160-10.1.1.170. Le premier objet d'adresse est lié à l'ID d'appareil 0 ; le second à l'ID d'appareil 1.

**STEP 1 |** Sur un pare-feu HA, créez les objets d'adresse.

1. Sélectionnez **Objects (Objets)** > **Addresses (Adresses)** et **Add (Ajoutez)** un **Name (Nom)** d'objet d'adresse, dans cet exemple, Dyn-IP-Pool-dev0.
2. Pour **Type (Type)**, sélectionnez **IP Range (Plage d'IP)** et saisissez la plage 10.1.1.140-10.1.1.150.
3. Cliquez sur **OK**.
4. Répétez cette étape pour configurer un autre objet d'adresse nommé Dyn-IP-Pool-dev1 avec la **IP Range (Plage d'IP)** 10.1.1.160-10.1.1.170.

**STEP 2 |** Créez la règle NAT source pour l'ID d'appareil 0.

1. Sélectionnez **Policies (Politiques)** > **NAT (NAT)** et sélectionnez **Add (Ajouter)** pour ajouter une règle de politique NAT avec un **Name (Nom)**, par exemple, Src-NAT-dev0.
2. Pour **Original Packet (Paquet d'origine)**, dans **Source Zone (Zone source)**, sélectionnez **Any (N'importe laquelle)**.
3. Pour **Destination Zone (Zone de destination)**, sélectionnez la zone de destination pour laquelle vous souhaitez traduire l'adresse source, comme la zone Non approuvé.
4. Pour **Translated Packet (Paquet traduit)**, dans **Translation Type (Type de traduction)**, sélectionnez **Dynamic IP and Port (IP et port dynamiques)**.
5. Pour **Translated Address (Adresse traduite)**, sélectionnez **Add (Ajouter)** pour ajouter l'objet d'adresse que vous avez créé pour le pool d'adresses appartenant à l'ID d'appareil 0 : Dyn-IP-Pool-dev0.
6. Pour **Active/Active HA Binding (Liaison HA Active/Active)**, sélectionnez **0** pour lier la règle NAT à l'ID d'appareil 0.
7. Cliquez sur **OK**.

**STEP 3 |** Créez la règle NAT source pour l'ID d'appareil 1.

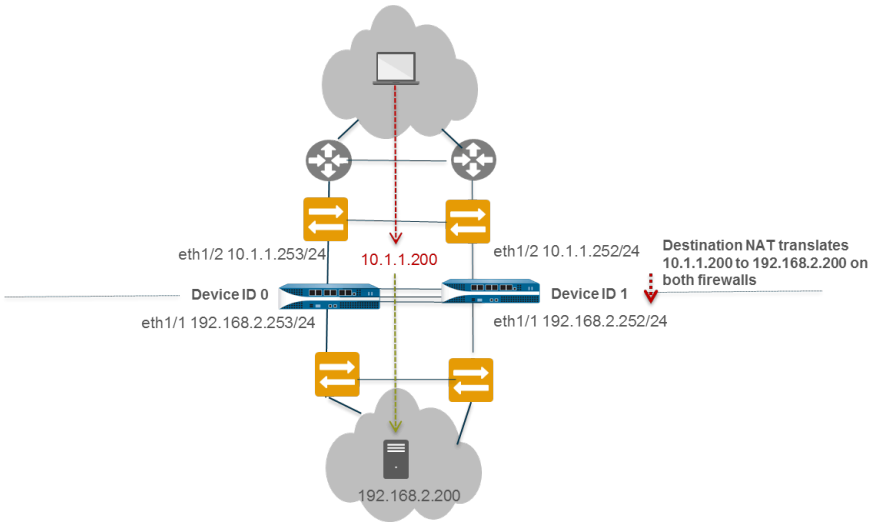
1. Sélectionnez **Policies (Politiques)** > **NAT (NAT)** et sélectionnez **Add (Ajouter)** pour ajouter une règle de politique NAT avec un **Name (Nom)**, par exemple, Src-NAT-dev1.
2. Pour **Original Packet (Paquet d'origine)**, dans **Source Zone (Zone source)**, sélectionnez **Any (N'importe laquelle)**.
3. Pour **Destination Zone (Zone de destination)**, sélectionnez la zone de destination pour laquelle vous souhaitez traduire l'adresse source, comme la zone Non approuvé.
4. Pour **Translated Packet (Paquet traduit)**, dans **Translation Type (Type de traduction)**, sélectionnez **Dynamic IP and Port (IP et port dynamiques)**.
5. Pour **Translated Address (Adresse traduite)**, sélectionnez **Add (Ajouter)** pour ajouter l'objet d'adresse que vous avez créé pour le pool d'adresses appartenant à l'ID d'appareil 1 : Dyn-IP-Pool-dev1.
6. Pour **Active/Active HA Binding (Liaison HA Active/Active)**, sélectionnez **1** pour lier la règle NAT à l'ID d'appareil 1.
7. Cliquez sur **OK**.

**STEP 4 |** **Commit (Validez)** la configuration.

## Cas d'utilisation : Configuration de la HA active/active avec le partage de charge ARP avec la NAT de destination

L'interface de Couche 3 utilise NAT en mode HA actif/actif et le Partage de charge ARP avec la NAT de destination. Les deux pare-feu HA répondent à une requête ARP pour l'adresse NAT de destination avec l'adresse MAC de l'interface d'entrée. La NAT de destination traduit l'adresse IP partagée publique (dans cet exemple 10.1.1.200) en adresse IP privée du serveur (dans cet exemple 192.168.2.200).

Lorsque les pare-feu HA reçoivent du trafic pour la destination 10.1.1.200, les deux pare-feu peuvent répondre à la requête ARP, ce qui peut causer une instabilité du réseau. Pour éviter le problème potentiel, configurez le pare-feu qui est en état actif-principal pour répondre à la requête ARP en liant la règle NAT de destination au pare-feu actif-principal.




**STEP 1 |** Sur PA-3050-2 (ID de périphérique 1), effectuez les étapes 1 à 3 de Configure Active/Active HA (Configuration de la HA active/active).

**STEP 2 |** Activez la HA active/active.

1. Dans **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, modifiez la configuration.
2. Sélectionnez **Enable HD (Activer la HD)**.
3. Saisissez un **Group ID (ID de groupe)**, qui doit être le même pour les deux pare-feu. Le pare-feu utilise un ID de groupe pour calculer l'adresse MAC virtuelle (la plage est de 1 à 63).
4. (Facultatif) Saisissez une **Description (Description)**.
5. Pour **Mode (Mode)**, sélectionnez **Active Active (Active Active)**.
6. Pour **Device ID (ID d'appareil)**, sélectionnez **1**.
7. Sélectionnez **Enable Config Sync (Activer la synchronisation de la configuration)**. Ce paramètre est requis pour synchroniser les deux configurations de pare-feu (activé par défaut).
8. Saisissez la **Peer HA1 IP Address (Adresse IP de l'homologue HA1)**, à savoir l'adresse IP de la liaison de contrôle HA1 sur le pare-feu homologue.
9. (Facultatif) Saisissez la valeur pour **Backup Peer HA1 IP Address (Adresse IP de l'homologue HA1 de sauvegarde)**, à savoir l'adresse IP de la liaison de contrôle de sauvegarde du pare-feu de l'homologue.
10. Cliquez sur **OK**.

**STEP 3 |** Effectuez les étapes 6 à 15 dans Configure Active/Active HA (Configuration de la HA active/active).

**STEP 4 |** Configurez une adresse virtuelle HA.

1. Sélectionnez **Device (Équipement)** > **High Availability (Haute disponibilité)** > **Active/Active Config (Configuration active/active)** > **Virtual Address (Adresse virtuelle)**, puis cliquez sur **Add (Ajouter)**.
2. Sélectionnez l'**Interface (Interface)** eth1/1.
3. Sélectionnez **IPv4 (IPv4)** et **Add (Ajoutez)** une **IPv4 Address (adresse IPv4)** de 10.1.1.200.
4. Pour **Type (Type)**, sélectionnez **ARP Load Sharing (Partage de charge ARP)**, qui configure l'adresse IP virtuelle de manière à ce que les deux homologues l'utilisent pour le Partage de charge ARP.

**STEP 5 |** Configurez le Partage de charge ARP.

L'algorithme de sélection d'appareil détermine le pare-feu HA qui répond aux requêtes ARP pour fournir le partage de charge.

1. Pour **Device Selection Algorithm (Algorithme de sélection d'appareil)**, sélectionnez **IP Modulo (Modulo IP)**. Le pare-feu qui répondra aux requêtes ARP en fonction de la parité de l'adresse IP du demandeur ARP.
2. Cliquez sur **OK**.

**STEP 6 |** Enable jumbo frames on firewalls other than the PA-7000 Series. (Activez les trames jumbo et pare-feu autres que les pare-feux PA-7000 Series.)

**STEP 7 |** Définition des conditions de basculement HA.

**STEP 8 |** **Commit (Validez)** la configuration.

**STEP 9 |** Configurez le pare-feu homologue, PA-3050-1 (ID d'appareil 0), avec les mêmes paramètres, à l'exception de l'étape 2 : sélectionnez **Device ID 0 (ID de périphérique 0)**.

**STEP 10 |** Toujours sur le PA-3050-1 (ID d'appareil 0), créez la règle NAT de destination pour que le pare-feu actif-principal réponde aux requêtes ARP.

1. Sélectionnez **Policies (Politiques)** > **NAT (NAT)**, puis cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name (Nom)** pour la règle qui, dans cet exemple, l'identifie comme la règle NAT de destination pour ARP de Couche 2.
3. Pour **NAT Type (Type de NAT)**, sélectionnez **ipv4** (paramètre par défaut).
4. Sur **Original Packet (Paquet d'origine)**, dans **Source Zone (Zone source)**, sélectionnez **Any (N'importe laquelle)**.
5. Pour **Destination Zone (Zone de destination)**, sélectionnez la zone Non validé que vous avez créée pour le réseau externe.
6. Laissez **Destination Interface (Interface de destination)**, **Service (Service)** et **Source Address (Adresse source)** sur **Any (Tout)**.
7. Pour **Destination Address (Adresse de destination)**, spécifiez 10.1.1.200.
8. Pour le **Translated Packet (Paquet traduit)**, la traduction d'adresse source reste **None (Aucune)**.
9. Pour **Destination Address Translation (Traduction d'adresse de destination)**, saisissez l'adresse IP privée du serveur de destination, dans cet exemple 192.168.1.200.
10. Dans l'onglet **Active/Active HA Binding (Liaison HA Active/Active)**, pour **Active/Active HA Binding (Liaison HA Active/Active)** sélectionnez **primary (principal)** pour lier la règle NAT à l'état actif-principal.
11. Cliquez sur **OK**.

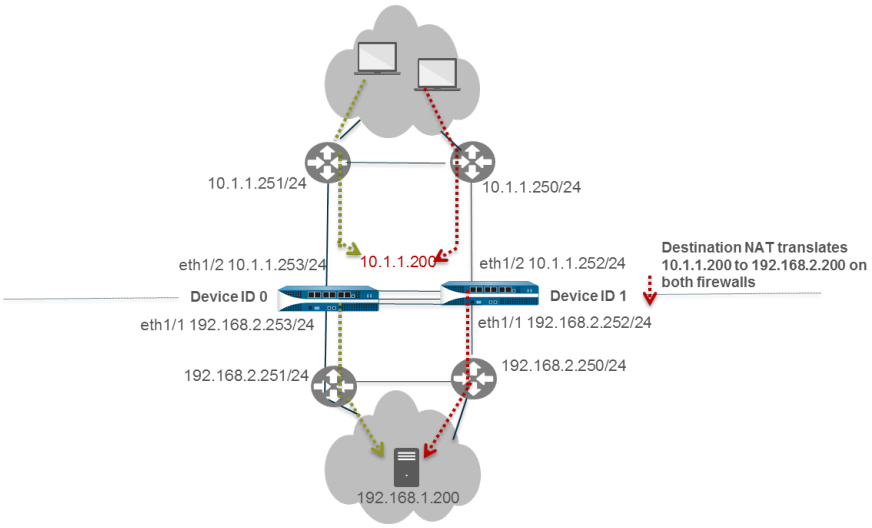
**STEP 11 |** **Commit (Validez)** la configuration.

## Cas d'utilisation : Configuration de la HA active/active avec le partage de charge ARP avec la NAT de destination dans la Couche 3

L'interface de Couche 3 utilise NAT en mode HA actif/actif et le Partage de charge ARP. PA-3050-1 a l'ID d'appareil 0 et son homologue HA, PA-3050-2, l'ID d'appareil 1.

Dans ce cas pratique, les deux pare-feu HA doivent répondre à une requête ARP pour l'adresse NAT de destination. Le trafic peut arriver sur n'importe lequel des pare-feu à partir de n'importe quel routeur WAN dans la zone non validée. Le NAT de destination traduit l'adresse IP partagée orientée public en adresse IP privée du serveur. La configuration nécessite qu'une règle NAT de destination soit liée aux deux ID d'appareil pour que les deux pare-feu puissent répondre aux requêtes ARP.




**STEP 1 |** Sur PA-3050-2 (ID de périphérique 1), effectuez les étapes 1 à 3 de Configure Active/Active HA (Configuration de la HA active/active).

**STEP 2 |** Activez la HA active/active.

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)** > **Setup (Configuration)**, puis modifiez.
2. Sélectionnez **Enable HD (Activer la HD)**.
3. Saisissez un **Group ID (ID de groupe)**, qui doit être le même pour les deux pare-feu. Le pare-feu utilise un ID de groupe pour calculer l'adresse MAC virtuelle (la plage est de 1 à 63).
4. (Optional (Facultatif)) Saisissez une **Description**.
5. Pour **Mode (Mode)**, sélectionnez **Active Active (Active Active)**.
6. Pour **Device ID (ID d'appareil)**, sélectionnez **1**.
7. Sélectionnez **Enable Config Sync (Activer la synchronisation de la configuration)**. Ce paramètre est requis pour synchroniser les deux configurations de pare-feu (activé par défaut).
8. Saisissez la **Peer HA1 IP Address (Adresse IP de l'homologue HA1)**, à savoir l'adresse IP de la liaison de contrôle HA1 sur le pare-feu homologue.
9. (Optional (Facultatif)) Saisissez la valeur pour **Backup Peer HA1 IP Address (Adresse IP de l'homologue HA1 de sauvegarde)**, à savoir l'adresse IP de la liaison de contrôle de sauvegarde du pare-feu de l'homologue.
10. Cliquez sur **OK**.

**STEP 3 |** Configuration de la HA active/active.

Effectuez les étapes 6 à 15.

**STEP 4 |** Configurez une adresse virtuelle HA.

1. Sélectionnez **Device (périphérique)** > **High Availability (Haute disponibilité)** > **Active/Active Config (Configuration active/active)** > **Virtual Address (Adresse virtuelle)**, puis cliquez sur **Add (Ajouter)**.
2. Sélectionnez l'**Interface** eth1/2.
3. Sélectionnez **IPv4 (IPv4)** et **Add (Ajoutez)** une **IPv4 Address (adresse IPv4)** de 10.1.1.200.
4. Pour **Type (Type)**, sélectionnez **ARP Load Sharing (Partage de charge ARP)**, qui configure l'adresse IP virtuelle de manière à ce que les deux homologues l'utilisent pour le Partage de charge ARP.

**STEP 5 |** Configurez le Partage de charge ARP.

L'algorithme de sélection d'appareil détermine le pare-feu HA qui répond aux requêtes ARP pour fournir le partage de charge.

1. Sous **Device Selection Algorithm (Algorithme de sélection d'appareil)**, sélectionnez l'une des options suivantes
   - **IP Modulo (Modulo IP)** : le pare-feu qui répondra aux requêtes ARP dépend de la parité de l'adresse IP du demandeur ARP.
   - **IP Hash (Hachage IP)** : le pare-feu qui répondra aux requêtes ARP en fonction d'un hachage des adresses IP source et de destination du demandeur ARP.
2. Cliquez sur **OK**.

**STEP 6 |** Activez les trames jumbo et pare-feu autres que les pare-feu PA-7000 Series.

**STEP 7 |** Définition des conditions de basculement HA.

**STEP 8 |** **Commit (Validez)** la configuration.

**STEP 9 |** Configurez le pare-feu homologue, PA-3050-1 (ID d'appareil 0), avec les mêmes paramètres, à l'exception du **Device ID (ID d'appareil)** sur **0** au lieu de **1**.

**STEP 10 |** Toujours sur le PA-3050-1 (ID d'appareil 0), créez la règle NAT de destination pour les ID d'appareil 0 et 1.

1. Sélectionnez **Policies (Politiques)** > **NAT (NAT)**, puis cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name (Nom)** pour la règle qui, dans cet exemple, l'identifie comme la règle NAT de destination pour ARP de Couche 3.
3. Pour **NAT Type (Type de NAT)**, sélectionnez **ipv4** (paramètre par défaut).
4. Sur **Original Packet (Paquet d'origine)**, dans **Source Zone (Zone source)**, sélectionnez **Any (N'importe laquelle)**.
5. Pour **Destination Zone (Zone de destination)**, sélectionnez la zone Non validé que vous avez créée pour le réseau externe.
6. Laissez **Destination Interface (Interface de destination)**, **Service (Service)** et **Source Address (Adresse source)** sur **Any (Tout)**.
7. Pour **Destination Address (Adresse de destination)**, spécifiez 10.1.1.200.
8. Pour le **Translated Packet (Paquet traduit)**, la traduction d'adresse source reste None (Aucune).
9. Pour **Destination Address Translation (Traduction d'adresse de destination)**, saisissez l'adresse IP privée du serveur de destination, dans cet exemple 192.168.1.200.
10. Dans l'onglet **Active/Active HA Binding (Liaison HA Active/Active)**, pour **Active/Active HA Binding (Liaison HA Active/Active)** sélectionnez **both (les deux)** pour lier la règle NAT aux ID d'appareil 0 et 1.
11. Cliquez sur **OK**.

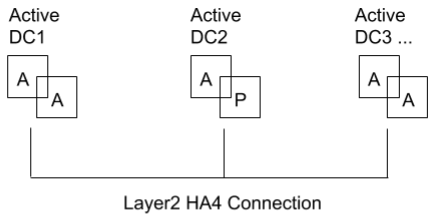
**STEP 11 |** **Commit (Validez)** la configuration.

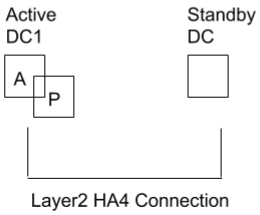
 

# Présentation de la mise en cluster HA

Un certain nombre de modèles de pare-feu Palo Alto Networks® prennent désormais en charge la synchronisation de l'état des sessions entre les pare-feu dans un cluster à haute disponibilité (HA) comprenant jusqu'à 16 pare-feu. Les homologues du cluster HA synchronisent les sessions pour se protéger contre les défaillances du centre de données ou d'un grand point d'inspection de sécurité avec des pare-feu à échelle horizontale. En cas de panne de réseau ou de défaillance d'un pare-feu, les sessions basculent vers un autre pare-feu dans le cluster. Cette synchronisation est particulièrement utile dans les cas d'utilisation suivants.

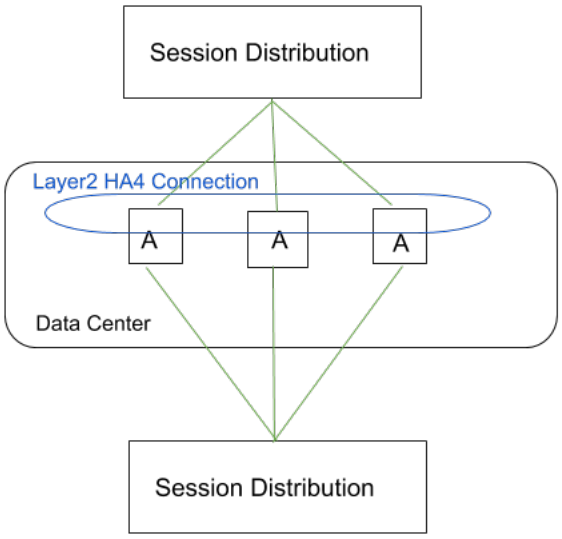
Un cas d'utilisation est celui où les homologues HA sont répartis sur plusieurs centres de données de sorte qu'il n'y a pas de point de défaillance unique au sein ou entre les centres de données. Un deuxième cas d'utilisation de centres de données multiples est celui où un centre de données est actif et l'autre est en veille.




Un troisième cas d'utilisation de la mise en cluster HA est la mise à l'échelle horizontale, dans laquelle vous ajoutez des membres du cluster HA à un seul centre de données pour augmenter la sécurité et assurer la survie des sessions.




Les clusters HA prennent en charge un déploiement de couche 3 ou de câble virtuel. Les homologues HA dans le cluster peuvent être une combinaison de paires HA et de membres autonomes du cluster. Dans un cluster HA, tous les membres sont considérés comme actifs ; il n'y a pas de concept de pare-feu passif, sauf pour les paires HA, qui peuvent conserver leur relation active/passive après que vous les ayez ajoutés à un cluster HA.

Tous les membres du cluster partagent l'état de la session. Lorsqu'un nouveau pare-feu rejoint un cluster HA, cela déclenche tous les pare-feu du cluster pour synchroniser toutes les sessions existantes. Les connexions de secours HA4 et HA4 sont les liens de cluster dédiés qui synchronisent l'état de la session entre tous les membres du cluster ayant le même ID de cluster. Le lien HA4 entre les membres du cluster détecte des échecs de connectivité entre les membres du cluster. HA1 (lien de contrôle), HA2 (lien de données) et HA3 (lien de transfert de paquets) ne sont pas pris en charge entre les membres du cluster qui ne sont pas des paires HA.

Pour une session normale qui n'a pas échoué, seul le pare-feu qui est le propriétaire de la session crée un journal de trafic. Pour une session qui a échoué, le nouveau propriétaire de la session (le pare-feu qui reçoit le trafic ayant échoué) crée le journal du trafic.

Les modèles de pare-feu qui prennent en charge la mise en cluster HA et le nombre maximum de membres pris en charge par cluster sont les suivants :

| Firewall Model (Modèle de pare-feu) | Nombre de membres pris en charge par cluster |
|---|---|
| PA-3200 Series | 6 |
| PA-5200 Series | 16 |
| PA-5450 | 8 |

| Firewall Model (Modèle de pare-feu) | Nombre de membres pris en charge par cluster |
|---|---|
| Les pare-feu de la série PA-7000 qui possèdent au moins une des cartes suivantes : PA-7000-100G-NPC, PA-7000-20GQXM-NPC, PA-7000-20GXM-NPC | PA-7080 : 4<br>PA-7050 : 6 |
| VM-300 | 6 |
| VM-500 | 6 |
| VM-700 | 16 |

Le clustering HA n'est pas pris en charge dans les déploiements de cloud public. Envisagez le Bonnes pratiques et approvisionnement de la mise en cluster HA avant de commencer à Configuration de la mise en cluster HA.

# Bonnes pratiques et approvisionnement de la mise en cluster HA

Il s'agit des exigences en matière d'approvisionnement et des meilleures pratiques pour la mise en cluster HA.

- Exigences d'approvisionnement et meilleures pratiques
  - Les membres du cluster HA doivent avoir le même modèle de pare-feu et utiliser la même version de PAN-OS®.

    ***Lors de la mise à niveau, les membres du pare-feu continueront à synchroniser les sessions avec un membre d'une version différente.***
  - Il est fortement recommandé et constitue une bonne pratique d'utiliser Panorama pour fournir aux membres du cluster HA la possibilité de garder toutes les configurations et les politiques synchronisées entre tous les membres du cluster.
  - Les membres du cluster HA doivent obtenir une licence pour les mêmes composants afin de garantir une application cohérente des politiques et des capacités d'inspection du contenu.
  - Les licences doivent expirer en même temps afin d'éviter des licences mal assorties et la perte de fonctionnalité.
  - Tous les membres du cluster doivent fonctionner avec la même version des mises à jour de contenu dynamiques pour une application cohérente de la sécurité.
  - Les membres du cluster HA doivent partager les mêmes noms de zone afin que les sessions puissent être transférées avec succès à un autre membre du cluster. Par exemple, supposons que les sessions allant vers une zone d'entrée nommée **`interne`** soient abandonnées parce que le lien est hors service. Pour que ces sessions passent à un pair de pare-feu HA dans le cluster, cet homologue doit également avoir une zone nommée **`interne`**.
  - Les flux client-serveur et serveur-client doivent retourner au même pare-feu dans des conditions normales (sans défaillance) pour que l'analyse du contenu de sécurité puisse avoir lieu. Le trafic asymétrique ne sera pas abandonné, mais il ne peut pas être analysé pour des raisons de sécurité.
- Meilleures pratiques en matière de synchronisation des sessions
  - Des interfaces de communication HA dédiées doivent être utilisées sur les interfaces de plan de données. Les interfaces HSCI ne sont pas utilisées pour HA4. Cela permet de séparer la synchronisation des sessions de la paire HA et du cluster afin de garantir une bande passante et une fiabilité maximales pour la synchronisation des sessions.
  - HA4 doit être de taille adéquate si vous utilisez des interfaces de plan de données. Cela garantit une synchronisation optimale de l'état des sessions entre les membres du groupe.
  - La meilleure pratique consiste à disposer d'un réseau en cluster dédié pour le lien de communication HA4 afin de garantir une bande passante adéquate et des connexions non encombrées et à faible latence entre les membres du cluster.
  - Architecturer vos réseaux et effectuer une ingénierie du trafic pour éviter d'éventuelles conditions de course, dans lesquelles un réseau dirige le trafic du propriétaire de la session vers un membre du cluster avant que la session ne soit synchronisée avec succès entre les

pare-feu. Les connexions HA4 de la couche 2 doivent avoir une largeur de bande suffisante et une faible latence pour permettre une synchronisation rapide entre les membres HA. La latence HA4 doit être inférieure à la latence encourue lorsque les périphériques d'échange de trafic commutent le trafic entre les membres du cluster.

  - Architecturez vos réseaux pour minimiser les flux asymétriques. La configuration de la session nécessite qu'un membre du cluster voit la communication TCP à trois voies complète.

- Meilleures pratiques en matière de contrôle de santé
  - Sur les paires HA dans un cluster, configurez une paire active/passive avec des liens de communication de secours HA pour HA1, HA2 et HA4. Configurez une paire active/active avec des liens de communication de secours HA pour HA1, HA2, HA3 et HA4.
  - Configurer les liens de secours HA4 sur tous les membres du cluster.

# Configuration de la mise en cluster HA

Apprenez-en plus sur la mise en cluster HA et suivez la Bonnes pratiques et approvisionnement de la mise en cluster HA avant de configurer des pare-feu HA en tant que membres d'un cluster.

**STEP 1 |** Établissement d'une interface en tant qu'interface HA (à assigner plus tard comme lien HA4).

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)** et choisissez une interface, par exemple, Ethernet1/1.
2. Sélectionnez le **Interface Type (Type d'interface) HA**.
3. Cliquez sur **OK**.
4. Répétez cette étape pour configurer une autre interface à utiliser comme lien de secours HA4.

**STEP 2 |** Activation de la mise en cluster HA.

1. Sélectionnez **Device (Appareil)** > **High Availability (Haute disponibilité)** > **General (Général)**, puis modifiez la section Clustering Settings (Paramètres de mise en cluster).
2. **Enable Cluster Participation (Activez la participation au cluster)**.
3. Saisissez le **Cluster ID (ID de cluster)**, un ID numérique unique pour un cluster HA dans lequel tous les membres peuvent partager l'état de la session ; la plage est de 1 à 99.
4. Saisissez une brève et utile **Cluster Description (Description du cluster)**.
5. (Facultatif) Modifiez le **Cluster Synchronization Timeout (min) (Délai d'expiration de synchronisation du cluster)**, qui est le nombre maximum de minutes que le pare-feu local attend avant de passer à l'état Actif lorsqu'un autre membre du cluster (par exemple, dans un état inconnu) empêche la synchronisation complète du cluster ; la plage est de 0 à 30 ; la valeur par défaut est 0.
6. (Facultatif) Modifiez le **Monitor Fail Hold Down Time (min) (Temps de maintien en cas de panne d'un moniteur)**, qui est le nombre de minutes après lequel un lien descendant est testé à nouveau pour voir s'il est à nouveau fonctionnel ; la plage est de 1 à 60 ; la valeur par défaut est 1.
7. Cliquez sur **OK**.

**STEP 3 |** Configurez la liaison HA4.

1. Sélectionnez **HA Communications (Communications HA)** et dans la section Clustering Links (Liaisons de mise en cluster), modifiez la section HA4.
2. Sélectionnez l'interface que vous avez configurée à la première étape en tant qu'interface **HA** pour qu'elle soit le **Port** de la liaison HA4 ; par exemple Ethernet1/1.
3. Saisissez l'**IPv4/IPv6 Address (Adresse IPv4/IPv6)** de l'interface HA4 locale.
4. Saisissez le **Netmask (Masque de réseau)**.
5. (Facultatif) Modifiez le **HA4 Keep-alive Threshold (ms) Seuil de maintien HA4 (ms))** pour spécifier le délai pendant lequel le pare-feu doit recevoir des messages de maintien d'un membre du cluster afin de savoir que le membre du cluster fonctionne (la plage est de 5 000 à 60 000 ; la valeur par défaut est 10 000).
6. Cliquez sur **OK**.

**STEP 4 |** Configurez la liaison de secours HA4.

1. Modifiez la section HA4 Backup (Secours HA4).
2. Sélectionnez l'autre interface que vous avez configurée à la première étape en tant qu'interface **HA** pour qu'elle soit le **Port** de la liaison de secours HA4.
3. Saisissez l'**IPv4/IPv6 Address (Adresse IPv4/IPv6)** de l'interface de secours HA4 locale.
4. Saisissez le **Netmask (Masque de réseau)**.
5. Cliquez sur **OK**.

**STEP 5 |** Spécifiez tous les membres du cluster HA, y compris le membre local et les deux homologues HA dans toute paire HA.

1. Sélectionnez **Cluster Config (Configuration du cluster)**.
2. (Sur un pare-feu pris en charge) **Add (Ajoutez)** le **Device Serial Number (Numéro de série de périphérique)** d'un membre homologue.
3. (Sur Panorama) **Add (Ajoutez)** et sélectionnez un **Device (Périphérique)** dans la liste déroulante et saisissez un **Device Name (Nom de périphérique)**.
4. Saisissez l'**HA4 IP Address (Adresse IP HA4)** de l'homologue HA dans le cluster.
5. Saisissez l'**HA4 Backup IP Address (Adresse IP de secours HA4)** de l'homologue HA dans le cluster.
6. Activez la **Session Synchronization (Synchronisation de session)** avec l'homologue que vous avez identifié.
7. (Facultatif) Saisissez une **Description** utile.
8. Cliquez sur **OK**.
9. Sélectionnez le périphérique et **Enable (Activez-le)**.

**STEP 6 |** Define HA failover conditions (Définissez les conditions de basculement HA) avec lien et surveillance des chemins.

**STEP 7 |** **Commit** (Valider).

**STEP 8 |** (Panorama uniquement) Actualisez la liste des pare-feu HA dans le cluster HA.

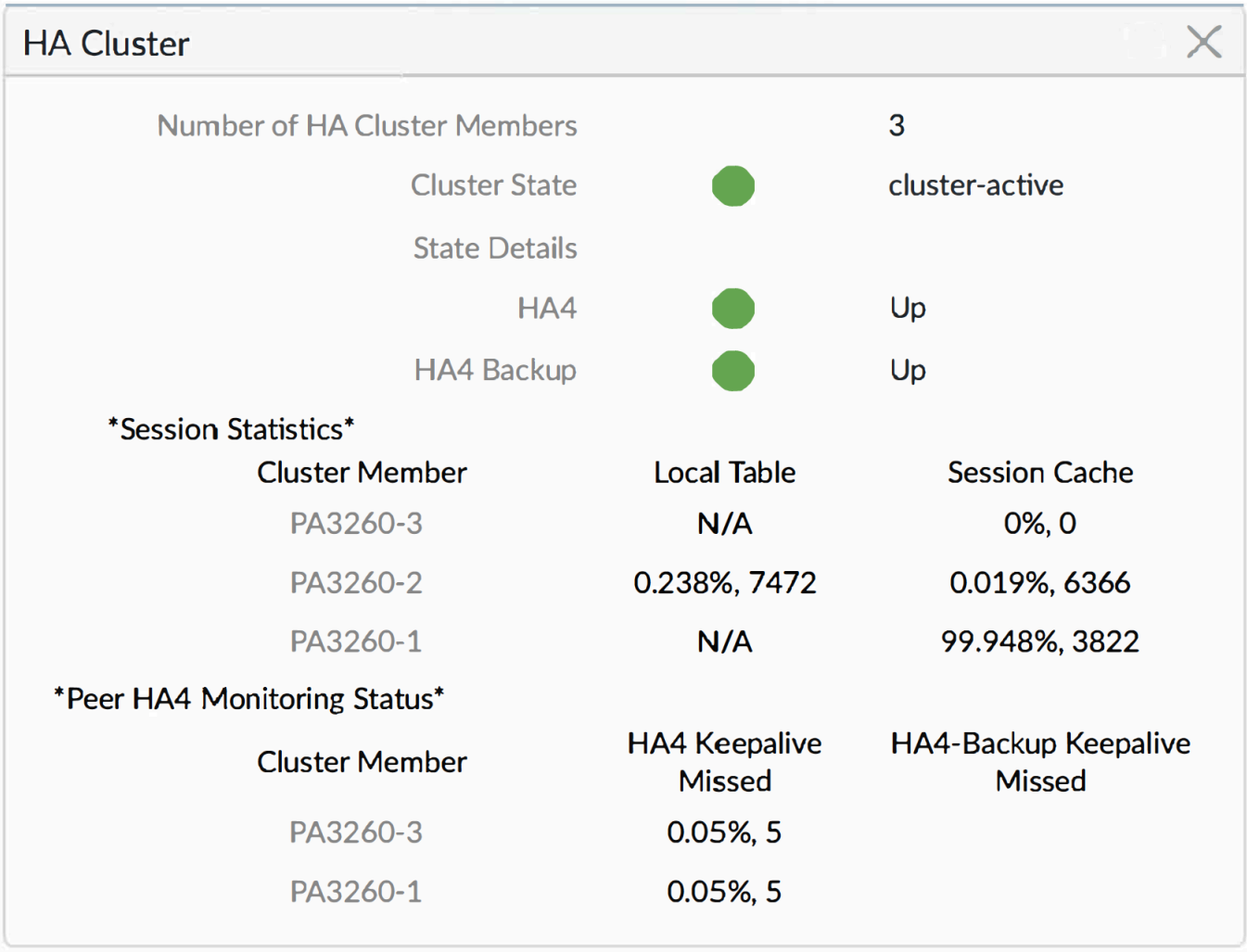
1. Sous Templates (Modèles), sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **Cluster Config (Configuration du cluster)**.
2. Cliquez sur **Refresh (Actualiser)** au bas de l'écran.

**STEP 9 |** Affichez les informations du cluster HA sur l'IU.

1. Sélectionnez **Dashboard (Tableau de bord)**.
2. Affichez les champs du cluster HA. La section supérieure affiche l'état du cluster et les connexions HA4 pour fournir un aperçu de la santé du cluster. Les indicateurs HA4 et HA4 Backup (Secours HA4) seront l'un des suivants : Vert indique que l'état de la liaison des membres du cluster est Up. Rouge indique que l'état de la liaison de tous les membres du cluster est Down. Jaune indique que l'état de la liaison de certains membres du cluster est Up tandis que l'état d'autres membres du cluster est Down. Gris indique l'absence de configuration. La section centrale affiche la capacité de la table de session locale et de la table de cache de session afin que vous puissiez surveiller le niveau de remplissage des tables et planifier les mises à niveau du pare-feu. La section inférieure affiche les erreurs

de communication sur les liaisons HA4 et de secours HA4, ce qui indique d'éventuels problèmes de synchronisation des informations entre les membres.


HA Cluster

| | | |
|---|---|---|
| Number of HA Cluster Members | | 3 |
| Cluster State | | cluster-active |
| State Details | | |
| HA4 | | Up |
| HA4 Backup | | Up |

*Session Statistics*

| Cluster Member | Local Table | Session Cache |
|---|---|---|
| PA3260-3 | N/A | 0%, 0 |
| PA3260-2 | 0.238%, 7472 | 0.019%, 6366 |
| PA3260-1 | N/A | 99.948%, 3822 |

*Peer HA4 Monitoring Status*

| Cluster Member | HA4 Keepalive Missed | HA4-Backup Keepalive Missed |
|---|---|---|
| PA3260-3 | 0.05%, 5 | |
| PA3260-1 | 0.05%, 5 | |

**STEP 10 |** Access the CLI (Accéder à la CLI) pour afficher le cluster HA et les informations de liaison HA4 et effectuer d'autres tâches de mise en cluster HA.

*Vous pouvez afficher les statistiques de volet de cluster HA. Le nombre de volets de cluster est réinitialisé lorsque le périphérique HA passe de suspendu à fonctionnel et vice versa. Le nombre de volets de cluster se réinitialise également lorsque le temps de maintien non fonctionnel expire.*

# Actualisation des clés SSH HA1 et configuration des options des clés

La Secure Shell (SSH) est préconfigurée sur tous les pare-feux Palo Alto Networks, et les pare-feux haute disponibilité (HA) peuvent faire office de serveur SSH et de client SSH simultanément. Lorsque vous configurez la HA active/passive ou la active/active, vous pouvez activer le chiffrement de la connexion HA1 (liaison de contrôle) entre les pare-feu HA. Nous vous recommandons de sécuriser le trafic HA1 entre les homologues HA par un cryptage, en particulier si les pare-feu ne sont pas situés sur le même site. Après avoir activé le cryptage sur la liaison de contrôle HA1, vous pouvez utiliser la CLI pour créer un profil de service SSH et sécuriser la connexion entre les pare-feu HA.

Les profils de service SSH vous permettent de changer le type de clé hôte par défaut, de générer une nouvelle paire de clés hôtes SSH publiques et privées pour la liaison de contrôle HA1, et de configurer d'autres paramètres SSH HA1. Vous pouvez appliquer les nouvelles clés d'hôte et les paramètres configurés aux pare-feu sans redémarrer les homologues HA. Le pare-feu rétablira les sessions HA1 avec son homologue pour synchroniser les changements de configuration. Il génère également des journaux système (sous-type **ha**) pour le rétablissement des sessions de secours HA1 et HA1.

Les exemples suivants montrent comment configurer divers paramètres SSH pour votre HA1 après avoir activé le cryptage et accédé à la CLI. (Consultez Actualisation des clés SSH et configuration des options des clés pour la connexion à l'interface de gestion pour des exemples de profils de serveurs de gestion SSH).

*Avant de pouvoir effectuer les tâches suivantes, vous devez activer le chiffrement sur une paire HA et celui-ci doit fonctionner correctement.*

*Si vous configurez la liaison de contrôle HA1 en mode FIPS-CC, vous devez définir les paramètres de régénération automatiques des clés de session.*

*Pour utiliser les mêmes paramètres de connexion SSH pour chaque collecteur de journaux dédié (M-Series ou appareil virtuel Panorama en mode collecteur de journaux) dans un Collector Group (Groupe de collecteurs), configurez un profil de service SSH à partir du serveur de gestion Panorama, **Commit (validez)** les changements dans Panorama, puis **Push (poussez)** la configuration vers les collecteurs de journaux. Vous pouvez utiliser les commandes **`set log-collector-group <name> general-setting management ssh`**.*

- Créez un profil de service SSH pour exercer un plus grand contrôle sur les connexions SSH entre vos pare-feu HA.

  Cet exemple crée un profil HA sans aucune configuration de paramètres.

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles *<name>***
  3. admin@PA-3250# **commit**
  4. admin@PA-3250# **exit**
  5. Pour vérifier que le nouveau profil a été créé et voir les paramètres de tout profil existant :

     admin@PA-3250> **configure**

     admin@PA-3250# **show deviceconfig system ssh profiles**

- (Facultatif) Définissez le serveur SSH pour qu'il utilise uniquement les chiffrements de cryptage spécifiés pour les sessions HA1.

  Par défaut, HA1 SSH permet tous les chiffrements pris en charge pour le cryptage des sessions CLI HA. Lorsque vous définissez un ou plusieurs codes, le serveur SSH ne publie que ces chiffres

lors de la connexion, et si le client SSH (homologue HA) tente de se connecter en utilisant un autre code, le serveur met fin à la connexion.

1. admin@PA-3250> **configure**
2. admin@PA-3250# **set deviceconfig system ssh profiles ciphers ha-profiles <*name*> ciphers <*cipher*>**

   **aes128-cbc** : chiffrement AES avec chaînage du chiffrement par blocs de 128 bits

   **aes128-ctr** : chiffrement AES de 128 bits en mode Compteur

   **aes128-gcm** : chiffrement AES de 128 bits en mode GCM (Galois/compteur)

   **aes192-cbc** : chiffrement AES avec chaînage du chiffrement par blocs de 192 bits

   **aes192-ctr** : Chiffrement AES de 192 bits en mode Compteur

   **aes256-cbc** : chiffrement AES avec chaînage du chiffrement par blocs de 256 bits

   **aes256-ctr** : chiffrement AES de 256 bits en mode Compteur

   **aes256-gcm** : chiffrement AES de 256 bits en mode GCM
3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. (La liaison HA1 de secours est configurée) admin@PA-3250> **request high-availability session-reestablish**
6. (Aucune liaison HA1 de secours n'est configurée ou la liaison HA1 de secours est en panne) admin@PA-3250> **request high-availability session-reestablish force**

   *Vous pouvez forcer le pare-feu à rétablir les sessions HA1 s'il n'y a pas de liaison HA1 de secours, ce qui cause une brève situation de « split brain » entre les homologues HA. (L'utilisation de l'option **force** lorsqu'une liaison HA1 de secours est configurée n'a aucun effet.)*
7. Pour vérifier que les chiffrements ont été mis à jour :

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles ciphers**

- (Facultatif) Définissez le type de clé d'hôte par défaut.

  Si vous activez le chiffrement sur la liaison de contrôle HA1, le pare-feu utilise une clé d'hôte par défaut (RSA 2048), sauf si vous le modifiez. La connexion SSH HA1 n'utilise que le `type de clé d'hôte par défaut` pour authentifier les homologues HA (avant qu'une session chiffrée soit établie entre eux). Vous pouvez modifier le type de clé d'hôte par défaut, les choix qui s'offrent à vous sont les suivants : ECDSA 256, 384 ou 521 ou RSA 2048, 3072 ou 4096. Modifiez le type de clé d'hôte par défaut si vous préférez une longue de clé RSA plus longue ou si vous préférez ECDSA au lieu de RSA. Cet exemple définit le type de clé d'hôte par défaut sur une clé ECDSA de 256 octets. Il rétablit également la connexion HA1 à l'aide de la nouvelle clé d'hôte sans redémarrer les homologues HA.

  1. admin@PA-3250> **configure**

2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles <*name*> default-hostkey key-type ECDSA key-length 256**
3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. admin@PA-3250> **request high-availability sync-to-remote ssh-key**

   *Une connexion HA doit déjà être établie entre les pare-feu HA. Si les pare-feu n'ont pas encore établi de connexion HA, vous devez activer le chiffrement sur la connexion de la liaison de contrôle, exportez la clé HA vers un emplacement réseau et importez la clé HA sur l'homologue. Reportez-vous aux rubriques* Configuration de la HA active/passive *ou* Configuration de la HA active/active.
6. (La liaison HA1 de secours est configurée) admin@PA-3250> **request high-availability session-reestablish**
7. (Aucune liaison HA1 de secours n'est configurée ou la liaison HA1 de secours est en panne) admin@PA-3250> **request high-availability session-reestablish force**

   *Vous pouvez forcer le pare-feu à rétablir les sessions HA1 s'il n'y a pas de liaison HA1 de secours, ce qui cause une brève situation de « split brain » entre les deux homologues HA. (L'utilisation de l'option* ***force*** *lorsqu'une liaison HA1 de secours est configurée n'a aucun effet.)*
8. Pour vérifier que la clé de l'hôte a été mise à jour :

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles <*name*> default-hostkey**

- (Facultatif) Supprimez un code de l'ensemble de codes que vous avez sélectionnés pour SSH sur la liaison de contrôle HA1.

  Dans cet exemple, le code AES à 128 bits en mode CBC est supprimé.

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **delete deviceconfig system ssh profiles ha-profiles <*name*> ciphers aes128-cbc**
  3. admin@PA-3250# **commit**
  4. admin@PA-3250# **exit**
  5. (La liaison HA1 de secours est configurée) admin@PA-3250> **request high-availability session-reestablish**
  6. (Aucune liaison HA1 de secours n'est configurée ou la liaison HA1 de secours est en panne) admin@PA-3250> **request high-availability session-reestablish force**

     *Vous pouvez forcer le pare-feu à rétablir les sessions HA1 s'il n'y a pas de liaison HA1 de secours, ce qui cause une brève situation de « split brain » entre les deux homologues HA. (Lorsqu'une liaison HA1 de secours est configurée, l'utilisation de l'option **force** n'a aucun effet.)*
  7. Pour vérifier que le chiffrement a été supprimé :

     admin@PA-3250> **configure**

     admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles <*name*> ciphers**

- (Facultatif) Définissez les algorithmes d'échange de clés de session que le serveur SSH HA1 prendra en charge.

  Par défaut, le serveur SSH (pare-feu HA) publie tous les algorithmes d'échange de clés au client SSH (pare-feu homologue HA).

  *Si vous utilisez un type de clé par défaut ECDSA, il est recommandé d'utiliser un algorithme de clé ECDH.*

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles <*name*> kex <*value*>**

     **diffie-hellman-group14-sha1** : groupe Diffie-Hellman 14 comportant un hachage SHA1

     **ecdh-sha2-nistp256** : Diffie-Hellman basé sur les courbes elliptiques P-256 du National Institute of Standards and Technology (l'Institut national des standards et de la technologie ; NIST) avec hachage SHA2-256

     **ecdh-sha2-nistp384** : Diffie-Hellman basé sur les courbes elliptiques P-384 du National Institute of Standards and Technology (l'Institut national des standards et de la technologie ; NIST) avec hachage SHA2-384

     **ecdh-sha2-nistp521** : Diffie-Hellman basé sur les courbes elliptiques P-521 du National Institute of Standards and Technology (l'Institut national des standards et de la technologie ; NIST) avec hachage SHA2-521
  3. admin@PA-3250# **commit**
  4. admin@PA-3250# **exit**
  5. (La liaison HA1 de secours est configurée) admin@PA-3250> **request high-availability session-reestablish**
  6. (Aucune liaison HA1 de secours n'est configurée ou la liaison HA1 de secours est en panne) admin@PA-3250> **request high-availability session-reestablish force**

     *Vous pouvez forcer le pare-feu à rétablir les sessions HA1 s'il n'y a pas de liaison HA1 de secours, ce qui cause une brève situation de « split brain » entre les deux homologues HA. (Lorsqu'une liaison HA1 de secours est configurée, l'utilisation de l'option **force** n'a aucun effet.)*
  7. Pour vérifier que les algorithmes d'échange de clés ont été mis à jour :

     admin@PA-3250> **configure**

     admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles**

- (Facultatif) Définissez les codes d'authentification des messages (MAC) que le serveur SSH HA1 prendra en charge.

  Par défaut, le serveur publie tous les algorithmes MAC au client.

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles <*name*> mac <*value*>**

     **hmac-sha1** : MAC comportant un hachage cryptographique SHA1

     **hmac-sha2-256** : MAC comportant un hachage cryptographique SHA2-256

     **hmac-sha2-512** : MAC comportant un hachage cryptographique SHA2-512
  3. admin@PA-3250# **commit**
  4. admin@PA-3250# **exit**
  5. (La liaison HA1 de secours est configurée) admin@PA-3250> **request high-availability session-reestablish**
  6. (Aucune liaison HA1 de secours n'est configurée ou la liaison HA1 de secours est en panne) admin@PA-3250> **request high-availability session-reestablish force**

     *Vous pouvez forcer le pare-feu à rétablir les sessions HA1 s'il n'y a pas de liaison HA1 de secours, ce qui cause une brève situation de « split brain » entre les deux homologues HA. (L'utilisation de l'option **force** n'a aucun effet lorsqu'une liaison HA1 de secours est configurée.*
  7. Pour vérifier que les algorithmes MAC ont été mis à jour :

     admin@PA-3250> **configure**

     admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles**

- (Facultatif) Régénérez les clés d'hôte ECDSA ou RSA pour que SSH HA1 remplace les clés existantes et rétablissez les sessions HA1 entre les homologues HA à l'aide de nouvelles clés sans redémarrer les homologues HA.

  Les homologues HA utilisent les clés d'hôte pour s'authentifier mutuellement. Cet exemple présente la régénération de la clé d'hôte par défaut 256 ECDSA.

  *La régénération d'une clé d'hôte ne change pas votre type de clé d'hôte par défaut. Pour régénérer la clé d'hôte par défaut que vous utilisez, vous devez spécifier votre type de clé d'hôte par défaut et la longueur lors de la régénération. La régénération d'une clé d'hôte qui ne correspond pas à votre type de clé d'hôte par défaut ne fait que régénérer une clé que vous n'utilisez pas, ce qui n'a aucun effet.*

  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh regenerate-hostkeys ha key-type ECDSA key-length 256**
  3. admin@PA-3250# **commit**
  4. admin@PA-3250# **exit**
  5. admin@PA-3250> **request high-availability sync-to-remote ssh-key**

     *Une connexion HA doit déjà être établie entre les pare-feu HA. Si les pare-feu n'ont pas encore établi de connexion HA, vous devez activer le chiffrement sur la connexion de la liaison de contrôle, exportez la clé HA vers un emplacement réseau et importez la clé HA sur l'homologue. Reportez-vous aux rubriques* Configuration de la HA active/passive *ou* Configuration de la HA active/active.
  6. (La liaison HA1 de secours est configurée) admin@PA-3250> **request high-availability session-reestablish**
  7. (Aucune liaison HA1 de secours n'est configurée ou la liaison HA1 de secours est en panne) admin@PA-3250> **request high-availability session-reestablish force**

     *Vous pouvez forcer le pare-feu à rétablir les sessions HA1 s'il n'y a pas de liaison HA1 de secours, ce qui cause une brève situation de « split brain » entre les deux homologues HA. (L'utilisation de l'option* ***force*** *lorsqu'une liaison HA1 de secours est configurée n'a aucun effet.)*

- (Facultatif) Définir les paramètres de ressaisie pour établir quand la régénération automatique des clés de session se produit pour SSH sur le lien de contrôle HA1.

  Les clés de session sont utilisées pour crypter le trafic entre les homologues HA. Les paramètres que vous pouvez définir sont le volume de données (en mégaoctets), l'intervalle de temps (en secondes) et le nombre de paquets. Une fois que l'un des paramètres de la nouvelle clé a atteint sa valeur configurée, SSH lance un échange de clés.

  Vous pouvez définir un deuxième ou un troisième paramètre si vous n'êtes pas sûr que le paramètre que vous avez configuré atteindra sa valeur dès que vous voulez que la régénération

se produise. Le premier paramètre à atteindre sa valeur configurée déclenchera une régénération de clé, puis le pare-feu réinitialisera tous les paramètres de la nouvelle clé.

1. admin@PA-3250> **configure**
2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles <*name*> session-rekey data 32**

   La régénération se produit après la transmission du volume de données (en mégaoctets) suivant la régénération précédente. La valeur par défaut est fondée sur chiffrement que vous utilisez, et se situe entre 1 Go et 4 Go ; la plage est de 10 Mo à 4 000 Mo. Vous pouvez également saisir la commande **set deviceconfig system ssh profiles ha-profiles <*name*> session-rekey data default**, qui fixe le paramètre de données à la valeur par défaut du chiffrement individuel que vous utilisez.
3. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles <*name*> session-rekey interval 3600**

   La régénération se produit après que l'intervalle (en secondes) spécifié se soit écoulé suivant la régénération précédente. Par défaut, la régénération basée sur la durée est désactivée (définie sur aucune). La plage est de 10 à 3 600.
4. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles <*name*> session-rekey packets 27**

   La régénération se produit après la transmission du nombre de paquets définis ($2^n$) suivant la régénération précédente. Par exemple, 14 configure qu'un maximum de $2^{14}$ paquets sont transmis avant qu'une régénération de clé n'ait lieu. La valeur par défaut est $2^{28}$. La plage est de 12 à 27 ($2^{12}$ à $2^{27}$). Vous pouvez également saisir **set deviceconfig system ssh profiles ha-profiles <*name*> session-rekey packets default**, qui fixe le paramètre des paquets à $2^{28}$.

   *Choisissez les paramètres de régénération en fonction du type de trafic et de la vitesse du réseau (en plus des exigences FIPS-CC si elles s'appliquent à vous). Ne définissez pas des paramètres trop bas, car ils pourraient affecter la performance SSH.*
5. admin@PA-3250# **commit**
6. admin@PA-3250# **exit**
7. (La liaison HA1 de secours est configurée) admin@PA-3250> **request high-availability session-reestablish**
8. (Aucune liaison HA1 de secours n'est configurée ou la liaison HA1 de secours est en panne) admin@PA-3250> **request high-availability session-reestablish force**

   *Vous pouvez forcer le pare-feu à rétablir les sessions HA1 s'il n'y a pas de liaison HA1 de secours, ce qui cause une brève situation de « split brain » entre les deux homologues HA. (L'utilisation de l'option **force** lorsqu'une liaison HA1 de secours est configurée n'a aucun effet.)*

9. Pour vérifier les modifications :

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles <*name*> session-rekey**

- Activez le profil en sélectionnant le profil et en redémarrant le service HA1 SSH.
  1. admin@PA-3250> **configure**
  2. admin@PA-3250# **set deviceconfig system ssh ha ha-profile <*name*>**
  3. admin@PA-3250# **commit**
  4. admin@PA-3250# **exit**
  5. admin@PA-3250> **set ssh service-restart ha**
  6. Pour vérifier que le bon profil est utilisé :

     admin@PA-3250> **configure**

     admin@PA-3250# **show deviceconfig system ssh ha**

# États des pare-feu HA

Un pare-feu HA peut afficher l'un des états suivants :

| État des pare-feu HA | Phase à laquelle il survient | Description |
|---|---|---|
| Initial | A/P ou A/A | État transitoire dans lequel se trouve le pare-feu lorsqu'il se joint à la paire HD. Le pare-feu conserve cet état après le redémarrage, jusqu'à ce qu'il découvre un homologue et que commence la négociation. Une fois le délai d'expiration écoulé, le pare-feu devient actif si la négociation HA n'a pas commencé. |
| Actif | A/P | État du pare-feu actif dans une configuration active/passive. |
| Passif | A/P | État du pare-feu passif dans une configuration active/passive. Le pare-feu passif est prêt à devenir le pare-feu actif sans interruption du réseau. Bien que le pare-feu passif ne traite pas d'autre trafic :<br>• Si l'état automatique de la liaison passive est configuré, le pare-feu passif exécute les protocoles de routage, surveille l'état des chemins et des liaisons et prénégocie LACP et LLDP si la prénégociation LACP et LLDP est configurée.<br>• Le pare-feu passif synchronise l'état du flux, l'exécution des objets et la configuration.<br>• Le pare-feu passif surveille l'état du pare-feu actif à l'aide du protocole hello. |
| Principal actif | A/A | Dans une configuration active/active, l'état du pare-feu qui se connecte aux agents User-ID, qui exécute le serveur DHCP et le relais DHCP et qui met en correspondance les règles NAT et PBF avec l'ID de périphérique du pare-feu actif principal. Lorsqu'il se trouve dans cet état, un pare-feu peut être propriétaire de sessions et de sessions de paramétrage. |
| Secondaire actif | A/A | Dans une configuration active/active, l'état du pare-feu qui se connecte aux agents User-ID, qui exécute le serveur DHCP et qui met en correspondance les règles NAT et PBF avec l'ID de périphérique du pare-feu actif secondaire. Lorsqu'ils se trouvent à l'état actif secondaire, les pare-feu ne prennent pas en charge le relais DHCP. Lorsqu'il se trouve dans cet état, un pare-feu peut être propriétaire de sessions et de sessions de paramétrage. |
| Provisoire | A/A | État d'un pare-feu (dans une configuration active/active) causé par l'une des situations suivantes :<br>• Échec d'un pare-feu. |

| État des pare-feu HA | Phase à laquelle il survient | Description |
|---|---|---|
| | | • Échec de la surveillance d'un objet (une liaison ou un chemin).<br>• Le pare-feu quitte l'état non fonctionnel ou suspendu.<br>Lorsqu'ils se trouvent à l'état provisoire, les pare-feu synchronisent les sessions et les configurations de l'homologue.<br>• Dans le déploiement d'un câble virtuel, lorsqu'un pare-feu passe à l'état provisoire en raison de l'échec de la surveillance d'un chemin et qu'il reçoit un paquet à transférer, il envoie le paquet au pare-feu homologue via la liaison HD3 pour son traitement. Le pare-feu homologue traite le paquet et le renvoie au pare-feu via la liaison HD3 pour que ce dernier l'envoie hors de l'interface de sortie. Cette façon de faire permet de protéger le chemin de transfert du déploiement de câble virtuel.<br>• Dans un déploiement de Couche 3, lorsqu'un pare-feu à l'état provisoire reçoit un paquet, il l'envoie via la liaison HD3 pour que le pare-feu homologue en soit propriétaire ou qu'il configure la session. Selon la topologie du réseau, ce pare-feu envoie le paquet à sa destination ou le retourne à l'homologue qui se trouve à l'état provisoire pour que ce dernier le transfère.<br>Une fois l'échec du chemin ou de la liaison estompé ou lors de la transition d'un pare-feu ayant fait l'objet d'un échec de l'état provisoire à l'état actif secondaire, le **Tentative Hold Time (Temps d'attente provisoire)** est déclenché et la convergence du routage se produit. Le pare-feu tente de créer une contiguïté de routage et de charger sa table de routage avant de traiter les paquets. Sans ce minuteur, le pare-feu en cours de récupération entrerait immédiatement en état actif-secondaire et rejetterait silencieusement les paquets parce qu'il ne disposerait pas des routes nécessaires.<br>Lorsqu'un pare-feu quitte l'état suspendu, il passe à l'état provisoire pour la durée de **Tentative Hold Time (Temps d'attente provisoire)** après que les liaisons sont actives et capables de traiter les paquets entrants.<br>La **Tentative Hold Time range (sec) (Plage de temps d'attente provisoire (s))** peut être désactivée (elle correspond à 0 seconde), dans la plage 10 à 600 ; la valeur par défaut est 60. |
| Non fonctionnel | A/P ou A/A | État d'erreur causé par un échec dans le panneau de données ou par une non-correspondance de configuration, par exemple, si un seul pare-feu a été configuré pour le transfert des paquets, la synchronisation VR ou la synchronisation QoS. |

| État des pare-feu HA | Phase à laquelle il survient | Description |
|---|---|---|
| | | En mode actif/passif, toutes les raisons justifiant l'état provisoire entraînent le passage à l'état non fonctionnel. |
| Suspended | A/P ou A/A | Le périphérique est désactivé. Il ne transmettra donc par le trafic des données. Et, bien que les communications HA persistent, le périphérique ne participe pas au processus de sélection HA. Il ne peut passer à l'état fonctionnel HA sans l'intervention d'un utilisateur. |

# Référence : Synchronisation de Haute Disponibilité

Si vous avez activé la synchronisation de la configuration sur les deux homologues d'une paire HD, la plupart des paramètres de configuration que vous définissez sur un homologue seront automatiquement synchronisés avec l'autre homologue lors de la validation. Pour éviter des conflits de configuration, apportez toujours des modifications à la configuration sur l'homologue actif (actif/passif) ou actif-principal (actif/actif) et attendez que les modifications soient synchronisées avec l'homologue avant d'effectuer toute modification supplémentaire.

***Dans une paire HD, seules les configurations validées sont synchronisées. Au moment d'une synchronisation HD, toute configuration en attente de validation ne sera pas synchronisée.***

Les rubriques suivantes identifient le type de réglages que vous devez configurer indépendamment sur chaque pare-feu (ces réglages ne sont pas synchronisés avec l'homologue d'une paire HD).

- Paramètres non synchronisés en mode HA active/passive
- Paramètres non synchronisés dans la HA active/active
- Synchronisation des informations d'exécution système

## Paramètres non synchronisés en mode HA active/passive

Vous devez configurer les paramètres suivants sur chaque pare-feu d'une paire HA dans un déploiement actif/passif. Ces paramètres ne sont pas synchronisés d'un homologue à l'autre.

| Élément de configuration | Paramètres non synchronisés en mode HA active/passive |
|---|---|
| Paramètres de l'interface de gestion | Tous les paramètres de configuration de la gestion doivent être définis individuellement sur chaque pare-feu, notamment les suivants :<br>• **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **General Settings (Paramètres généraux)** : nom d'hôte, domaine, bannière de connexion, profil de service SSL/TLS (et les certificats associés), fuseau horaire, paramètres régionaux, date, heure, latitude et longitude.<br>• **Device (Équipement)** > **Setup (Configuration)** > **Management (Gestion)** > **Management Interface Settings (Paramètres de l'interface de gestion)** : Type d'IP, Adresse IP, Masque réseau, Passerelle par défaut, Adresse IPv6/Longueur de préfixe, Passerelle IPv6 par défaut, Vitesse, MTU et Services (HTTP, HTTP OCSP, HTTPS, Telnet, SSH, Ping, SNMP, User-ID, Écouteur SSL Syslog User-ID, Écouteur UDP Syslog User-ID). |
| Fonction de systèmes virtuels multiples | Vous devez activer la licence pour les systèmes virtuels sur chaque pare-feu de la paire pour augmenter le nombre de systèmes virtuels au-delà de la limite de base fournie par défaut sur les pare-feu PA-3200 Series, PA-5200 Series et PA-7000 Series. |

| Élément de configuration | Paramètres non synchronisés en mode HA active/passive |
|---|---|
| | Vous devez également activer l'option **Multi Virtual System Capability (Fonction de systèmes virtuels multiples)** sur chaque pare-feu (**Device (Équipement)** > **Setup (Configuration)** > **Management (Gestion)** > **General Settings (Paramètres généraux)**). |
| Paramètres de Panorama | Définissez les paramètres de Panorama sur chaque pare-feu (**Device (Équipement)** > **Setup (Configuration)** > **Management (Gestion)** > **Panorama Settings (Paramètres de panorama)**).<br>• **Serveurs de Panorama**<br>• **Disable Panorama Policy and Objects (Désactiver la politique et les objets de Panorama)** et **Disable Device and Network Template (Désactiver le modèle de périphérique et réseau)** |
| SNMP | **Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)** > **SNMP Setup (Réglage SNMP)** |
| Services | **Device (Périphérique)** > **Setup (Configuration)** > **Services** |
| Itinéraires de service globaux | **Device (Périphérique)** > **Setup (Configuration)** > **Services** > **Service Route Configuration (Configuration des itinéraires de service)** |
| Paramètres des renseignements télémétriques et sur les menaces | **Device (Périphérique)** > **Setup (Configuration)** > **Telemetry and Threat Intelligence (Renseignements télémétriques et sur les menaces)** |
| Protection des données | **Device (Périphérique)** > **Setup (Configuration)** > **Content-ID (Content-ID)** > **Manage Data Protection (Gérer la protection des données)** |
| Trames Jumbo | **Device (Périphérique)** > **Setup (Configuration)** > **Session (Session)** > **Session Settings (Paramètres de session)** > **Enable Jumbo Frame (Activer les trames Jumbo)** |
| Protection de la mémoire tampon des paquets | **Device (Périphérique)** > **Setup (Configuration)** > **Session** > **Session Settings (Paramètres de session)** > **Packet Buffer Protection (Protection de la mémoire tampon des paquets)**<br>**Network (Réseau)** > **Zones** > **Enable Packet Buffer Protection (Activer la protection de la mémoire tampon des paquets)** |
| Paramètres de certificat du serveur proxy de transfert | **Device (Équipement)** > **Setup (Configuration)** > **Session (Session)** > **Decryption Settings (Paramètres de décryptage)** > **SSL Forward Proxy Settings (Paramètres du proxy de transfert SSL)** |
| Clé principale sécurisée par HSM | **Device (Équipement)** > **Setup (Configuration)** > **HSM (HSM)** > **Hardware Security Module Provider (Fournisseur de module de** |

| Élément de configuration | Paramètres non synchronisés en mode HA active/passive |
|---|---|
| | **sécurité matériel)** > **Master Key Secured by HSM (Clé principale sécurisée par HSM)** |
| Paramètres d'exportation des journaux | **Device (Périphérique)** > **Scheduled Log Export (Exportation programmée des journaux)** |
| Mises à jour logicielles | Vous pouvez télécharger et installer les mises à jour logicielles séparément sur chaque pare-feu, ou les télécharger sur un homologue et les synchroniser avec l'autre homologue. Vous devez installer les mises à jour sur chaque homologue (**Device (Périphérique)** > **Software (Logiciels)**). |
| Mises à jour de l'agent GlobalProtect | Vous pouvez télécharger et installer les mises à jour de l'application GlobalProtect séparément sur chaque pare-feu, ou les télécharger sur un homologue et les synchroniser avec l'autre homologue. Vous devez activer les mises à jour séparément sur chaque homologue (**Device (Périphérique)** > **GlobalProtect Client (Client GlobalProtect)**). |
| Mises à jour du contenu | Vous pouvez télécharger et installer les mises à jour du contenu séparément sur chaque pare-feu, ou les télécharger sur un homologue et les synchroniser avec l'autre homologue. Vous devez installer les mises à jour sur chaque homologue (**Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**). |
| Licences/ Abonnements | **Device (Périphérique)** > **Licenses (Licences)** |
| Abonnement au support | **Device (Périphérique)** > **Support (Support)** |
| Clé principale | La clé principale doit être identique sur chaque pare-feu d'une paire HA, mais vous devez la saisir manuellement sur chaque équipement (**Device (Équipement)** > **Master Key and Diagnostics (Clé principale et diagnostics)**).<br><br>Pour pouvoir modifier la clé principale, vous devez d'abord désactiver la synchronisation de la configuration sur les deux homologues (sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)** > **Setup (Configuration)** et décochez la case **Enable Config Sync (Activer la synchronisation de la configuration)**) puis la réactiver après la modification de la clé. |

| Élément de configuration | Paramètres non synchronisés en mode HA active/passive |
|---|---|
| Paramètres des rapports, des journaux et du tableau de bord | Les données et les paramètres des journaux, des rapports et du tableau de bord (affichage des colonnes, widgets) ne sont pas synchronisés entre les homologues. Toutefois, les paramètres de configuration des rapports sont synchronisés. |
| Paramètres de HD | **Device (Périphérique)** > **High Availability (Haute disponibilité)** |
| Données sur l'utilisation des règles | Les données sur l'utilisation des règles, comme le nombre de correspondances, la date de création et la date de modification ne sont pas synchronisées entre les homologues. Vous devez vous connecter à chaque pare-feu pour afficher les données sur le nombre de correspondance à la règle de politique pour chaque pare-feu ou utiliser Panorama pour afficher les informations sur les homologues HA. |
| Certificats pour la gestion des périphériques et la communication Syslog sur SSL uniquement | **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**<br>Les certificats utilisés pour la gestion des périphériques ou pour la communication syslog sur SSL ne sont pas synchronisés avec un homologue HA. |
| Certificats dans un profil de certificat | **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificat)** |
| Profil de service SSL/TLS pour la gestion des périphériques uniquement | **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **SSL/TLS Service Profile (Profil de service SSL/TLS)**<br>Le profil de service SSL/TLS pour la gestion des périphériques n'est pas synchronisé avec un homologue HA. |
| Device-ID et IoT Security | Les mappages adresse IP/périphérique et les recommandations de règles de politique ne se synchronisent pas avec un homologue HA. |

## Paramètres non synchronisés dans la HA active/active

Vous devez configurer les paramètres suivants sur chaque pare-feu d'une paire HA dans un déploiement HA active/active. Ces paramètres ne sont pas synchronisés d'un homologue à l'autre.

| Élément de configuration | Paramètres non synchronisés en mode HA active/active |
|---|---|
| Paramètres de l'interface de gestion | Vous devez configurer tous les paramètres de gestion individuellement sur chaque pare-feu, dont :<br>• **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **General Settings (Paramètres généraux)** : nom d'hôte, |

| Élément de configuration | Paramètres non synchronisés en mode HA active/active |
|---|---|
| | domaine, bannière de connexion, profil de service SSL/TLS (et les certificats associés), fuseau horaire, paramètres régionaux, date, heure, latitude et longitude.<br>• **Device (Équipement)** > **Setup (Configuration)** > **Management (Gestion)** > **Management Interface Settings (Paramètres de l'interface de gestion)** : Adresse IP, Masque réseau, Passerelle par défaut, Adresse IPv6/Longueur de préfixe, Passerelle IPv6 par défaut, Vitesse, MTU et Services (HTTP, HTTP OCSP, HTTPS, Telnet, SSH, Ping, SNMP, User-ID, Écouteur SSL Syslog User-ID, Écouteur UDP Syslog User-ID). |
| Fonction de systèmes virtuels multiples | Vous devez activer la licence pour les systèmes virtuels sur chaque pare-feu de la paire pour augmenter le nombre de systèmes virtuels au-delà de la limite de base fournie par défaut sur les pare-feu PA-3200 Series, PA-5200 Series et PA-7000 Series.<br>Vous devez également activer l'option **Multi Virtual System Capability (Fonction de systèmes virtuels multiples)** sur chaque pare-feu (**Device (Équipement)** > **Setup (Configuration)** > **Management (Gestion)** > **General Settings (Paramètres généraux)**). |
| Paramètres de Panorama | Définissez les paramètres de Panorama sur chaque pare-feu (**Device (Équipement)** > **Setup (Configuration)** > **Management (Gestion)** > **Panorama Settings (Paramètres de panorama)**).<br>• **Serveurs de Panorama**<br>• **Disable Panorama Policy and Objects (Désactiver la politique et les objets de Panorama)** et **Disable Device and Network Template (Désactiver le modèle de périphérique et réseau)** |
| SNMP | **Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)** > **SNMP Setup (Réglage SNMP)** |
| Services | **Device (Périphérique)** > **Setup (Configuration)** > **Services** |
| Itinéraires de service globaux | **Device (Périphérique)** > **Setup (Configuration)** > **Services** > **Service Route Configuration (Configuration des itinéraires de service)** |
| Paramètres des renseignements télémétriques et sur les menaces | **Device (Périphérique)** > **Setup (Configuration)** > **Telemetry and Threat Intelligence (Renseignements télémétriques et sur les menaces)** |
| Protection des données | **Device (Périphérique)** > **Setup (Configuration)** > **Content-ID (Content-ID)** > **Manage Data Protection (Gérer la protection des données)** |

| Élément de configuration | Paramètres non synchronisés en mode HA active/active |
|---|---|
| Trames Jumbo | **Device (Périphérique)** > **Setup (Configuration)** > **Session (Session)** > **Session Settings (Paramètres de session)** > **Enable Jumbo Frame (Activer les trames Jumbo)** |
| Protection de la mémoire tampon des paquets | **Device (Périphérique)** > **Setup (Configuration)** > **Session** > **Session Settings (Paramètres de session)** > **Packet Buffer Protection (Protection de la mémoire tampon des paquets)**<br>**Network (Réseau)** > **Zones** > **Enable Packet Buffer Protection (Activer la protection de la mémoire tampon des paquets)** |
| Paramètres de certificat du serveur proxy de transfert | **Device (Équipement)** > **Setup (Configuration)** > **Session (Session)** > **Decryption Settings (Paramètres de décryptage)** > **SSL Forward Proxy Settings (Paramètres du proxy de transfert SSL)** |
| Configuration du HSM | **Device (Périphérique)** > **Setup (Configuration)** > **HSM** |
| Paramètres d'exportation des journaux | **Device (Périphérique)** > **Scheduled Log Export (Exportation programmée des journaux)** |
| Mises à jour logicielles | Vous pouvez télécharger et installer les mises à jour logicielles séparément sur chaque pare-feu, ou les télécharger sur un homologue et les synchroniser avec l'autre homologue. Vous devez installer les mises à jour sur chaque homologue (**Device (Périphérique)** > **Software (Logiciels)**). |
| Mises à jour de l'agent GlobalProtect | Vous pouvez télécharger et installer les mises à jour de l'application GlobalProtect séparément sur chaque pare-feu, ou les télécharger sur un homologue et les synchroniser avec l'autre homologue. Vous devez activer les mises à jour séparément sur chaque homologue (**Device (Périphérique)** > **GlobalProtect Client (Client GlobalProtect)**). |
| Mises à jour du contenu | Vous pouvez télécharger et installer les mises à jour du contenu séparément sur chaque pare-feu, ou les télécharger sur un homologue et les synchroniser avec l'autre homologue. Vous devez installer les mises à jour sur chaque homologue (**Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**). |
| Licences/ Abonnements | **Device (Périphérique)** > **Licenses (Licences)** |
| Abonnement au support | **Device (Périphérique)** > **Support (Support)** |

| Élément de configuration | Paramètres non synchronisés en mode HA active/active |
|---|---|
| Adresse IP de l'interface Ethernet | Tous les paramètres de configuration de l'interface Ethernet sont synchronisés excepté l'adresse IP (**Network (Réseau)** > **Interface (Interface)** > **Ethernet (Ethernet)**). |
| Adresse IP de l'interface en boucle | Tous les paramètres de configuration de l'interface en boucle sont synchronisés excepté l'adresse IP (**Network (Réseau)** > **Interface (Interface)** > **Loopback (En boucle)**). |
| Adresse IP de l'interface de tunnel | Tous les paramètres de configuration de l'interface de tunnel sont synchronisés excepté l'adresse IP (**Network (Réseau)** > **Interface (Interface)** > **Tunnel (Tunnel)**). |
| Priorité système LACP | Chaque homologue doit disposer d'un ID système LACP unique dans un déploiement actif/actif (**Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)** > **Add Aggregate Group (Ajouter un groupe agrégé)** > **System Priority (Priorité système)**). |
| Adresse IP de l'interface VLAN | Tous les paramètres de configuration de l'interface VLAN sont synchronisés excepté l'adresse IP (**Network (Réseau)** > **Interface (Interface)** > **VLAN (VLAN)**). |
| Routeurs virtuels | La configuration des routeurs virtuels est synchronisée uniquement si vous avez activé la fonction Synchronisation VR (**Device (Périphérique)** > **High Availability (Haute disponibilité)** > **Active/Active Config (Configuration active/active)** > **Packet Forwarding (Transfert des paquets)**). L'activation de cette fonction dépend de la conception de votre réseau, notamment du routage asymétrique. |
| Tunnels IPSec | La synchronisation de la configuration des tunnels IPsec dépend de l'utilisation d'adresses IP virtuelles flottantes (**Device (Périphérique)** > **High Availability (Haute disponibilité)** > **Active/Active Config (Configuration active/active)** > **Virtual Address (Adresse virtuelle)**). Si vous avez configuré une adresse IP flottante, ces paramètres sont automatiquement synchronisés. Sinon, vous devez configurer ces paramètres indépendamment sur chaque homologue. |
| Portail GlobalProtect | La synchronisation de la configuration des portails GlobalProtect dépend de l'utilisation d'adresses IP virtuelles flottantes (**Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portails (Portals)**). Si vous avez configuré une adresse IP flottante, les paramètres de configuration des portails GlobalProtect sont automatiquement synchronisés. Sinon, vous devez configurer ces paramètres indépendamment sur chaque homologue. |

| Élément de configuration | Paramètres non synchronisés en mode HA active/active |
|---|---|
| Configuration des passerelles GlobalProtect | La synchronisation de la configuration des passerelles GlobalProtect dépend de l'utilisation d'adresses IP virtuelles flottantes (**Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Gateways (Passerelles)**). Si vous avez configuré une adresse IP flottante, les paramètres de configuration des passerelles GlobalProtect sont automatiquement synchronisés. Sinon, vous devez configurer ces paramètres indépendamment sur chaque homologue. |
| QoS | La configuration du QoS est synchronisée uniquement si vous avez activé la fonction **QoS Sync (Synchronisation QoS)** (**Device (Périphérique)** > **High Availability (Haute disponibilité)** > **Active/Active Config (Configuration active/active)** > **Packet Forwarding (Transfert des paquets)**). Vous pouvez choisir de ne pas synchroniser les paramètres QoS si, par exemple, vous disposez de différentes bandes passantes sur chaque liaison ou différentes latences entre vos fournisseurs de services. |
| LLDP | Aucune donnée de pare-feu ni aucun état LLDP n'est synchronisé dans une configuration active/active (**Network (Réseau)** > **Network Profiles (Profils réseau)** > **LLDP (LLDP)**). |
| BFD | Aucune donnée de configuration BFD ou de session BFD n'est synchronisée dans une configuration active/active (**Network (Réseau)** > **Network Profiles (Profils réseau)** > **BFD Profile (Profil BFD)**). |
| Passerelles IKE | La synchronisation de la configuration des passerelles IKE dépend de l'utilisation d'adresses IP virtuelles flottantes (**Network (Réseau)** > **IKE Gateways (Passerelles IKE)**). Si vous avez configuré une adresse IP flottante, les paramètres de configuration des passerelles IKE sont automatiquement synchronisés. Sinon, vous devez configurer ces paramètres indépendamment sur chaque homologue. |
| Clé principale | La clé principale doit être identique sur chaque pare-feu d'une paire HA, mais vous devez la saisir manuellement sur chaque équipement (**Device (Équipement)** > **Master Key and Diagnostics (Clé principale et diagnostics)**).<br><br>Pour pouvoir modifier la clé principale, vous devez d'abord désactiver la synchronisation de la configuration sur les deux homologues (sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)** > **Setup (Configuration)** et décochez la case **Enable Config Sync (Activer la synchronisation de la configuration)**) puis la réactiver après la modification de la clé. |

| Élément de configuration | Paramètres non synchronisés en mode HA active/active |
|---|---|
| Paramètres des rapports, des journaux et du tableau de bord | Les données et les paramètres des journaux, des rapports et du tableau de bord (affichage des colonnes, widgets) ne sont pas synchronisés entre les homologues. Toutefois, les paramètres de configuration des rapports sont synchronisés. |
| Paramètres de HD | • **Device (Périphérique)** > **High Availability (Haute disponibilité)**<br>• (L'exception est **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **Active/Active Configuration (Configuration active/active)** > **Virtual Addresses (Adresses virtuelles)**, qui effectue la synchronisation). |
| Données sur l'utilisation des règles | Les données sur l'utilisation des règles, comme le nombre de correspondances, la date de création et la date de modification ne sont pas synchronisées entre les homologues. Vous devez vous connecter à chaque pare-feu pour afficher les données sur le nombre de correspondance à la règle de politique pour chaque pare-feu ou utiliser Panorama pour afficher les informations sur les homologues HA. |
| Certificats pour la gestion des périphériques et la communication Syslog sur SSL uniquement | **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**<br>Les certificats utilisés pour la gestion des périphériques ou pour la communication syslog sur SSL ne sont pas synchronisés avec un homologue HA. |
| Certificats dans un profil de certificat | **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificat)** |
| Profil de service SSL/TLS pour la gestion des périphériques uniquement | **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **SSL/TLS Service Profile (Profil de service SSL/TLS)**<br>Le profil de service SSL/TLS pour la gestion des périphériques n'est pas synchronisé avec un homologue HA. |
| Device-ID et IoT Security | Les mappages adresse IP/périphérique et les recommandations de règles de politique ne se synchronisent pas avec un homologue HA. |

## Synchronisation des informations d'exécution système

Le tableau suivant résume quelles informations d'exécution système sont synchronisées entre homologues HD.

| Informations d'exécution | Configuration synchronisée ? | | Liaison HD | Détails |
|---|---|---|---|---|
| | A/P | A/A | | |
| **Plan de gestion** | | | | |
| Mappage d'utilisateurs à des groupes | Oui | Oui | HA1 | |
| Mappages d'utilisateurs sur l'ensemble des systèmes virtuels | Oui | Oui | HA1 | |
| Mappage d'utilisateurs à des adresses IP | Oui | Oui | HA1 | |
| Bail DSCP (en tant que serveur) | Oui | Oui | HA1 | Si les versions PAN-OS sur les homologues HA ne correspondent pas, les informations de configuration du bail DHCP (en tant que serveur) ne seront pas synchronisées. |
| Cache DNS | Non | Non | S. O. | |
| Actualisation du FQDN | Non | Non | S. O. | |
| Clés IKE (phase 2) | Oui | Oui | HA1 | |
| Forward Information Base (FIB) (Base d'informations de transfert (FIB)) | Oui | Oui | HA1 | |
| Cache d'URL PAN-DB | Oui | Non | HA1 | Cette fonctionnalité est synchronisée lors de la sauvegarde de la base de données sur le disque (toutes les huit heures, lors de la mise à jour de la version de la base de données d'URL) ou au redémarrage du pare-feu. |
| Contenu (synchronisation manuelle) | Oui | Oui | HA1 | |

| Informations d'exécution | Configuration synchronisée ? | | Liaison HD | Détails |
|---|---|---|---|---|
| | A/P | A/A | | |
| PPPoE, bail PPPoE | Oui | Oui | HA1 | |
| Bail et paramètres du client DHCP | Oui | Oui | HA1 | Si les versions PAN-OS sur les homologues HA ne correspondent pas, les informations de configuration du bail et des paramètres du client DHCP ne seront pas synchronisées. |
| SSL VPN Logged in User List (Liste des utilisateurs connectés au VPN SSL) | Oui | Oui | HA1 | |
| **Panneau de données** | | | | |
| Table de sessions | Oui | Oui | HD2 | • Les homologues actif/passif ne synchronisent pas les informations ICMP ou de session hôte.<br>• Les homologues actif/actif ne synchronisent pas les informations de |

| Informations d'exécution | Configuration synchronisée ? | | Liaison HD | Détails |
|---|---|---|---|---|
| | A/P | A/A | | |
| | | | | session hôte, multicast ou BFD.<br><br>*Une session hôte est une session qui se termine sur l'une des interfaces du pare-feu, comme une session ICMP qui lance un ping sur l'une des interfaces du pare-feu ou un tunnel GP.* |
| Table ARP | Oui | Non | HD2 | |
| Neighbor Discovery (ND) Table (Table Neighbor Discovery (détection de voisins - ND)) | Oui | Non | HD2 | |
| MAC Table (Table MAC) | Oui | Non | HD2 | |
| Numéro de séquence IPSec (anti-relecture) | Oui | Oui | HD2 | |
| Listes d'interdiction DoS | Non | Non | S. O. | |
| Adresse MAC virtuelle | Oui | Oui | HD2 | |

| Informations d'exécution | Configuration synchronisée ? | | Liaison HD | Détails |
|---|---|---|---|---|
| | A/P | A/A | | |
| Associations SCTP | Oui | Non | HD2 | |

# Surveillance

Pour anticiper les éventuels problèmes et accélérer la réponse aux incidents lorsque cela est nécessaire, le pare-feu fournit une intelligence sur les modèles de trafic et utilisateur ainsi que des rapports personnalisés et instructifs. Le tableau de bord, l'Application Command Center (Centre de commande des applications ; ACC), les rapports et les journaux sur le pare-feu vous permettent de surveiller l'activité sur votre réseau. Vous pouvez contrôler les journaux et filtrer les informations afin de générer des rapports avec des vues prédéfinies ou personnalisées. Par exemple, utiliser les modèles prédéfinis pour générer des rapports sur les activités d'un utilisateur ou analyser les rapports et les journaux afin d'interpréter un comportement inhabituel sur votre réseau et générer un rapport personnalisé sur le modèle de trafic. Pour une présentation visuelle utile de l'activité réseau, le tableau de bord et l'ACC incluent des widgets, des graphiques et des tableaux avec lesquels vous pouvez interagir pour retrouver les informations dont vous avez besoin. Vous pouvez également configurer le pare-feu pour transférer les informations surveillées en tant que notifications par e-mail, messages Syslog messages, pièges SNMP et enregistrements NetFlow à des services externes.

# Utilisation du tableau de bord

Les widgets de l'onglet **Dashboard (Tableau de bord)** affichent des informations générales concernant un pare-feu, comme la version du logiciel, l'état opérationnel de chaque interface, l'utilisation des ressources et jusqu'à 10 des entrées les plus récentes des journaux des menaces, de configuration et système. Tous les widgets disponibles s'affichent par défaut, mais chaque administrateur peut supprimer et ajouter des widgets individuels, le cas échéant. Cliquez sur l'icône d'actualisation pour mettre à jour le tableau de bord ou un widget. Pour modifier l'intervalle d'actualisation automatique, sélectionnez un intervalle dans la liste déroulante (**1 min**, **2 min**, **5 min** ou **Manual (Manuel)**). Pour ajouter un widget au tableau de bord, cliquez sur la liste déroulante Widget, sélectionnez une catégorie, puis le nom du widget. Pour supprimer un widget, cliquez sur dans la barre de titre. Le tableau suivant décrit les widgets du Tableau de bord.

| Diagrammes du tableau de bord | Descriptions |
|---|---|
| Applications principales | Affiche les applications ayant le plus grand nombre de sessions. La taille du bloc indique le nombre relatif de sessions (passez la souris sur le bloc pour afficher le nombre correspondant) et la couleur indique les risques de sécurité, vert pour des risques faibles et rouge pour des risques élevés. Cliquez sur une application pour afficher son profil d'application. |
| Applications principales à haut risque | Identique à Principales applications, sauf que les applications présentant les risques les plus élevés avec la plupart des sessions sont affichées. |
| Informations générales | Affiche le nom du pare-feu, le modèle, la version du logiciel PAN-OS, l'application, la menace et les versions de définition du filtrage des URL, la date et l'heure actuelles, ainsi que le temps écoulé depuis le dernier redémarrage. |
| État de l'interface | Indique si chaque interface est active (vert), inactive (rouge) ou si son état est inconnu (gris). |
| Journaux des menaces | Affiche l'ID de menace, l'application, ainsi que la date et l'heure des 10 dernières entrées du journal des menaces. L'ID de menace correspond à la description ou à l'URL d'un site malveillant qui va à l'encontre du profil de filtrage des URL. |
| Journaux de configuration | Affiche le nom d'utilisateur de l'administrateur, le client (Web ou CLI), ainsi que la date et l'heure des 10 dernières entrées du journal de configuration. |
| Journaux de filtrage des données | Affiche la description, ainsi que la date et l'heure des 60 dernières minutes du journal de filtrage des données. |

| Diagrammes du tableau de bord | Descriptions |
|---|---|
| Journaux de filtrage des URL | Affiche la description, ainsi que la date et l'heure des 60 dernières minutes du journal de filtrage des URL. |
| Journaux systèmes | Affiche la description, ainsi que la date et l'heure des 10 dernières entrées du journal système.<br><br>*Notez qu'une entrée **`Config installed`** indique que les modifications apportées à la configuration ont été correctement validées.* |
| Ressources systèmes | Affiche la gestion de l'utilisation du processeur, l'utilisation du plan de données et le nombre de sessions qui regroupe le nombre de sessions établies via le pare-feu. |
| Administrateurs connectés | Affiche l'adresse IP source, le type de session (Web ou CLI) et l'heure de début de session pour chaque administrateur actuellement connecté. |
| Facteur de risque de ACC | Affiche le facteur de risque moyen (entre 1 et 5) du trafic réseau traité au cours de la semaine passée. Plus la valeur est élevée, plus le risque est important. |
| Haute disponibilité | Si la High Availability (haute disponibilité ; HA) est activée, indique l'état HA du pare-feu local et homologue : vert (actif), jaune (passif) ou noir (autre). Pour plus d'informations sur la HA, reportez-vous à la section Haute disponibilité. |
| Verrous | Affiche les verrous de configuration utilisés par les administrateurs. |

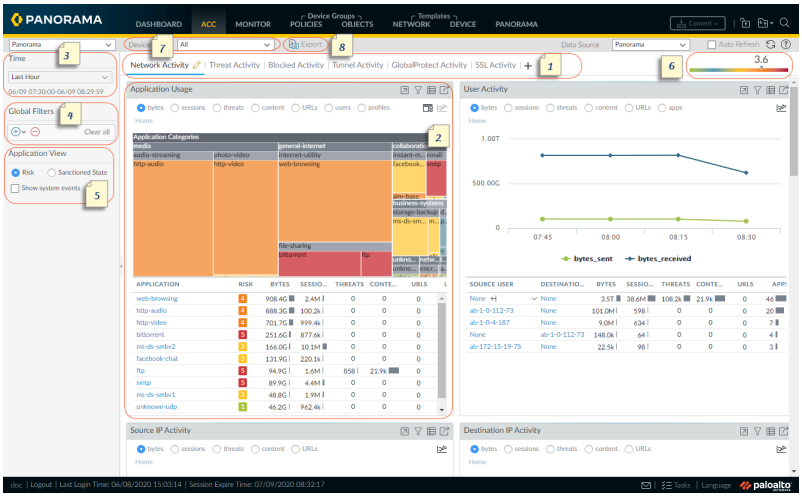
# Utilisation de l'Application Command Center (centre de commande de l'application - ACC)

L'Application Command Center (centre de commande de l'application ; ACC) offre un récapitulatif graphique et interactif des applications, utilisateurs, URL, menaces et du contenu qui traversent votre réseau. L'ACC utilise les journaux du pare-feu pour offrir une visibilité sur les modèles de trafic et les informations pratiques relatives aux menaces. La présentation de l'ACC inclut une vue à onglets de l'activité du réseau, des menaces et bloquée, et chaque onglet inclut des widgets utiles pour une meilleure visibilité sur le trafic réseau. Cette représentation graphique vous permet d'interagir avec les données et de visualiser les relations entre les événements sur le réseau, vous permettant ainsi d'identifier les anomalies ou de trouver des améliorations à apporter à vos règles de sécurité réseau. Pour disposer d'une vue personnalisée sur votre réseau, vous pouvez également ajouter un onglet personnalisé et inclure des widgets qui vous permettent d'accéder aux informations qui vous sont utiles.

- Aperçu de l'ACC
- Onglets de l'ACC
- Widgets de l'ACC (Description des widgets)
- Filtres de l'ACC
- Interaction avec l'ACC
- Cas d'utilisation : ACC — Chemin détection d'informations

## Aperçu de l'ACC

Découvrez l'ACC.




| Aperçu de l'ACC | | |
|---|---|---|
| 1 | **Onglets** | L'ACC inclut trois onglets prédéfinis qui fournissent une visibilité du trafic réseau, de l'activité des menaces et de l'activité bloquée. Pour plus |

| Aperçu de l'ACC | | |
|---|---|---|
| | | d'informations sur chaque onglet, reportez-vous à la sectionOnglets ACC. |
|  | **Widgets (Widgets)** | Chaque onglet inclut un ensemble de widgets par défaut qui représentent le mieux les événements/ tendances associé(e)s à l'onglet. Les widgets vous permettent d'étudier les données à l'aide des filtres suivants :<br>• octets (en entrée et sortie)<br>• sessions<br>• contenu (fichiers et données)<br>• URL Category (Catégorie d'URL)<br>• menaces (et nombre)<br>Pour plus d'informations sur chaque widget, reportez-vous à la sectionWidgets ACC. |
|  | **Période** | Les diagrammes ou graphiques de chaque widget fournissent un résumé et un historique. Vous pouvez choisir un intervalle personnalisé ou utiliser une période prédéfinie, allant des 15 dernières minutes aux 90 derniers jours ou aux 30 derniers jours calendaires. La période sélectionnée s'applique à tous les onglets de l'ACC.<br>La période utilisée pour effectuer le rendu des données est, par défaut, la**Last Hour (Dernière heure)**, mise à jour toutes les 15 minutes. L'intervalle de date et d'heure s'affiche à l'écran, par exemple à 11h40, la plage horaire est 01/12 10:30:00-01/12 11:29:59. |
|  | **Filtres Globaux** | Les filtres généraux vous permettent de définir un filtre pour tous les widgets et tous les onglets. Les diagrammes/graphiques appliquent les filtres sélectionnés avant d'effectuer le rendu des données. Pour plus d'informations sur l'utilisation des filtres, reportez-vous à la sectionFiltres ACC. |
|  | Affichage des applications par | L'affichage de l'application vous permet de filtrer la vue ACC soit par les applications approuvées et non approuvées utilisées sur votre réseau, soit par le niveau de risque des applications utilisées sur votre réseau. Le vert indique les applications approuvées, le bleu, les applications non approuvées et le jaune, les applications partiellement approuvées. Les applications partiellement approuvées sont celles |

| Aperçu de l'ACC | | |
|---|---|---|
| | | dont l'état d'approbation est variable ; c'est-à-dire que l'application est identifiée comme étant approuvée de façon incohérente, par exemple, il se peut qu'elle soit approuvée sur un ou plusieurs systèmes virtuels d'un pare-feu comportant plusieurs systèmes virtuels ou sur un ou plusieurs pare-feu d'un groupe de périphériques installés sur Panorama. |
|  | **Risk Factor (Facteur de risque)** | Le facteur de risque (1 = risque le plus faible à 5 = risque le plus élevé) indique le risque relatif basé en fonction des applications utilisées sur votre réseau. Le facteur de risque utilise différents facteurs pour évaluer les niveaux de risque associés, tels que si l'application peut partager des fichiers, si elle est susceptible d'être utilisée de manière inappropriée ou si elle tente de quitter les pare-feu, ainsi que des facteurs liés à l'activité des menaces et les logiciels malveillants via le nombre de menaces bloquées, les hôtes compromis ou le trafic vers les hôtes/domaines malveillants. |
|  | **Source** | Les données utilisées pour l'affichage ACC. Les options sont différentes sur le pare-feu et sur Panorama.<br><br>Sur le pare-feu, si celui-ci prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, vous pouvez utiliser la liste déroulante**Virtual System (Système virtuel)** pour modifier l'affichage de l'ACC de manière à inclure les données provenant de tous les systèmes virtuels ou uniquement d'un système virtuel sélectionné.<br><br>Sur Panorama, vous pouvez sélectionner le menu déroulant**Device Group (Groupe de périphériques)** pour modifier l'affichage ACC pour inclure des données provenant de tous les groupes de périphériques ou uniquement d'une sélection de groupes de périphériques.<br><br>De plus, sur Panorama, vous pouvez modifier la**Data Source (Source de données)** en tant que données**Panorama (Panorama)** ou**Remote Device Data (Données du périphérique distant)**.**Remote Device Data (Données du périphérique distant)** n'est disponible que si tous les pare-feu gérés sont sur PAN-OS 7.0.0 ou version ultérieure. |

| Aperçu de l'ACC | | |
|---|---|---|
| | | Lorsque vous filtrez l'affichage pour un groupe de périphériques spécifique, les données**Panorama (Panorama)** sont utilisées comme source de données**.** |
|  | **Export (Exporter)** | Vous pouvez exporter les widgets affichés dans l'onglet actuellement sélectionné au format PDF. Le fichier PDF est téléchargé et enregistré dans le dossier de téléchargements associé à votre navigateur Web, sur votre ordinateur. |

## Onglets de l'ACC

L'ACC inclut les onglets prédéfinis suivants pour l'affichage de l'activité du réseau, l'activité des menaces et l'activité bloquée.

| Onglet | Description |
|---|---|
| **Network Activity (Activité du réseau)** | Affiche une vue d'ensemble du trafic et de l'activité des utilisateurs sur votre réseau, notamment :<br>• Principales applications utilisées<br>• Principaux utilisateurs qui génèrent du trafic (en examinant le nombre d'octets, le contenu, les menaces ou les URL consultées par les utilisateurs)<br>• Règles de sécurité les plus utilisées par rapport auxquelles des correspondances de trafic sont détectées<br>De plus, vous pouvez également afficher l'activité réseau par zone source ou de destination, région, adresse IP, interface d'entrée ou de sortie et par information sur l'hôte GlobalProtect, notamment les systèmes d'exploitation des périphériques les plus couramment utilisés sur le réseau. |
| **Threat Activity (Activité des menaces)** | Affiche une vue d'ensemble des menaces sur le réseau, en se concentrant sur les principales menaces : vulnérabilités, logiciels espions, virus, hôtes visitant des domaines ou URL malveillants, principaux envois WildFire par type de fichier et application, et applications qui utilisent des ports non standard. Le widget Hôtes compromis de cet onglet (pris en charge sur certaines plates-formes uniquement) complète la détection avec de meilleures techniques de visualisation ; il utilise les informations de l'onglet Correlated Events (Événements corrélés) (**Automated Correlation Engine (Moteur de corrélation automatique)** > **Correlated Events (Événements corrélés)** pour présenter une vue agrégée des hôtes compromis sur |

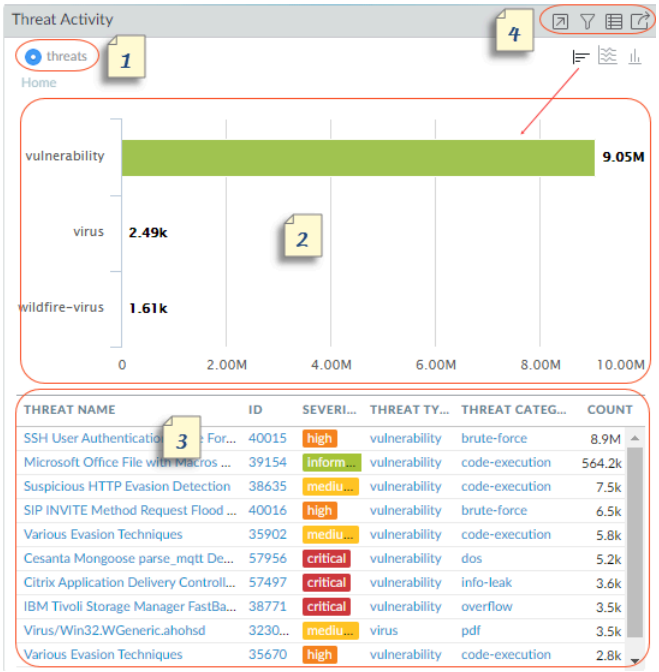
| Onglet | Description |
| --- | --- |
| | votre réseau par utilisateurs/adresses IP source et triés par niveau de gravité. |
| **Blocked Activity (Activité bloquée)** | Se concentre sur le trafic qui a été empêché d'entrer sur le réseau. Les widgets de cet onglet vous permettent d'afficher l'activité refusée par nom d'application, nom d'utilisateur, nom de menace, contenu bloqué (fichiers et données bloqués par un profil de blocage des fichiers). Il dresse également la liste des principales règles de sécurité mises en correspondance pour bloquer les menaces, le contenu et les URL. |
| **Activités des tunnels** | Affiche l'activité du trafic du tunnel que le pare-feu a inspecté en fonction de vos politiques d'inspection du tunnel. Les informations incluent l'utilisation du tunnel en fonction de l'ID de tunnel, de la balise de surveillance, de l'utilisateur et des protocoles de tunnel tels que l'Encapsulation générique de routage (GRE), le Protocole de tunnel de type GPRS (General Packet Radio Service) pour les Données utilisateur (GTP-U) et le protocole IPSec non crypté. |
| **Activité GlobalProtect** | Affiche une vue d'ensemble de l'activité des utilisateurs de votre déploiement GlobalProtect. Les informations incluent le nombre d'utilisateurs et le nombre de fois que les utilisateurs se sont connectés, les passerelles auxquelles les utilisateurs se sont connectés, le nombre d'échecs de connexion ainsi que la raison de l'échec, un récapitulatif des méthodes d'authentification et les versions de l'application GlobalProtect utilisées, ainsi que le nombre de postes en quarantaine.<br><br>En outre, cet onglet affiche une vue graphique récapitulative des périphériques qui ont été mis en quarantaine. Utilisez le bouton en haut du tableau pour afficher les périphériques mis en quarantaine selon les actions qui ont amené GlobalProtect à mettre le périphérique en quarantaine, la raison pour laquelle GlobalProtect a mis le périphérique en quarantaine et l'emplacement des périphériques mis en quarantaine. |
| **Activité SSL** | Affiche une présentation de l'activité de décryptage TLS/SSL sur le pare-feu. Les informations comprennent les activités de décryptage réussies ou non dans votre réseau, les raisons des échecs de décryptage telles que les problèmes de protocole, de certificat et de version, les versions TLS, les algorithmes d'échange de clés, ainsi que la quantité et le type de trafic décrypté et non décrypté.<br><br>Utilisez les informations ACC pour évaluer le fonctionnement du décryptage sur votre réseau, puis utilisez le Journal de décryptage pour approfondir les détails. |

Une Interaction avec l'ACC est également possible pour créer des onglets personnalisés avec une présentation et des widgets personnalisés qui répondent à vos besoins de surveillance du réseau ainsi que pour exporter l'onglet et le partager avec un autre administrateur.

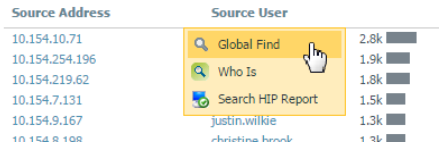
# Widgets de l'ACC

Les widgets de chaque onglet sont interactifs ; vous pouvez définir leswidgets de l'ACC et accéder aux informations de chaque tableau ou graphique, ou personnaliser les widgets de l'onglet pour vous concentrer sur celles dont vous avez réellement besoin. Pour plus d'informations sur l'affichage de chaque widget, reportez-vous à la sectionDescription des widgets.




| Widgets (Widgets) | | |
|---|---|---|
| 1 | **Vue** | Vous pouvez trier les données par nombre d'octets, session, menace, nombre, contenu, URL, caractère malveillant, bénin, fichier, application, donnée, profil, objet ou utilisateur. Les options disponibles varient selon le widget. |
| 2 | **Graphique** | Les options d'affichage graphique sont treemap, graphique linéaire, graphique à barres horizontales, graphique à aires empilées, graphique à barres empilées et carte. Les options disponibles varient selon le widget ; l'interactivité varie également selon le type de graphique. Par exemple, le widget Applications utilisant des ports non standard vous permet de choisir entre une treemap et un graphique linéaire. |

| Widgets (Widgets) | | |
|---|---|---|
| | | Pour obtenir un affichage détaillé, cliquez sur le graphique. La zone sur laquelle vous cliquez devient un filtre et vous permet de faire un zoom avant sur la sélection et d'afficher des informations plus granulaires sur la sélection. |
| 3 | **Table** | La vue détaillée des données utilisées pour effectuer un rendu du graphique est fournie dans une table sous le graphique. Vous pouvez interagir avec la table de différentes manières :<br>• Cliquez et définissez un filtre local pour un attribut de la table. Le graphique est mis à jour et la table est triée à l'aide du filtre local. Les informations affichées dans le graphique et la table sont toujours synchronisées.<br>• Pointez avec la souris l'attribut dans la table et utilisez les options disponibles dans la liste déroulante.<br>  |
| 4 | **Actions** | **Agrandir la vue** : vous permet d'agrandir le widget et d'afficher la table dans un espace plus grand à l'écran et avec plus d'informations.<br>**Configurer les filtres locaux** : vous permet d'ajouter desfiltres de l'ACC pour préciser l'affichage dans le widget. Utilisez ces filtres pour personnaliser les widgets ; ces personnalisations sont conservées entre les connexions.<br>**Accéder aux journaux** : vous permet d'accéder directement aux journaux (ongletMonitor (Surveillance) > Logs (Journaux) > <log-type (<type de journal)). Les journaux sont filtrés selon la période pour laquelle le rendu du graphique est effectué.<br>Si vous avez défini des filtres locaux et généraux, la requête de journal concatène la période et les filtres, puis affiche uniquement les journaux qui correspondent à l'ensemble de filtres combinés |

| Widgets (Widgets) | | |
|---|---|---|
| | | **Exporter** : vous permet d'exporter le graphique au format PDF. Le fichier PDF est téléchargé et enregistré sur votre ordinateur. Il est enregistré dans le dossier Téléchargements associé à votre navigateur Web. |

## Description des widgets

Chaque onglet de l'ACC inclut un ensemble de widgets différent.

| Widget | Description |
|---|---|
| **Network Activity (Activité du réseau)** – Affiche une vue d'ensemble du trafic et de l'activité des utilisateurs sur votre réseau. | |
| **Utilisation de l'application** | Le tableau affiche les 10 principales applications utilisées sur votre réseau, toutes les autres applications utilisées sur le réseau sont agrégées et affichées séparément. Le graphique affiche toutes les applications par catégorie d'applications, sous-catégorie et application. Utilisez ce widget pour retrouver les applications utilisées sur le réseau. Il vous indique les applications prédominantes par bande passante, nombre de sessions, transfert de fichiers, déclenchement le plus de menaces et accès aux URL.<br>Attributs de tri : octets, sessions, menaces, contenu, URL<br>Graphiques disponibles : treemap, aires, colonnes, lignes (les graphiques varient selon l'attribut de tri sélectionné) |
| **Activité utilisateurs** | Affiche les 10 principaux utilisateurs les plus actifs sur le réseau qui ont généré le plus de volume de trafic et utilisé le plus de ressources réseau pour obtenir du contenu. Utilisez ce widget pour surveiller les principaux utilisateurs par utilisation, triés par octets, sessions, menaces, contenu (fichiers et modèles), et URL consultées.<br>Attributs de tri : octets, sessions, menaces, contenu, URL<br>Graphiques disponibles : aires, colonnes, lignes (les graphiques varient selon l'attribut de tri sélectionné) |
| **Activité des IP source** | Affiche les 10 principales adresses IP ou noms d'hôtes des périphériques à l'origine de l'activité sur le réseau. Tous les autres périphériques sont agrégés et affichés séparément.<br>Attributs de tri : octets, sessions, menaces, contenu, URL<br>Graphiques disponibles : aires, colonnes, lignes (les graphiques varient selon l'attribut de tri sélectionné) |

| Widget | Description |
|---|---|
| **Activité des IP de destination** | Affiche les adresses IP ou noms d'hôtes des 10 principales destinations consultées par les utilisateurs sur le réseau.<br>Attributs de tri : octets, sessions, menaces, contenu, URL<br>Graphiques disponibles : aires, colonnes, lignes (les graphiques varient selon l'attribut de tri sélectionné) |
| **Source Regions (Régions source)** | Affiche les 10 principales régions (intégrées ou personnalisées) du monde d'origine des utilisateurs de l'activité sur le réseau.<br>Attributs de tri : octets, sessions, menaces, contenu, URL<br>Graphiques disponibles : carte, barres |
| **Destination Regions (Régions de destination)** | Affiche les 10 principales régions de destination (intégrées ou personnalisées) de la carte du monde d'origine d'accès au contenu par les utilisateurs sur le réseau.<br>Attributs de tri : octets, sessions, menaces, contenu, URL<br>Graphiques disponibles : carte, barres |
| **GlobalProtect Host Information (Informations sur l'hôte GlobalProtect)** | Affiche des informations sur l'état des hôtes sur lesquels l'agent GlobalProtect est exécuté ; le système hôte est un point de terminaison GlobalProtect. Ces informations proviennent d'entrées du journal de correspondance HIP générées lorsque les données envoyées par l'application GlobalProtect correspondent à un objet HIP ou à un profil HIP que vous avez défini sur le pare-feu. Si vous ne disposez d'aucun journal de correspondance HIP, ce widget est vide. Pour savoir comment créer des objets et profils HIP et les utiliser comme critères de correspondance de politique, reportez-vous à la section Configuration de la mise en œuvre de politiques basées sur HIP.<br>Attributs de tri : profils, objets, systèmes d'exploitation<br>Graphiques disponibles : barres |
| **Rule Usage (Utilisation d'une règle)** | Affiche les 10 principales règles qui ont autorisé la plupart du trafic sur le réseau. Utilisez ce widget pour afficher les règles les plus fréquemment utilisées, surveiller les modèles d'utilisation et pour déterminer si les règles protègent efficacement votre réseau.<br>Attributs de tri : octets, sessions, menaces, contenu, URL<br>Graphiques disponibles : lignes |
| **Ingress Interfaces (Interfaces d'entrée)** | Affiche les interfaces de pare-feu qui sont les plus utilisées pour autoriser le trafic sur le réseau.<br>Attributs de tri : octets, octets envoyés, octets reçus<br>Graphiques disponibles : lignes |

| Widget | Description |
|---|---|
| **Egress Interfaces (Interfaces de sortie)** | Affiche les interfaces de pare-feu qui sont les plus utilisées par le trafic quittant le réseau.<br>Attributs de tri : octets, octets envoyés, octets reçus<br>Graphiques disponibles : lignes |
| **Source Zones (Zones source)** | Affiche les zones les plus utilisées pour autoriser le trafic sur le réseau.<br>Attributs de tri : octets, sessions, menaces, contenu, URL<br>Graphiques disponibles : lignes |
| **Destination Zones (Zones de destination)** | Affiche les zones les plus utilisées par trafic sortant du réseau.<br>Attributs de tri : octets, sessions, menaces, contenu, URL<br>Graphiques disponibles : lignes |
| **Threat Activity (Activité des menaces)** : affiche une vue d'ensemble des menaces sur le réseau. | |
| **Compromised Hosts (Hôtes compromis)** | Affiche les hôtes susceptibles d'être compromis sur votre réseau. Ce widget récapitule les événements des journaux de corrélation. Pour chaque utilisateur/adresse IP source, il indique l'objet de corrélation à l'origine de la correspondance, ainsi que le nombre de correspondances agrégé à partir de la preuve de correspondance recueillie dans les journaux des événements corrélés. Pour plus de précisions, reportez-vous à la section Utilisation du moteur de corrélation automatique.<br>Disponible sur les pare-feu PA-5200 Series, PA-7000 Series et sur Panorama.<br>Attributs de tri : gravité (par défaut) |
| **Hosts Visiting Malicious URLs (Hôtes consultant des URL malveillantes)** | Affiche la fréquence à laquelle des hôtes (adresses IP/noms d'hôtes) sur votre réseau ont consulté des URL malveillantes. Ces URL sont connues pour être malveillantes en fonction d'une catégorisation dans PAN-DB.<br>Attributs de tri : nombre<br>Graphiques disponibles : lignes |
| **Hôtes résolvant des domaines malveillants** | Affiche les principaux hôtes correspondant à des signatures DNS ; les hôtes sur le réseau qui tentent de résoudre le nom d'hôte ou le domaine d'une URL malveillante. Ces informations sont collectées dans une analyse de l'activité DNS sur votre réseau. Il utilise la surveillance DNS passive, le trafic DNS généré sur le réseau, l'activité visible dans le sandbox si vous avez configuré un entonnoir DNS sur le pare-feu, et les rapports DNS sur les sources DNS malveillantes accessibles aux clients Palo Alto Networks.<br>Attributs de tri : nombre |

| Widget | Description |
|---|---|
| | Graphiques disponibles : lignes |
| **Threat Activity (Activité des menaces)** | Affiche les menaces détectées sur votre réseau. Ces informations sont basées sur des correspondances de signatures dans les profils Antivirus, Antispyware et Protection contre les vulnérabilités et les virus signalés par WildFire.<br>Attributs de tri : menaces<br>Graphiques disponibles : barres, aires, colonnes |
| **WildFire Activity by Application (Activité WildFire par application)** | Affiche les applications ayant généré le plus grand nombre d'envois WildFire. Ce widget utilise le verdict malveillant ou bénin du journal d'envois WildFire.<br>Attributs de tri : malveillant, bénin<br>Graphiques disponibles : barres, lignes |
| **WildFire Activity by File Type (Activité WildFire par type de fichier)** | Affiche le vecteur de menace par type de fichier. Ce widget affiche les types de fichiers qui ont généré le plus d'envois WildFire et utilise le verdict malveillant ou bénin du journal d'envois WildFire. Si ces données ne sont pas disponibles, le widget est vide.<br>Attributs de tri : malveillant, bénin<br>Graphiques disponibles : barres, lignes |
| **Applications utilisant des ports non standard** | Affiche les applications qui sont entrées sur votre réseau via des ports non standard. Si vous avez migré vos règles de pare-feu d'un pare-feu basé sur le port, utilisez ces informations pour créer des règles de politique autorisant le trafic sur le port par défaut de l'application uniquement. Si nécessaire, créez une exception pour autoriser le trafic sur un port non standard ou créez une application personnalisée.<br>Attributs de tri : octets, sessions, menaces, contenu, URL<br>Graphiques disponibles : treemap, lignes |
| **Rules Allowing Applications On Non Standard Ports (Règles autorisant les applications sur les ports non standard)** | Affiche les règles de politique de sécurité qui ont autorisé des applications sur des ports non par défaut. Le graphique affiche toutes les règles, alors que le tableau affiche les 10 principales règles et agrège les données des autres règles séparément.<br>Ces informations vous permettent d'identifier les failles de sécurité du réseau en vous permettant d'évaluer si une application ignore des ports ou en évite sur votre réseau. Par exemple, vous pouvez vérifier que vous disposez d'une règle autorisant le trafic sur n'importe quel port à l'exception du port par défaut de l'application. Supposons, par exemple, que vous disposez d'une règle autorisant le trafic DNS sur le port ***application-default*** (le port 53 est le port standard pour DNS). Ce |

| Widget | Description |
|---|---|
| | widget affichera toute règle autorisant le trafic DNS sur votre réseau sur n'importe quel port sauf le port 53.<br>Attributs de tri : octets, sessions, menaces, contenu, URL<br>Graphiques disponibles : treemap, lignes |
| **Blocked Activity (Activité bloquée)** : se concentre sur le trafic qui a été empêché d'entrer sur le réseau. | |
| **Activité des applications bloquées** | Affiche les applications qui ont été refusées sur votre réseau, et vous permet d'afficher les menaces, le contenu et les URL maintenus en dehors de votre réseau.<br>Attributs de tri : menaces, contenu, URL<br>Graphiques disponibles : treemap, aires, colonnes |
| **Activités de l'utilisateur bloquées** | Affiche les requêtes utilisateurs qui ont été bloquées par une correspondance avec un profil antivirus, antispyware, de blocage des fichiers ou de filtrage des URL associé à une règle de politique de sécurité.<br>Attributs de tri : menaces, contenu, URL<br>Graphiques disponibles : barres, aires, colonnes |
| **Blocked Threats (Menaces bloquées)** | Affiche les menaces qui ont été correctement refusées sur votre réseau. Ces menaces correspondaient à des signatures antivirus, des signatures de vulnérabilités et des signatures DNS disponibles via les mises à jour du contenu dynamiques sur le pare-feu.<br>Attributs de tri : menaces<br>Graphiques disponibles : barres, aires, colonnes |
| **Blocked Content (Contenu bloqué)** | Affiche les fichiers et données qui ont été empêchés d'entrer sur le réseau. Le contenu a été bloqué car une politique de sécurité a refusé l'accès en fonction de critères définis dans un profil de sécurité de blocage des fichiers ou de filtrage des données.<br>Attributs de tri : fichiers, données<br>Graphiques disponibles : barres, aires, colonnes |
| **Security Policies Blocking Activity (Politiques de sécurité bloquant l'activité)** | Affiche les règles de politique de sécurité qui ont bloqué ou limité du trafic sur votre réseau. Ce widget affichant les menaces, le contenu et les URL dont l'accès a été refusé sur votre réseau, vous pouvez l'utiliser pour évaluer l'efficacité de vos règles de politique. Ce widget n'affiche pas le trafic bloqué en raison de règles de refus que vous avez définies dans une politique.<br>Attributs de tri : menaces, contenu, URL |

| Widget | Description |
|---|---|
| | Graphiques disponibles : barres, aires, colonnes |
| **Activité GlobalProtect** – Affiche des informations sur l'activité des utilisateurs de votre déploiement GlobalProtect. | |
| **Réussite de l'activité de connexion à GlobalProtect** | Affiche un tableau des activités de connexion à GlobalProtect qui ont réussi sur la période de temps sélectionnée. Utilisez la touche à bascule qui se trouve au haut du tableau pour faire basculer les statistiques de connexion selon les utilisateurs, les portails et les passerelles et l'emplacement.<br>Triez les attributs : utilisateurs, portails/passerelles, emplacement<br>Graphiques disponibles : barres, lignes |
| **Échec de l'activité de connexion à GlobalProtect** | Affiche un tableau des activités de connexion à GlobalProtect qui ont échoué sur la période de temps sélectionnée. Utilisez la touche à bascule qui se trouve au haut du tableau pour faire basculer les statistiques de connexion selon les utilisateurs, les portails et les passerelles et l'emplacement. Pour vous aider à identifier et à résoudre les problèmes de connexion, vous pouvez également afficher le tableau ou le graphique des motifs. Pour ce tableau, l'ACC indique l'erreur, l'utilisateur source, l'adresse IP publique et les autres informations qui vous aident à identifier et à résoudre le problème rapidement.<br>Triez les attributs : utilisateurs, portails/passerelles, motifs, emplacement<br>Graphiques disponibles : barres, lignes |
| **Activité de déploiement GlobalProtect** | Affiche un tableau récapitulatif de votre déploiement. Utilisez la touche à bascule au haut du tableau pour consulter la distribution des utilisateurs par méthode d'authentification, la version de l'application GlobalProtect et la version du système d'exploitation.<br>Triez les attributs : méthode d'authentification, la version de l'application globalprotect, le système d'exploitation<br>Graphiques disponibles : barres, lignes |
| **Activité de quarantaine GlobalProtect** | Affiche une vue graphique récapitulative des périphériques qui ont été mis en quarantaine. Utilisez le bouton en haut du tableau pour afficher les périphériques mis en quarantaine selon les actions qui ont amené GlobalProtect à mettre le périphérique en quarantaine, la raison pour laquelle GlobalProtect a mis le périphérique en quarantaine et l'emplacement des périphériques mis en quarantaine.<br>Attributs de tri : actions, motif, emplacement<br>Graphiques disponibles : barres, lignes |
| **Activité SSL** : affiche des informations sur l'activité SSL/TLS sur votre réseau. | |

| Widget | Description |
|---|---|
| **Activité de trafic** | Affiche l'activité SSL/TLS comparée à l'activité non-SSL/TLS par le nombre total de sessions ou par octet. |
| **Activité SSL/TLS** | Affiche les connexions TLS réussies par version TLS et application ou SNI. Ce widget vous aide à comprendre le risque que vous prenez en autorisant des versions plus faibles du protocole TLS. L'identification des applications et des SNI qui utilisent des protocoles faibles vous permet d'évaluer chacune d'entre elles et de décider si vous devez en autoriser l'accès pour des raisons professionnelles. Si vous n'avez pas besoin de l'application à des fins professionnelles, vous pouvez bloquer le trafic au lieu de l'autoriser. Cliquez sur une application ou un SNI pour approfondir et voir des informations détaillées. |
| **Raisons de l'échec du décryptage** | Affiche les raisons de l'échec du décryptage, telles que les problèmes de certificat ou de protocole, par SNI. Utilisez ces informations pour détecter les problèmes causés par une politique de décryptage ou une mauvaise configuration du profil ou par un trafic qui utilise des protocoles ou des algorithmes faibles. Cliquez sur une raison d'échec pour approfondir et isoler le nombre de sessions par SNI ou cliquez sur un SNI pour voir tous les échecs pour ce SNI. |
| **Activité de version TLS réussie** | Affiche la quantité de trafic décrypté et non décrypté par session ou par octet. Le trafic qui n'a pas été décrypté peut être exempté du décryptage par une politique, une mauvaise configuration de la politique, ou en étant sur la liste d'exclusion de décryptage (**Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **SSL Decryption Exclusion (Exclusion de décryptage SSL)**). |
| **Activité d'échange réussie** | Affiche les activités d'échange de clés réussies par algorithme, par application ou par SNI. Cliquez sur un algorithme d'échange de clés pour voir l'activité de cet algorithme ou cliquez sur une application ou un SNI pour voir l'activité d'échange de clés pour cette application ou ce SNI. |

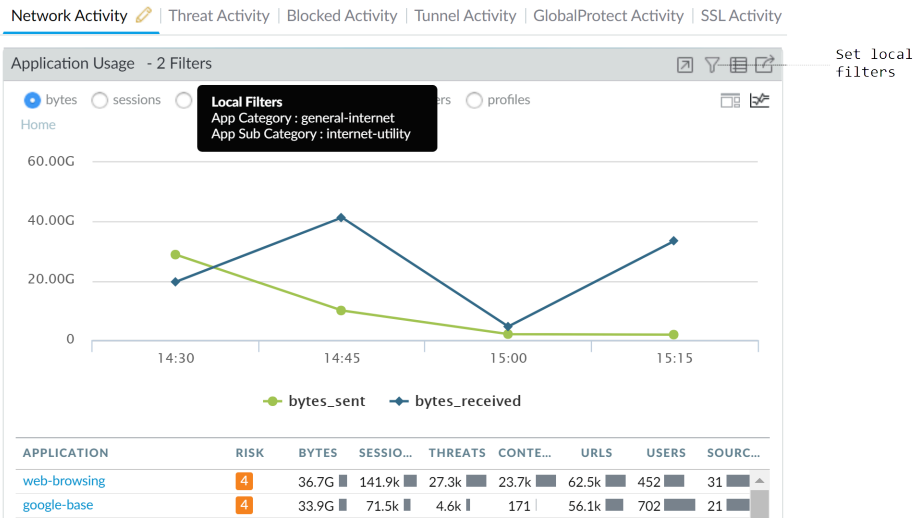
## Filtres de l'ACC

Les graphiques et tableaux des widgets de l'ACC vous permettent d'utiliser des filtres pour réduire les données affichées. Vous pouvez ainsi isoler des attributs spécifiques et analyser les informations à afficher de manière plus approfondie. L'ACC prend en charge l'utilisation simultanée de filtres de widget et généraux.

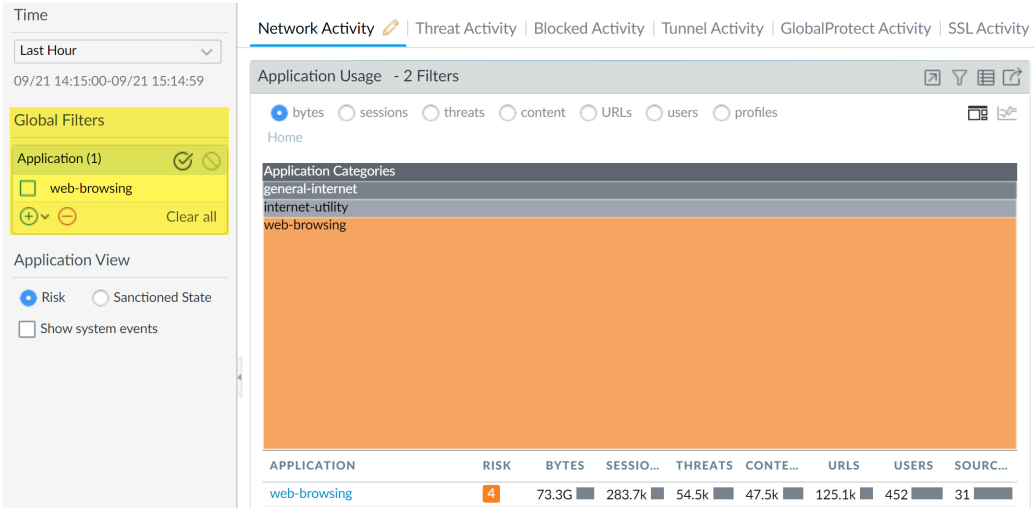
- **Filtres de widget** : appliquez un filtre de widget, à savoir un filtre***local*** sur un widget spécifique. Un filtre de widget vous permet d'interagir avec le graphique et de personnaliser l'affichage de manière à pouvoir accéder aux détails et accéder aux informations que vous souhaitez surveiller

sur un widget spécifique. Pour créer un filtre de widget conservé après un redémarrage, utilisez l'option**Set Local Filter (Définir un filtre local)**.




- **Filtres généraux** : appliquez des filtres généraux à tous les onglets de l'ACC. Un filtre général vous permet de pivoter l'affichage sur les détails dont vous avez besoin et d'exclure les informations sans rapport de l'affichage actif. Par exemple, pour afficher tous les éléments relatifs à un utilisateur et une application spécifiques, vous pouvez appliquer le nom d'utilisateur et l'application comme filtre général et afficher uniquement les informations qui se rapportent à l'utilisateur et l'application via tous les onglets et les widgets dans l'ACC. Les filtres généraux ne sont pas persistants.




Vous pouvez appliquer des filtres généraux de trois manières différentes :

- **Définir un filtre général à partir d'une table** : sélectionnez un attribut dans la table d'un widget et appliquez-le comme filtre général.
- **Ajout d'un filtre widget à un filtre général** : placez la souris sur l'attribut et cliquez sur l'icône en forme de flèche qui se trouve à droite de l'attribut. Cette option vous permet d'élever un filtre local utilisé dans un widget et d'appliquer l'attribut globalement de sorte que l'affichage de l'ensemble des onglets de l'ACC soit mis à jour.

- **Définition d'un filtre général** : définissez un filtre à l'aide du volet**Global Filters (Filtres généraux)** de l'ACC.

Pour plus d'informations sur l'utilisation de ces filtres, reportez-vous à la sectionInteraction avec l'ACC.

## Interaction avec l'ACC

Pour personnaliser et préciser l'affichage de l'ACC, vous pouvez ajouter, supprimer, exporter et importer des onglets et des widgets, définir des filtres locaux et généraux, et interagir avec les widgets.

- Ajouter un onglet
  1. Sélectionnez l'icône ➕ dans la liste des onglets.
  2. Ajoutez un **View Name (Nom de vue)**. Ce nom sera utilisé comme nom d'onglet. Vous pouvez ajouter jusqu'à cinq onglets.

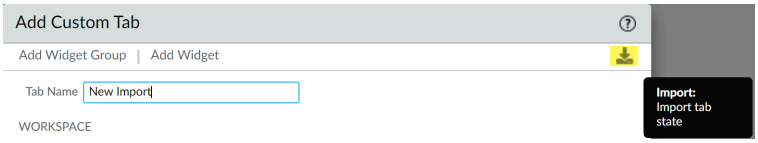
- Modifier un onglet.

  Sélectionnez l'onglet et cliquez sur l'icône de crayon en regard du nom de l'onglet pour le modifier. Par exemple, Threat Activity .

  La modification d'un onglet vous permet d'ajouter, de supprimer ou de réinitialiser les widgets affichés dans l'onglet. Vous pouvez également modifier le modèle du widget dans l'onglet.

  *Pour enregistrer l'onglet en tant qu'onglet par défaut, sélectionnez .*

- Exporter et importer des onglets
  1. Sélectionnez l'onglet et cliquez sur l'icône de crayon en regard du nom de l'onglet pour le modifier.
  2. Sélectionnez l'icône pour exporter l'onglet actuel en tant que fichier .txt. Vous pouvez partager ce fichier .txt avec un autre administrateur.
  3. Pour importer l'onglet en tant que nouvel onglet sur un autre pare-feu, sélectionnez l'icône ➕ dans la liste des onglets, puis indiquez un nom, cliquez sur l'icône d'importation et accédez au fichier .txt.




- Observez les widgets inclus dans un onglet.
  1. Sélectionnez l'onglet et cliquez sur l'icône de crayon pour le modifier.
  2. Cliquez sur la liste déroulante **Add Widget (Ajouter un widget)** pour voir les widgets dont les cases sont cochées.

- Ajout d'un widget ou d'un groupe de widgets
  1. Ajoutez un nouvel onglet ou modifiez un onglet prédéfini.
  2. Sélectionnez **Add Widget (Ajouter un widget)**, puis cochez la case correspondant au widget que vous souhaitez ajouter. Vous pouvez sélectionner un maximum de 12 widgets.
  3. (Facultatif) Pour créer un modèle à 2 colonnes, sélectionnez **Add Widget Group (Ajouter un groupe de widgets)**. Vous pouvez faire glisser et déposer des widgets dans l'affichage à 2 colonnes. Lorsque vous faites glisser le widget sur le modèle, un espace réservé s'affiche et vous permet de déposer le widget.

     *Vous ne pouvez pas nommer de groupe de widgets.*

- Supprimez un onglet ou un widget/groupe de widgets.
  1. Pour supprimer un onglet personnalisé, sélectionnez l'onglet et cliquez sur l'icône X.

     *Vous ne pouvez pas supprimer d'onglet prédéfini.*
  2. Pour supprimer un widget/groupe de widgets, modifiez l'onglet dans la section de l'espace de travail, puis cliquez sur l'icône [X] à droite. Vous ne pouvez pas annuler une suppression.

- Rétablissez les widgets par défaut dans un onglet.

  Dans un onglet prédéfini, tel que l'onglet **Blocked Activity (Activité bloquée)**, vous pouvez supprimer un ou plusieurs widgets. Si vous souhaitez réinitialiser le modèle pour inclure l'ensemble de widgets par défaut de l'onglet, modifiez l'onglet et cliquez sur **Reset View (Réinitialiser la vue)**.

- Faites un zoom avant pour accéder aux détails d'un graphique en aires, colonnes ou lignes.

  Observez le fonctionnement du zoom avant.

  Cliquez et faites glisser une aire du graphique pour faire un zoom avant. Par exemple, lorsque vous zoomez sur un graphique en lignes, une nouvelle requête est exécutée et le pare-feu extrait les données de la période sélectionnée. Il ne s'agit pas vraiment d'un agrandissement.

- Utilisez la liste déroulante de la table pour obtenir plus d'informations sur un attribut.
  1. Pointez avec la souris un attribut dans une table pour afficher la liste déroulante.
  2. Cliquez sur la liste déroulante pour afficher les options disponibles.
     - **Global Find (Recherche globale)** : l'Utilisation de la recherche globale pour effectuer une recherche sur le serveur de gestion du pare-feu ou de Panorama pour obtenir des références à l'attribut (nom d'utilisateur/adresse IP, nom d'objet, nom de règle de politique, ID de menace ou nom d'application) n'importe où dans la configuration candidate.
     - **Value (Valeur)** : affiche les informations sur l'ID menace, le nom d'application ou l'objet d'adresse.

- **Who Is (Qui)** : procède à une recherche de nom de domaine (*WHOIS*) pour l'adresse IP. La recherche interroge les bases de données qui renferment les utilisateurs enregistrés ou cessionnaires d'une ressource Internet.
- **Search HIP Report (Rechercher dans le rapport HIP)** : utilise le nom d'utilisateur ou l'adresse IP pour rechercher des correspondances dans un rapport de correspondance HIP.

- Définissez un filtre de widget.

  *Vous pouvez également cliquer sur un attribut dans la table (sous le graphique) pour l'appliquer comme filtre de widget.*

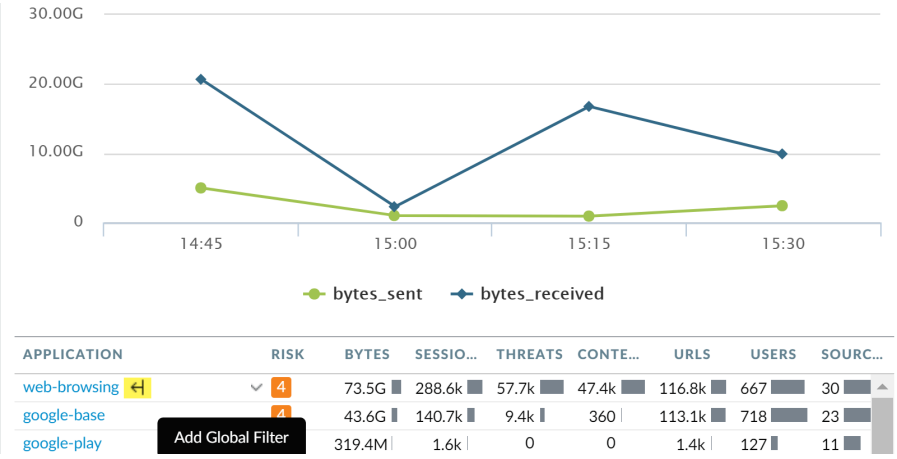
  1. Sélectionnez un widget et cliquez sur l'icône .
  2. Cliquez sur l'icône pour ajouter les filtres que vous souhaitez appliquer.
  3. Cliquez sur **Apply (Appliquer)**. Ces filtres sont persistants au redémarrage.

     *Les filtres du widget actif sont indiqués en regard du nom du widget.*

- Refusez un filtre de widget.
  1. Cliquez sur l'icône pour afficher la boîte de dialogue Configuration des filtres locaux.
  2. Ajoutez un filtre, puis cliquez sur l'icône de refus .

- Définissez un filtre général à partir d'une table.

  Placez la souris sur un attribut du tableau sous le graphique, puis cliquez sur la flèche qui apparaît à droite de l'attribut.



- Définissez un filtre général à l'aide du volet Filtres généraux.

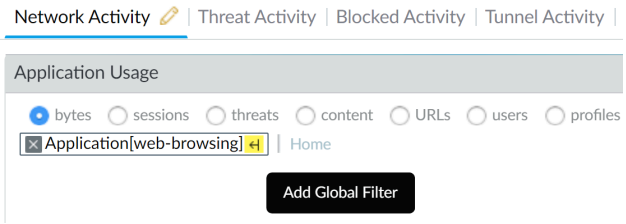
  Observez les filtres généraux en action.

  1. Accédez au volet **Global Filters (Filtres généraux)** à gauche de l'ACC.

  2. Cliquez sur l'icône pour afficher la liste de filtres que vous pouvez appliquer.

- Promouvez un filtre local comme filtre général.
  1. Dans n'importe quelle table d'un widget, cliquez sur le lien d'un attribut. Ceci définit l'attribut comme filtre de widget.
  2. Pour promouvoir le filtre comme filtre général, cliquez sur la flèche à droite du filtre.

- Supprimez un filtre.

  Cliquez sur l'icône pour supprimer un filtre.

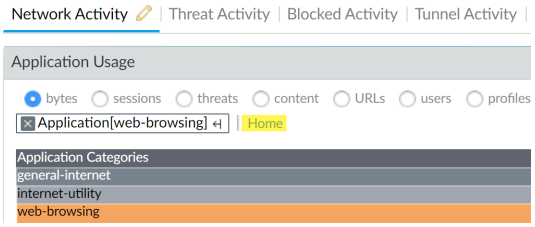
  - Pour les filtres généraux : elle se trouve dans le volet Global Filters (Filtres généraux).
  - Pour les filtres de widget : cliquez sur l'icône pour afficher la boîte de dialogue Configuration des filtres locaux, sélectionnez le filtre, puis cliquez sur l'icône .

- Effacez tous les filtres.
  - Pour les filtres généraux : cliquez sur le bouton **Clear All (Effacer tout)** sous Global Filters (Filtres généraux).
  - Pour les filtres de widget : Sélectionnez un widget et cliquez sur l'icône . Puis cliquez sur le bouton **Clear All (Effacer tout)** dans la boîte de dialogue Setup Local Filters (Configuration des filtres locaux).

- Observez les filtres en cours d'utilisation.
  - Pour les filtres généraux : le nombre de filtres généraux appliqués est affiché dans le volet de gauche sous Global Filters (Filtres généraux).
  - Pour les filtres de widget : le nombre de filtres de widget appliqués à un widget est affiché en regard de son nom. Pour afficher les filtres, cliquez sur l'icône .

- Réinitialisez l'affichage sur un widget.
  - Si vous définissez un filtre de widget ou accédez à un graphique, cliquez sur le lien **Home (Accueil)** pour réinitialiser l'affichage du widget.



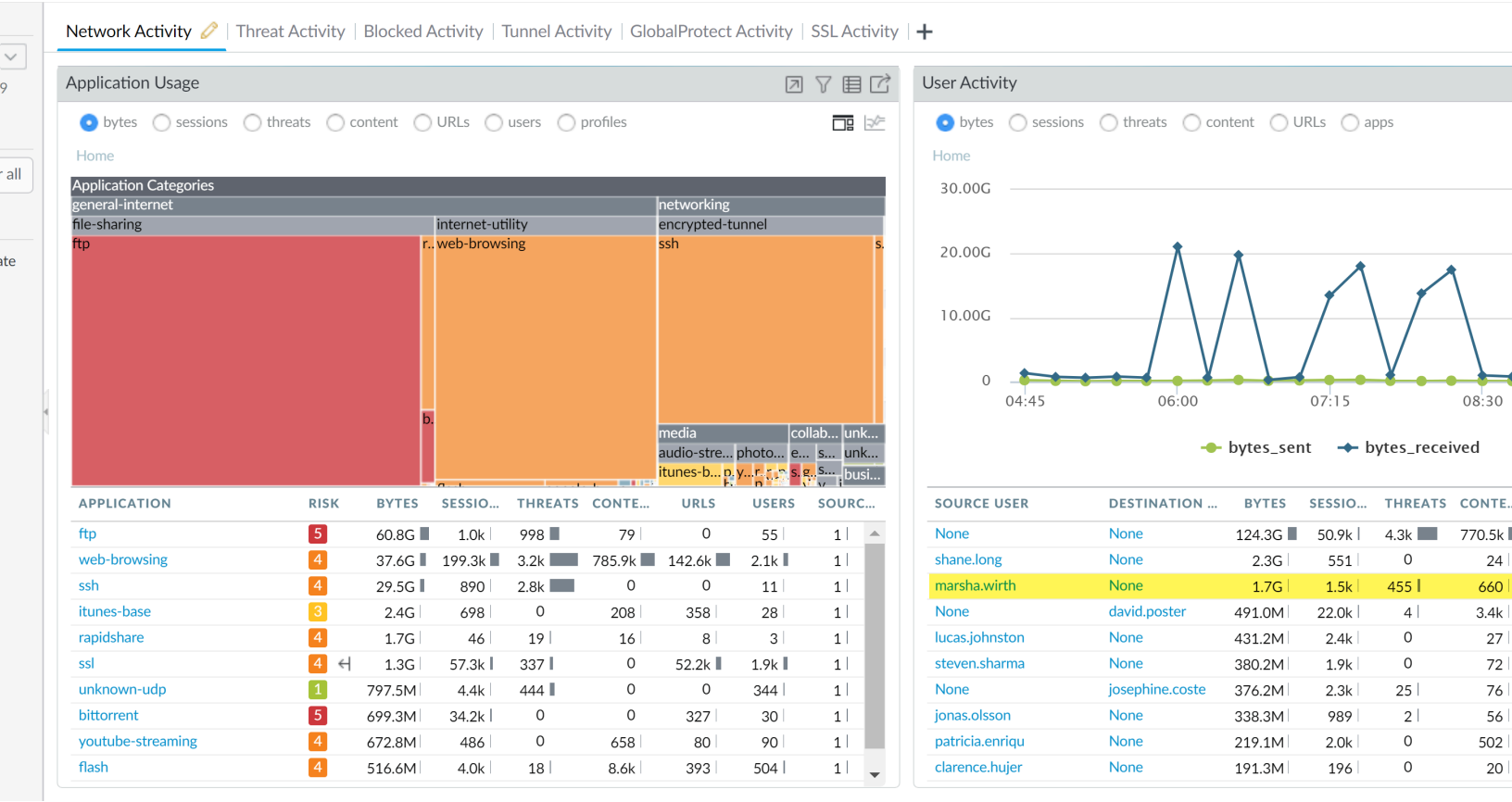

# Cas d'utilisation : ACC — Chemin détection d'informations

L'ACC propose une grande variété d'informations que vous pouvez utiliser comme point de départ à l'analyse du trafic réseau. Étudions un exemple d'utilisation de l'ACC pour détecter des événements utiles. Cet exemple montre comment vous pouvez utiliser l'ACC pour vous assurer que des utilisateurs légitimes peuvent être tenus pour responsables de leurs actes, détecter et suivre une activité non autorisée, et détecter et diagnostiquer des hôtes compromis et des systèmes vulnérables sur votre système.

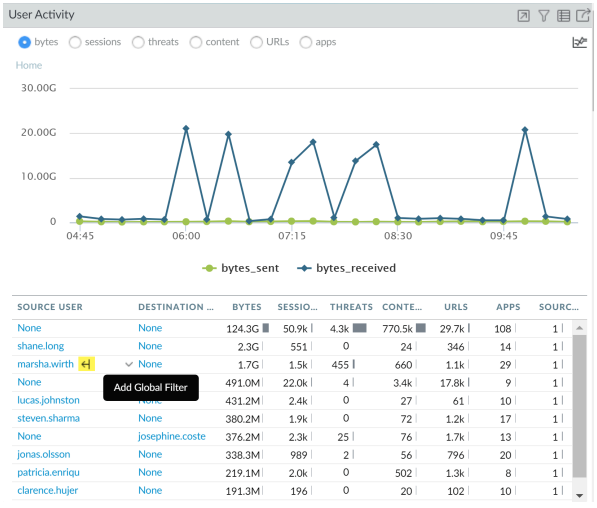
Les widgets et les filtres de l'ACC vous permettent d'analyser les données et de filtrer les vues sur la base d'événements intéressants ou pertinents. Vous pouvez suivre les événements qui vous sont utiles, exporter directement un PDF d'un onglet, accéder aux journaux bruts, et enregistrer une vue personnalisée de l'activité que vous souhaitez suivre. Ces possibilités vous permettent de surveiller l'activité et de développer des politiques et contre-mesures pour renforcer la protection de votre réseau contre les activités malveillantes. Dans cette section, vous allez procéder à une Interaction avec l'ACC (widgets) dans différents onglets, accéder à l'aide de filtres de widgets, basculer entre les vues de l'ACC à l'aide de filtres généraux et exporter un PDF pour partager avec les équipes de réponse aux incidents ou informatiques.

Vous voyez tout d'abord les widgets Utilisation de l'application et Activité de l'utilisateur de l'onglet **ACC (ACC)** > **Network Activity (Activité du réseau)**. Le widget User Activity (Activité de l'utilisateur) montre que l'utilisateur Marsha Wirth a transféré 154 méga-octets de données au cours de la dernière heure. Ce volume est quasiment six fois plus important que tout autre utilisateur sur le réseau. Pour afficher la tendance sur quelques heures, augmentez la période **Time (Heure)** à **Last 6 Hrs (6 dernières heures)**. L'activité de Marsha est alors de 1,7 giga-octets sur 1,500 sessions et a déclenché 455 signatures de menaces.




Étant donné que Marsha a transféré un volume important de données, appliquez à son nom d'utilisateur en tant que filtre général (Filtres de l'ACC) et basculez toutes les vues de l'ACC sur l'activité du trafic de Marsha.

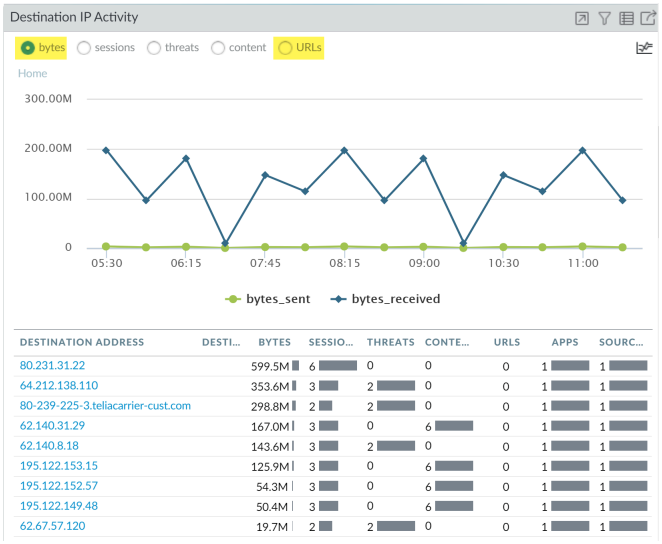



L'onglet Application Usage (Utilisation de l'application) indique maintenant que l'application principale utilisée par Martha était rapidshare, un site d'hébergement de fichiers détenu par une société suisse qui relève de la catégorie d'URL de partage de fichiers. Pour une étude plus approfondie, ajoutez rapidshare en tant que filtre général, puis affichez l'activité de Marsha liée à cette application.

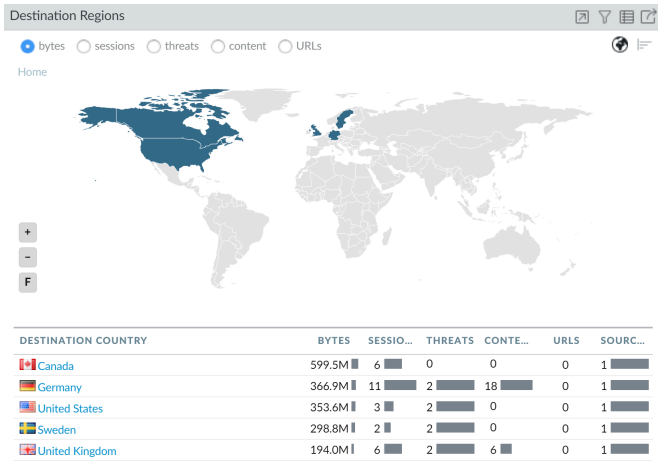
 

*Déterminez si vous souhaitez autoriser l'utilisation de rapidshare dans le cadre professionnel. Voulez-vous autoriser les chargements sur ce site et avez-vous besoin d'une politique QoS pour limiter la bande passante ?*

Pour connaître les adresses IP avec lesquelles Marsha a communiqué, cochez le widget **Destination IP Activity (Activité de l'adresse IP de destination)** et affichez les données par octets et par URL.

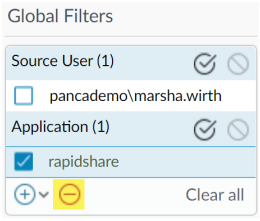



Pour connaître les pays avec lesquels Marsha a communiqué, triez par **sessions (Sessions)** dans le widget **Destination Regions (Régions de destination)**.



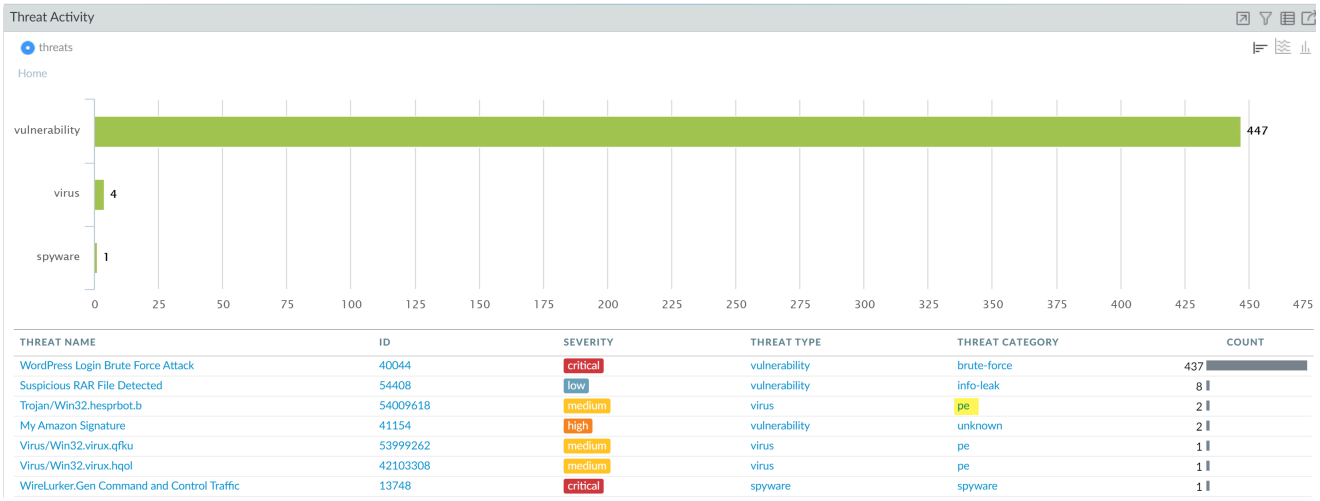

À partir de ces données, vous pouvez confirmer que Marsha, un utilisateur de votre réseau, a établi des sessions au Canada, en Allemagne, en Suède, au Royaume-Uni et aux États-Unis. Elle a enregistré 2 menaces dans ses sessions avec chaque pays de destination.

Pour observer l'aspect menaces de l'activité de Marsha, supprimez le filtre général pour rapidshare.



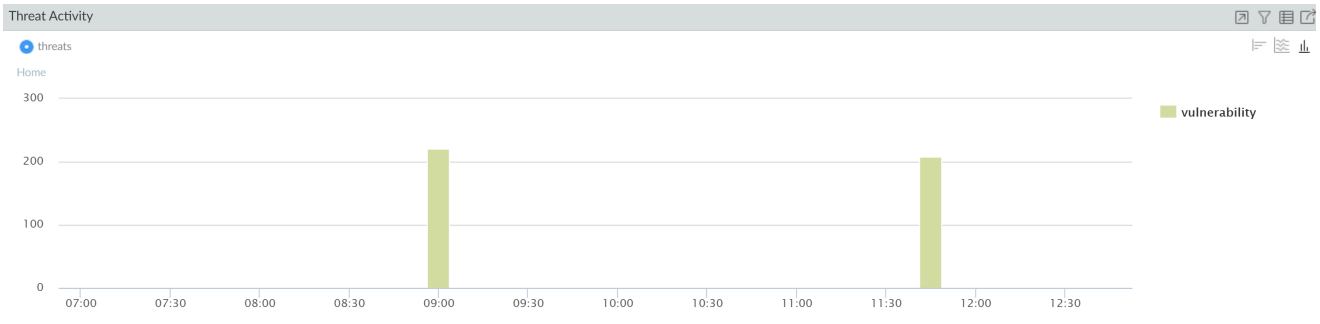

 

Dans le widget **Threat Activity (Activité des menaces)** de l'onglet **Threat Activity (Activité des menaces)**, consultez les menaces. Le widget affiche que son activité a déclenché une correspondance pour 452 vulnérabilités dans la catégorie des menaces de force brute, de fuite d'informations, d'exécutable portable (PE) et de logiciels espions. Le niveau de gravité de plusieurs de ces vulnérabilités est critique.



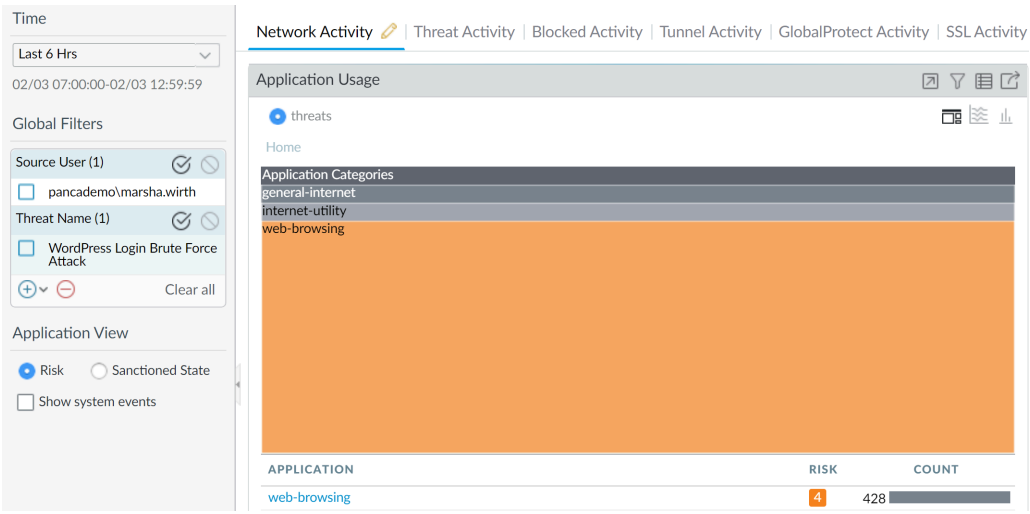

| THREAT NAME | ID | SEVERITY | THREAT TYPE | THREAT CATEGORY | COUNT |
|---|---|---|---|---|---|
| WordPress Login Brute Force Attack | 40044 | critical | vulnerability | brute-force | 437 |
| Suspicious RAR File Detected | 54408 | low | vulnerability | info-leak | 8 |
| Trojan/Win32.hesprbot.b | 54009618 | medium | virus | pe | 2 |
| My Amazon Signature | 41154 | high | vulnerability | unknown | 2 |
| Virus/Win32.virux.qfku | 53999262 | medium | virus | pe | 1 |
| Virus/Win32.virux.hqol | 42103308 | medium | virus | pe | 1 |
| WireLurker.Gen Command and Control Traffic | 13748 | critical | spyware | spyware | 1 |

Pour en savoir plus sur chaque vulnérabilité, cliquez sur le graphique et réduisez l'étendue de votre recherche. Chaque clic applique automatiquement un filtre local au widget.



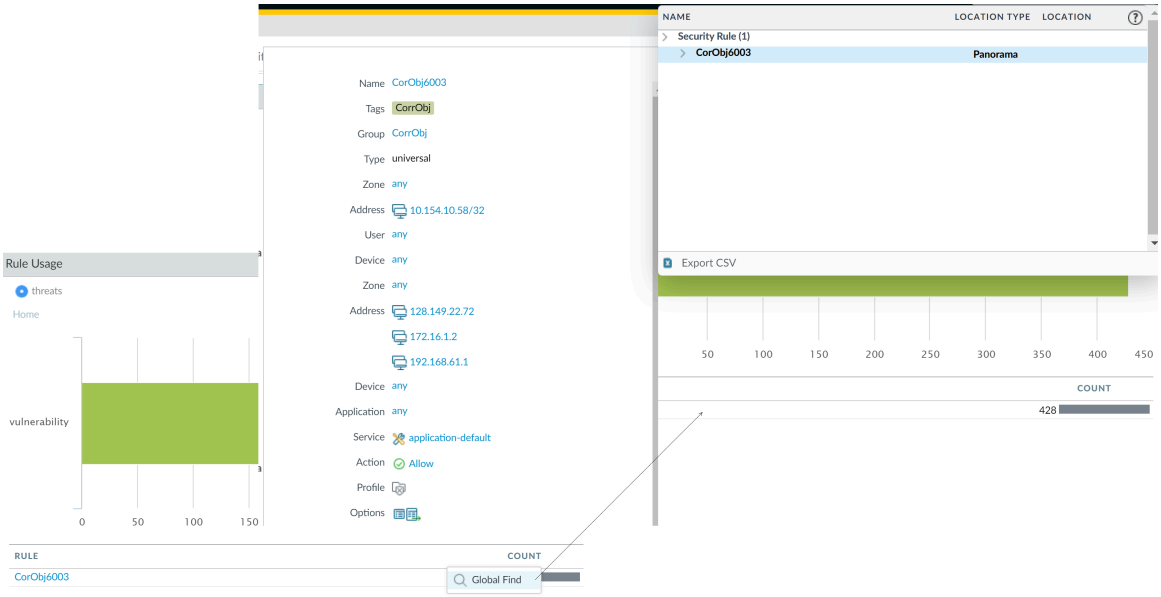

| THREAT NAME | ID | SEVERITY | THREAT TYPE | THREAT CATEGORY | COUNT |
|---|---|---|---|---|---|
| WordPress Login Brute Force Attack | 40044 | critical | vulnerability | brute-force | 428 |

Pour enquêter sur chaque menace par son nom, vous pouvez créer un filtre global pour, par exemple, **WordPress Login Brute Force Attack**. Affichez ensuite le widget **User Activity (Activité de l'utilisateur)** de l'onglet **Network Activity (Activité du réseau)**. L'onglet est automatiquement filtré pour afficher l'activité des menaces de Marsha (notez les filtres généraux dans la capture d'écran).




Notez que cette vulnérabilité d'exécution de code Microsoft a été déclenchée par e-mail, par l'application imap. Vous savez désormais que Martha présente des vulnérabilités IE et de pièces jointes d'e-mail, et que son ordinateur doit donc probablement être corrigé. Vous pouvez maintenant accéder au widget **Blocked Threats (Menaces bloquées)** de l'onglet **Blocked Activity (Activité bloquée)** pour savoir combien de ces vulnérabilités ont été bloquées.

Vous pouvez également consulter le widget **Rule Usage (Utilisation d'une règle)** de l'onglet **Network Activity (Activité du réseau)** pour savoir combien de vulnérabilités sont entrées sur votre réseau et la règle de sécurité qui a autorisé ce trafic. Accédez ensuite directement à la règle de sécurité à l'aide de la **Global Find (Recherche globale)**.

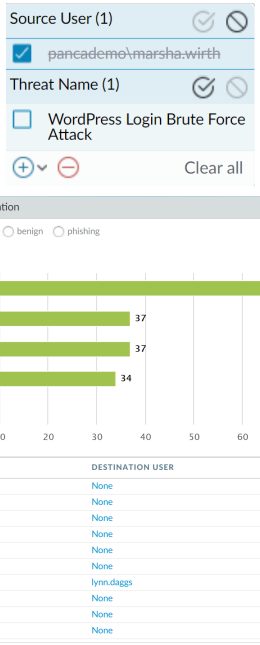



Ensuite, explorez les attaquants en utilisant la navigation Web pour attaquer la destination cible. Envisagez de modifier la règle de politique de sécurité pour restreindre ces adresses IP malveillantes ou définir plus précisément quelles adresses IP peuvent accéder à vos ressources réseau.

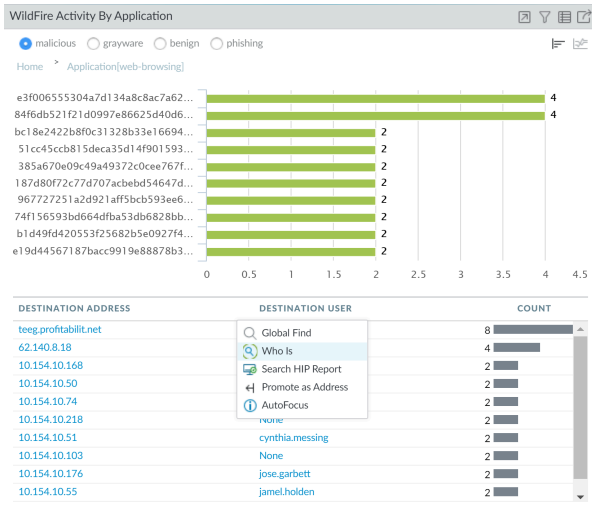
Pour savoir si des menaces ont été consignées sur la navigation web, vérifiez l'activité de Marsha dans le widget **WildFire Activity by Application (Activité WildFire par application)** de l'onglet **Threat Activity (Activité des menaces)**. Vous pouvez vous assurer que Marsha n'a eu aucune

activité malveillante, mais pour vérifier qu'aucun autre utilisateur n'a été compromis par l'application navigation web, supprimez Marsha en tant que filtre général et recherchez les autres utilisateurs qui ont déclenché des menaces sur la navigation web.




Cliquez sur la barre d'imap dans le graphique et étudiez les menaces entrantes associées à l'application. Pour savoir pour qui une adresse IP est enregistrée, pointez l'adresse IP du pirate et cliquez sur le lien **Who Is (Qui)** dans la liste déroulante.




Le nombre de sessions provenant de cette adresse IP étant élevé, consultez les widgets **Blocked Content (Contenu bloqué)** et **Blocked Threats (Menaces bloquées)** dans l'onglet **Blocked Activity (Activité bloquée)** pour voir les événements liés à cette adresse IP. L'onglet **Blocked Activity (Activité bloquée)** vous permet de vérifier si vos règles de politique bloquent efficacement le contenu ou les menaces lorsqu'un hôte sur votre réseau est compromis.

Utilisez l'option **Export PDF (Exporter au format PDF)** de l'ACC pour exporter la vue en cours (créer un instantané des données) et l'envoyer à une équipe de réponse aux incidents. Pour afficher les journaux des menaces directement depuis le widget, vous pouvez également cliquer sur l'icône

pour accéder aux journaux ; la requête est générée automatiquement et seuls les journaux pertinents s'affichent à l'écran (par exemple dans **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat Logs (Journaux des menaces)**).

Vous avez utilisé l'ACC pour passer en revue les données/tendances du réseau afin de rechercher les applications ou utilisateurs qui génèrent le plus de trafic, et combien d'applications sont responsables des menaces détectées sur le réseau. Vous avez pu identifier quels utilisateurs et applications ont généré le trafic, déterminer si l'application se trouvait sur le port par défaut, quelles règles de politique ont autorisé le trafic sur le réseau et si la menace se propage latéralement sur le réseau. Vous avez également identifié les adresses IP, géolocalisations, de destination avec lesquelles les hôtes du réseau communiquent. Utilisez les conclusions de votre recherche pour créer des politiques orientées sur un objectif permettant de sécuriser les utilisateurs et votre réseau.

# Utilisation de l'App-Scope

Les rapports App-Scope fournissent des outils de visibilité et d'analyse afin d'identifier un comportement problématique, vous permettant ainsi de comprendre les changements d'utilisation de l'application et d'activité de l'utilisateur, de connaître les utilisateurs et applications consommant le plus de bande passante réseau, et d'identifier les menaces réseau.

Grâce aux rapports App-Scope, vous pouvez rapidement identifier tout comportement inhabituel ou inattendu. Chaque rapport propose une fenêtre dynamique et personnalisable par l'utilisateur dans le réseau ; pointez la souris et cliquez sur les lignes ou les barres des diagrammes pour afficher des informations détaillées sur l'application, la catégorie d'applications, l'utilisateur ou la source spécifique, disponibles sur l'ACC. Les diagrammes App-Scope dans **Monitor (Surveillance)** > **App Scope (App Scope)** vous permettent de :

- Activer/désactiver les attributs de la légende pour n'afficher que les détails du diagramme que vous souhaitez consulter. La possibilité d'inclure ou d'exclure des données du diagramme vous permet de modifier l'échelle et de vérifier des détails de manière plus approfondie.
- Cliquez sur un attribut dans un diagramme en barres et parcourez les sessions correspondantes dans l'ACC. Cliquez sur un nom d'application, une catégorie d'applications, un nom de menace, une catégorie de menaces, une adresse IP source ou une adresse IP de destination dans un diagramme en barres pour filtrer sur l'attribut et afficher les sessions correspondantes dans l'ACC.
- Exporter un diagramme ou une carte au format PDF ou d'image. À des fins de portabilité et d'affichage hors ligne, vous pouvez exporter des diagrammes et des cartes au format PDF ou d'images PNG.

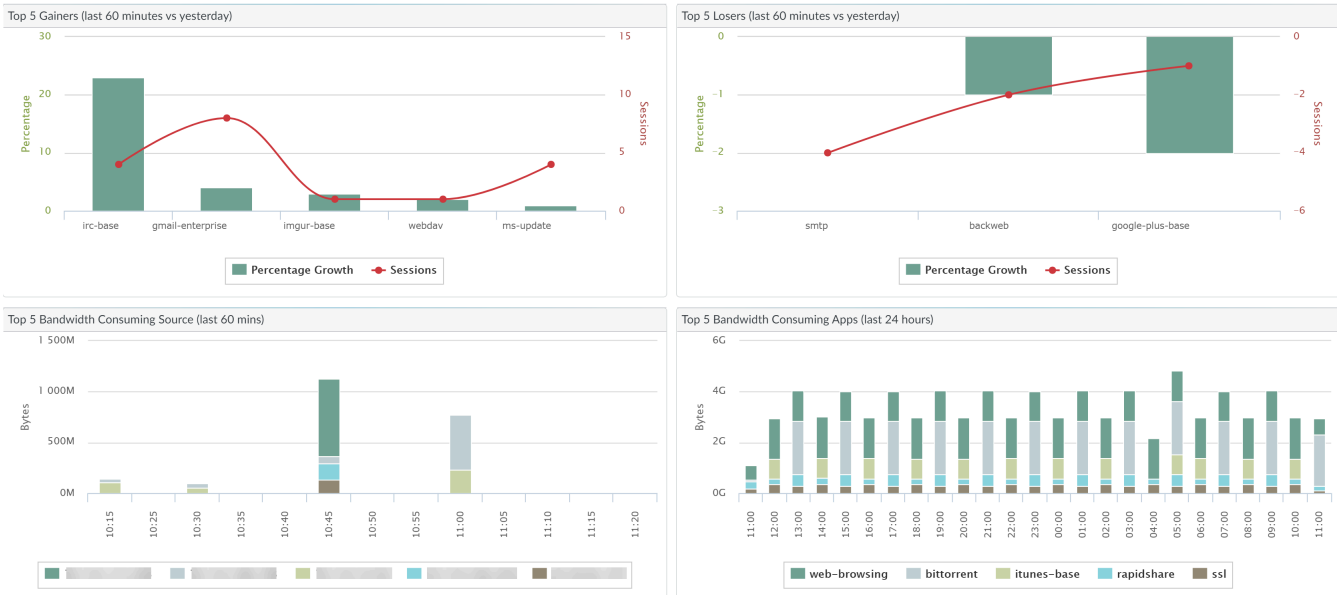
Les rapports App-Scope suivants sont disponibles :

- Rapport récapitulatif
- Rapport de surveillance des modifications
- Rapport de surveillance des menaces
- Rapport de la carte des menaces
- Rapport de surveillance du réseau
- Rapport de la carte du trafic

## Rapport récapitulatif

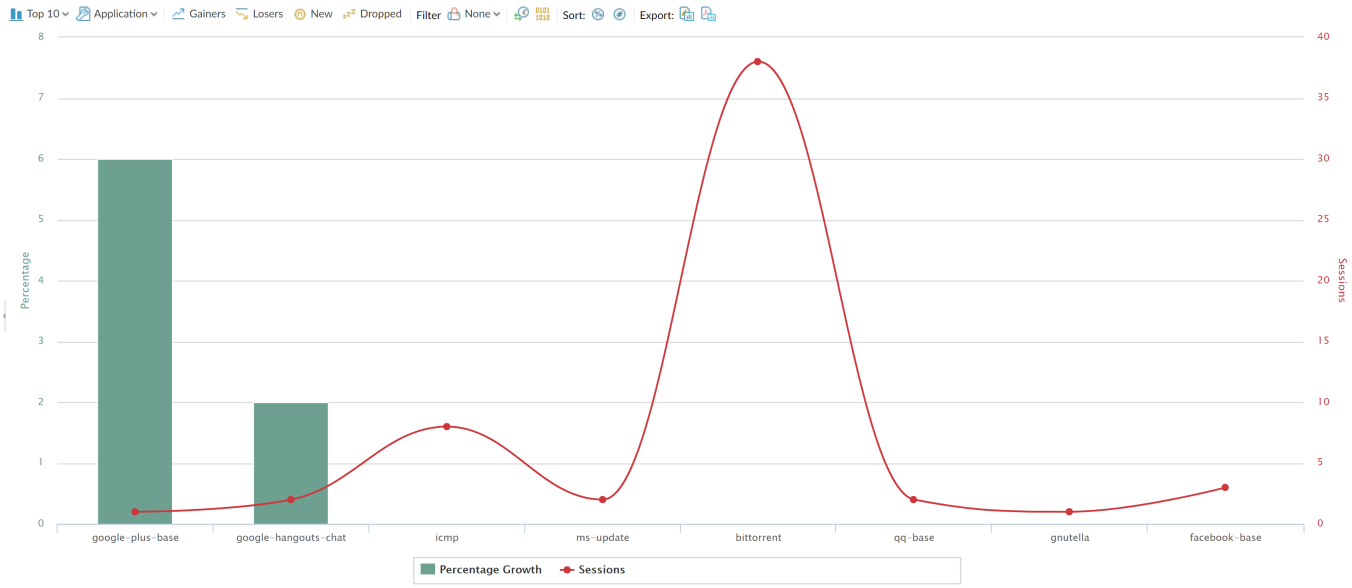
Le rapport récapitulatif App-Scope (**Monitor (Surveillance)** > **App Scope** > **Summary (Récapitulatif)**) affiche les diagrammes des cinq applications, les catégories d'applications, les utilisateurs et les sources obtenant, perdant et consommant le plus de bande passante.




# Rapport de surveillance des modifications

Le rapport de surveillance des modifications App-Scope (**Monitor (Surveillance)** > **App Scope (App-Scope)** > **Change Monitor (Surveillance des modifications)**) affiche les modifications apportées au cours d'une période définie. Par exemple, le diagramme suivant affiche les applications les plus utilisées au cours de la dernière heure par rapport à la dernière période de 24 heures. Les principales applications sont définies par nombre de sessions et triées par pourcentage.




Le rapport de surveillance des modifications contient les boutons et options suivants.

| Bouton | Description |
|---|---|
| **Top 10** | Détermine le nombre d'enregistrements dont la mesure la plus élevée est incluse dans le diagramme. |

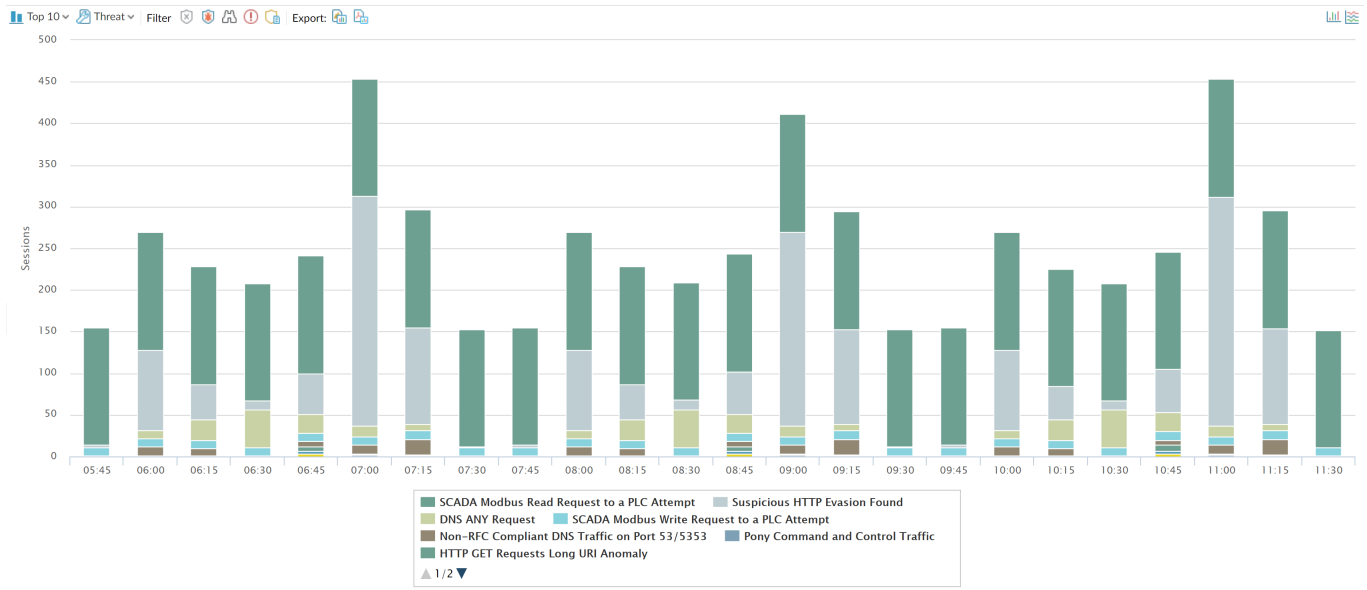
 

| Bouton | Description |
|---|---|
| **Application** | Détermine le type d'élément signalé : application, catégorie d'applications, source ou destination. |
| **Gagnants** | Affiche les mesures des éléments dont le nombre a augmenté au cours de la période évaluée. |
| **Perdants** | Affiche les mesures des éléments dont le nombre a baissé au cours de la période évaluée. |
| **Nouveau** | Affiche les mesures des éléments ajoutés au cours de la période évaluée. |
| **Dropped** | Affiche les mesures des éléments abandonnés au cours de la période évaluée. |
| **Filtre** | Applique un filtre afin d'afficher uniquement l'élément sélectionné. Aucun affichage dans toutes les entrées. |
|  | Indique si des informations de sessions ou d'octets doivent être affichées. |
| **Trier** | Indique si des entrées doivent être triées par pourcentage ou par croissance brute. |
| **Exporter** | Exporte le graphique sous forme d'image .png ou au format PDF. |
| **Comparer** | Indique la période au bout de laquelle les mesures des modifications apportées sont réalisées. |

## Rapport de surveillance des menaces

Le rapport de surveillance des menaces App-Scope (**Monitor (Surveillance)** > **App Scope (App-Scope)** > **Threat Monitor (Surveillance des menaces)**) affiche le nombre de menaces principales identifiées au cours de la période sélectionnée. Par exemple, la figure suivante affiche les 10 types de menaces principales rencontrées au cours des 6 dernières heures.




Chaque type de menace est représenté par une couleur, comme indiqué dans la légende située sous le diagramme. Le rapport de surveillance des menaces contient les boutons et options suivants.

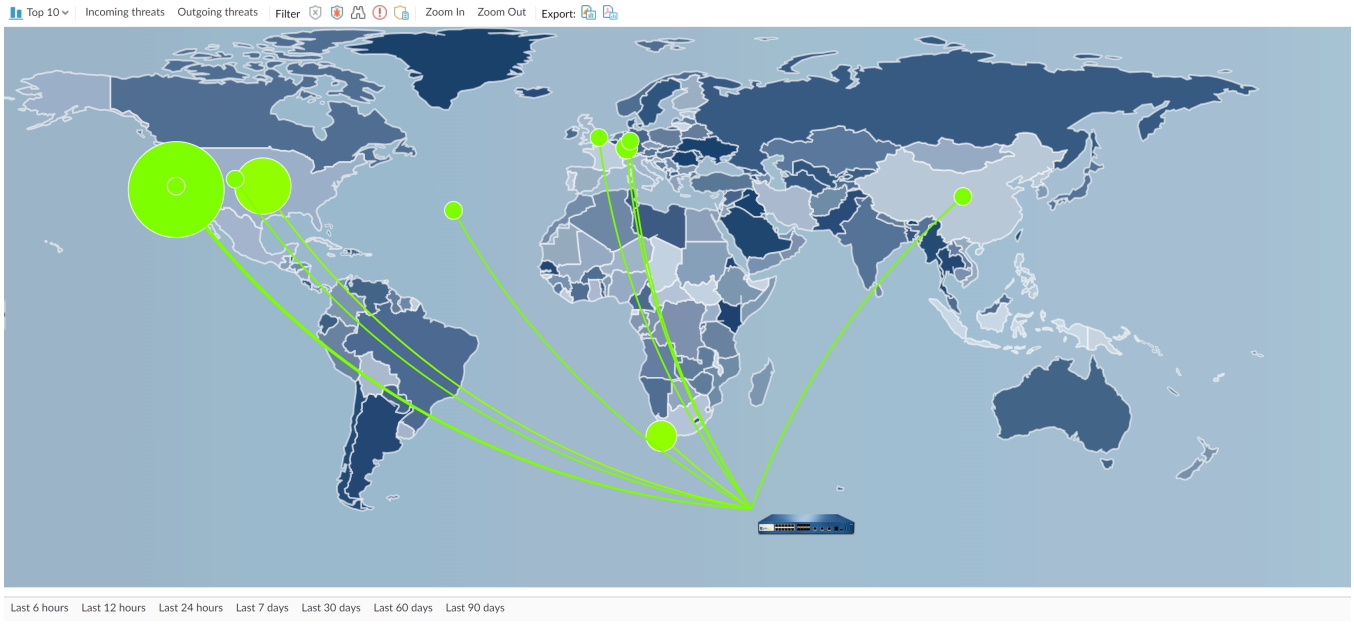
| Bouton | Description |
|---|---|
| **Top 10** | Détermine le nombre d'enregistrements dont la mesure la plus élevée est incluse dans le diagramme. |
| **Threats** | Détermine le type d'élément mesuré : menace, catégorie de menaces, source ou destination. |
| **Filtre** | Applique un filtre afin d'afficher uniquement le type d'élément sélectionné. |
|  | Indique si les informations sont présentées sous la forme d'un histogramme empilé ou d'un diagramme en aires empilées. |
| **Exporter** | Exporte le graphique sous forme d'image .png ou au format PDF. |
|   | Indique la période au bout de laquelle des mesures sont réalisées. |

# Rapport de la carte des menaces

Le rapport de la carte des menaces App-Scope (**Monitor (Surveillance)** > **App Scope (App-Scope)** > **Threat Map (Carte des menaces)**) affiche une vue géographique des menaces, ainsi que leur gravité. Chaque type de menace est représenté par une couleur, comme indiqué dans la légende située sous le diagramme.

Le pare-feu utilise la géolocalisation pour créer des cartes des menaces. Le pare-feu se situe au bas de l'écran de la carte des menaces si vous n'avez pas spécifié les coordonnées de géolocalisation (**Device (Équipement)** > **Setup (Configuration)** > **Management (Gestion)**, section General Settings (Paramètres généraux)) sur le pare-feu.

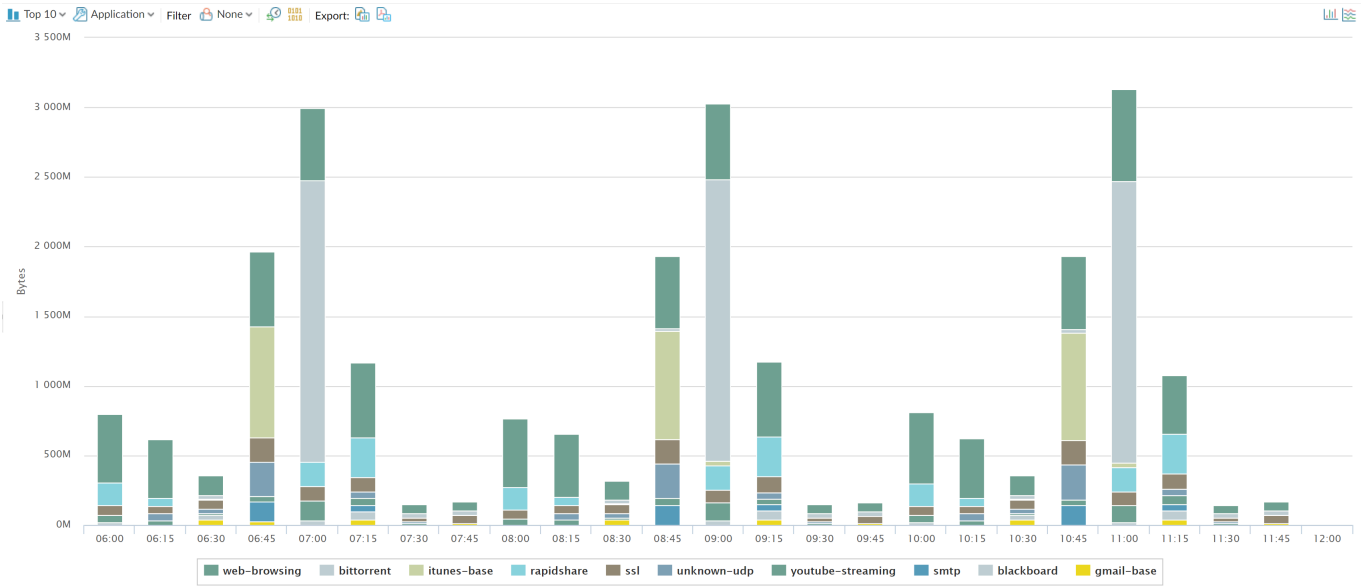



Le rapport de la carte des menaces contient les boutons et options suivants.

| Bouton | Description |
|---|---|
| **Top 10** | Détermine le nombre d'enregistrements dont la mesure la plus élevée est incluse dans le diagramme. |
| **Menaces entrantes** | Affiche les menaces entrantes. |
| **Menaces sortantes** | Affiche les menaces sortantes. |
| **Classification** | Applique un filtre afin d'afficher uniquement le type d'élément sélectionné. |
| **Zoom avant et zoom arrière** | Zoom avant et zoom arrière de la carte. |
| **Exporter** | Exporte le graphique sous forme d'image .png ou au format PDF. |
| Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days | Indique la période au bout de laquelle des mesures sont réalisées. |

# Rapport de surveillance du réseau

Le rapport de surveillance du réseau App-Scope (**Monitor (Surveillance)** > **App Scope (App-Scope)** > **Network Monitor** (Surveillance du réseau)) affiche la bande passante dédiée aux différentes fonctions réseau au cours de la période définie. Chacune de ces fonctions est représentée par une couleur, comme indiqué dans la légende située sous le diagramme. Par exemple, l'image ci-dessous montre la bande passante de l'application au cours des 7 derniers jours et se base sur des informations de session.




Le rapport de surveillance du réseau contient les boutons et options suivants.

| Bouton | Description |
|---|---|
| **Top 10** | Détermine le nombre d'enregistrements dont la mesure la plus élevée est incluse dans le diagramme. |
| **Application** | Détermine le type d'élément signalé : application, catégorie d'applications, source ou destination. |
| **Filtre** | Applique un filtre afin d'afficher uniquement l'élément sélectionné. **None (Aucun)** affiche toutes les entrées. |
| | Indique si des informations de sessions ou d'octets doivent être affichées. |
| **Export (Exporter)** | Exporte le graphique sous forme d'image .png ou au format PDF. |
| | Indique si les informations sont présentées sous la forme d'un histogramme empilé ou d'un diagramme en aires empilées. |

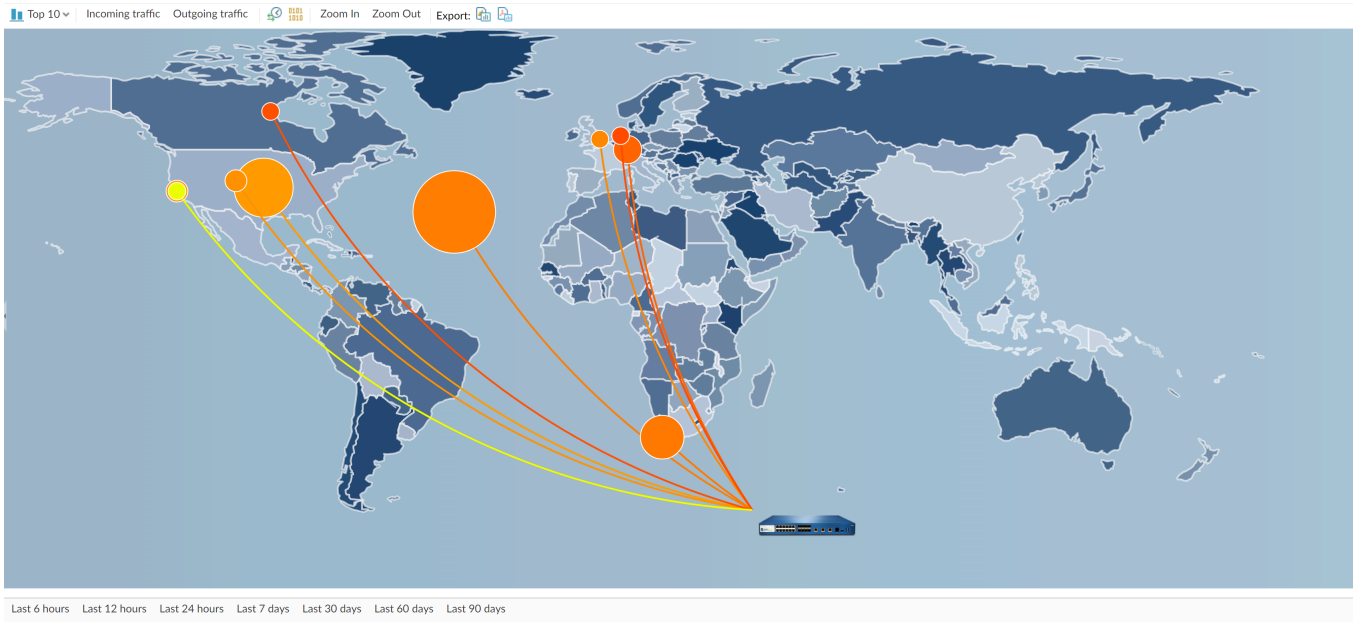
 

| Bouton | Description |
| --- | --- |
| Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days | Indique la période au bout de laquelle les mesures des modifications apportées sont réalisées. |

## Rapport de la carte du trafic

Le rapport de la carte du trafic App-Scope (**Monitor (Surveillance)** > **App Scope (App-Scope)** > **Traffic Map (Carte du trafic)**) affiche une vue géographique des flux de trafic en fonction des sessions ou des flux.

Le pare-feu utilise la géolocalisation pour créer des cartes du trafic. Le pare-feu se situe au bas de l'écran de la carte du trafic si vous n'avez pas spécifié les coordonnées de géolocalisation (**Device (Équipement)** > **Setup (Configuration)** > **Management (Gestion),**, section General Settings (Paramètres généraux)) sur le pare-feu.




Chaque type de trafic est représenté par une couleur, comme indiqué dans la légende située sous le diagramme. Le rapport de la carte du trafic contient les boutons et options suivants.

| Boutons | Description |
| --- | --- |
| **Top 10** | Détermine le nombre d'enregistrements dont la mesure la plus élevée est incluse dans le diagramme. |
| **Menaces entrantes** | Affiche les menaces entrantes. |
| **Menaces sortantes** | Affiche les menaces sortantes. |
| | Indique si des informations de sessions ou d'octets doivent être affichées. |

| Boutons | Description |
| --- | --- |
| **Zoom avant et zoom arrière** | Zoom avant et zoom arrière de la carte. |
| **Exporter** | Exporte le graphique sous forme d'image .png ou au format PDF. |
| Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days | Indique la période au bout de laquelle les mesures des modifications apportées sont réalisées. |

# Utilisation du moteur de corrélation automatique

Le moteur de corrélation automatique est un outil d'analyse qui utilise les journaux sur le pare-feu pour détecter des événements pratiques sur votre réseau. Le moteur corrèle une série d'événements de menaces liés qui, lorsqu'ils sont combinés, révèlent un hôte potentiellement compromis sur votre réseau ou une autre conclusion de niveau supérieur. Il met en évidence les zones à risque, comme des hôtes compromis sur le réseau, vous permettant ainsi d'évaluer le risque et d'entreprendre une action pour empêcher l'utilisation des ressources du réseau. Le moteur de corrélation automatique utilise des ***objets de corrélation*** pour analyser les journaux de modèles et, lorsqu'une correspondance est trouvée, il génère un ***événement corrélé***.

***Les modèles suivants prennent en charge le moteur de corrélation automatique :***

- *Panorama - appareils et appareils virtuels de la série M*
- *Pare-feu PA-7000 Series*
- *Pare-feu PA-5200 Series*
- *Pare-feu PA-3200 Series*



## Concepts du moteur de corrélation automatique

Le moteur de corrélation automatique utilise des ***objets de corrélation*** pour analyser les journaux de modèles et, lorsqu'une correspondance est trouvée, il génère un ***événement corrélé***.



### Objet Corrélation

Un objet de corrélation est un fichier de définition qui spécifie les modèles de correspondance, les sources de données à utiliser pour les recherches et la période de recherche de ces modèles. Un modèle est une structure booléenne de conditions interrogeant les sources de données (ou journaux) suivantes sur le pare-feu : statistiques d'application, trafic, récapitulatif du trafic, récapitulatif des menaces, menaces, filtrage des données et filtrage des URL. Chaque modèle présente un niveau de gravité, et un seuil de correspondances du modèle doit être atteint au cours d'une période spécifiée pour indiquer une activité malveillante. Lorsque des conditions de correspondance sont remplies, un événement corrélé est consigné.

Un objet de corrélation permet de lier des événements réseau isolés et de rechercher des modèles indiquant un événement plus significatif. Ces objets identifient des modèles de trafic suspect et des anomalies réseau, comme une activité IP suspecte, une activité de commande et contrôle connue, une exploitation des vulnérabilités connue ou une activité du Botnet qui, lorsqu'elles sont corrélées, indiquent avec une très forte probabilité qu'un hôte du réseau a été compromis. Les objets de

corrélation sont définis et développés par l'équipe de recherche de menaces Palo Alto Networks et sont distribués au pare-feu et à Panorama lors des mises à jour dynamiques hebdomadaires. Pour obtenir de nouveaux objets de corrélation, le pare-feu doit disposer d'une licence Threat Prevention. Panorama nécessite une licence de support pour obtenir les mises à jour.

Les modèles définis dans un objet de corrélation peuvent être statiques ou dynamiques. Les objets corrélés qui incluent des modèles observés dans WildFire sont dynamiques, et vous pouvez corréler des modèles malveillants détectés par WildFire avec l'activité de commande et contrôle lancée par un hôte ciblé par l'activité malveillante sur votre réseau ou avec l'activité vue par un point de terminaison protégé par Traps sur Panorama. Par exemple, lorsqu'un hôte envoie un fichier au cloud WildFire et que le verdict est malveillant, l'objet de corrélation recherche d'autres hôtes ou clients sur le réseau avec le même comportement dans le cloud. Si l'exemple malveillant a effectué une recherche DNS et accédé à un domaine malveillant, l'objet de corrélation recherche un événement similaire dans les journaux. Lorsque l'activité sur un hôte correspond à l'analyse dans le cloud, un événement corrélé de gravité élevée est consigné.

### Événements corrélés

Un événement de corrélation est consigné lorsque les modèles et seuils définis dans un objet de corrélation correspondent aux modèles de trafic sur votre réseau. Pour l'Interprétation des événements corrélés et pour afficher une vue graphique des événements, reportez-vous à la section Utilisation du widget Hôtes compromis de l'ACC.

## Affichage des objets corrélés

Vous pouvez visualiser les objets de corrélation actuellement disponibles sur le pare-feu.

**STEP 1 |** Sélectionnez **Monitor (Surveillance)** > **Automated Correlation Engine (Moteur de corrélation automatisé)** > **Correlation Objects (Objets de corrélation)**. Tous les objets de la liste sont cochés par défaut.

| TITLE | CATEGORY | STATE | DESCRIPTION |
|---|---|---|---|
| Multiple User from One Endpoint MFA Credential Theft | credential-theft-abuse | active | This correlation object detects multiple account abuse from a possibly compromised endpoint |
| WildFire C2 | compromised-host | active | This correlation object detects hosts that have exhibited command-and-control (C2) network behavior corresponding to malware detected by WildFire elsewhere on your network. |
| WildFire and Traps ESM Correlated C2 | compromised-host | active | This correlation object detects hosts that have received malware detected by WildFire or executed malware as seen by Traps, and have also exhibited command- and-control (C2) network behavior corresponding to the detected malware. |
| Single Account and Endpoint MFA Credential Theft | credential-theft-abuse | active | This correlation object detects activity from a possibly compromised user account from a single endpoint |
| Compromise Activity Sequence | compromised-host | active | This correlation object detects a host involved in a sequence of activity indicating remote compromise, starting with scanning or probing activity, progressing to exploitation, and concluding with network contact to a known malicious domain. |
| Exploit Kit Activity | compromised-host | active | This object detects probable exploit kit activity targeted at a host on the network. Exploit kits are identified by a vulnerability exploit or exploit kit landing page signature, combined with either a malware download signature or a known command-and-control signature. |
| Single Account 1 FA Multiple Endpoints Credential Timeouts | credential-theft-abuse | active | This correlation object detects timed out attempts of first factor authentications from multiple endpoints using a single user account |
| Beacon Detection | compromised-host | active | This correlation object detects likely compromised hosts based on activity that resembles command-and-control (C2) beaconing, such as repeated visits to recently registered domains or dynamic DNS domains, repeated file downloads from the same location, generation of unknown traffic, etc. |
| Single Account and Endpoint MFA Credential Timeout | credential-theft-abuse | active | This correlation object detects timedout MFA authentication attempts from a single endpoint using single account |
| Multiple Endpoint MFA Credential Timeout Abuse | credential-theft-abuse | active | This correlation object detects timed out second factor authentications from multiple endpoints using a single user account |
| Multiple Endpoint MFA Credential Abuse | credential-theft-abuse | active | This correlation object detects activity from multiple endpoints using a single user account |
| Exploit Kit Delivering XOR obfuscated malware | compromised-host | active | This correlation object detects exclusive-or (XOR) obfuscated malware downloaded to a host. XOR obfuscation is a technique to evade detection by encrypting portions of a file in order to hide malicious code. This correlation object specifically identifies XOR obfuscated malware that is delivered to the host by an exploit kit. While the Exploit Kit Activity object detects exploit kits combined with either a malware download signature or a known command-and-control signature, this object is provided to specifically detect an event where XOR obfuscation malware inserted on a host by an exploit kit and to distinguish such an event from other exploit kit activities. |
| Single Account 1 FA Credential Abuse | credential-theft-abuse | active | This correlation object detects timed out first factor authentications from an endpoint using a single user account |

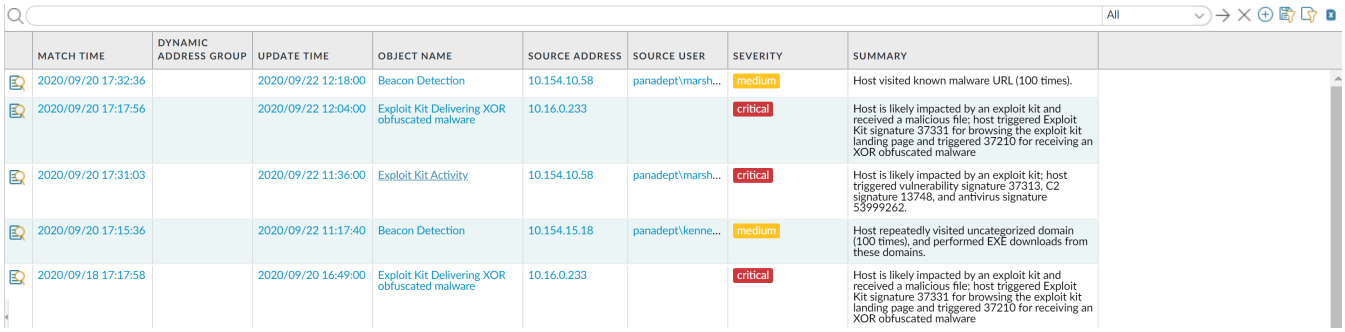
**STEP 2 |** Affichez les informations de chaque objet de corrélation. Chaque objet fournit les informations suivantes :

- **Name (Nom)** et **Title (Titre)** : le nom et le titre indiquent le type d'activité que l'objet de corrélation détecte. La colonne Name (Nom) est masquée par défaut. Pour consulter la définition de l'objet, affichez la colonne et cliquez sur le lien du nom.
- **ID (ID)** : un numéro unique qui identifie l'objet de corrélation ; cette colonne est également masquée par défaut. Les ID se trouvent dans la série 6000.
- **Category (Catégorie)** : un récapitulatif du type de menace ou nuisance qui pèse sur le réseau, l'utilisateur ou l'hôte. Actuellement, tous les objets identifient des hôtes compromis sur le réseau.
- **State (État)** : indique si l'objet de corrélation est activé (actif) ou désactivé (inactif). Tous les objets de la liste sont cochés par défaut, et donc actifs. Ces objets étant basés sur des données d'intelligence des menaces et définis par l'équipe de recherche de menaces Palo Alto Networks, maintenez-les actifs pour suivre et détecter une activité malveillante sur votre réseau.
- **Description (Description)** : spécifie les conditions de correspondance pour lesquelles le pare-feu ou Panorama analysera les journaux. Elle décrit la séquence de conditions mises en correspondance pour identifier une accélération ou remontée de l'activité malveillante ou comportement suspect de l'hôte. Par exemple, l'objet **Compromise Lifecycle (Cycle de vie compromis)** détecte un hôte impliqué dans un cycle de vie d'attaque complet dans une remontée en trois étapes qui commence par l'analyse ou le sondage de l'activité, la progression jusqu'à l'exploitation et la conclusion de la mise en contact du réseau avec un domaine malveillant connu.

Pour plus d'informations, reportez-vous aux sections Concepts du moteur de corrélation automatique et Utilisation du moteur de corrélation automatique.

## Interprétation des événements corrélés

Vous pouvez afficher et analyser les journaux générés pour chaque événement corrélé dans l'onglet **Monitor (Surveillance)** > **Automated Correlation Engine (Moteur de corrélation automatique)** > **Correlated Events (Événements corrélés)**.




Événements corrélés incluent les informations suivantes :

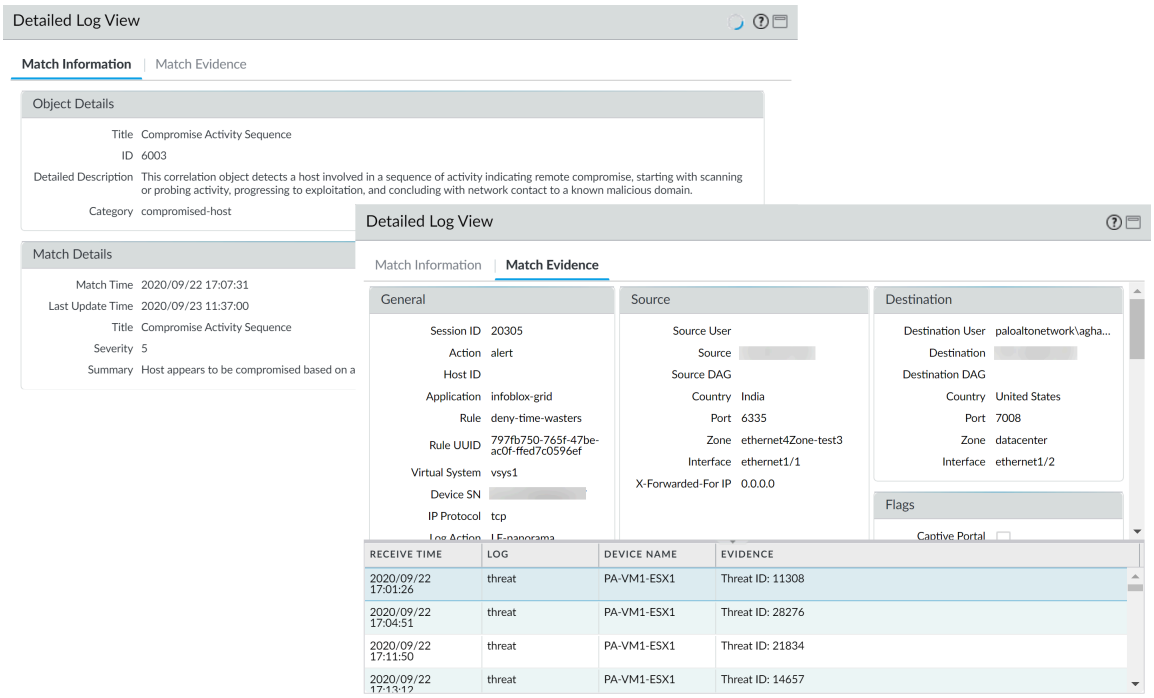
| Champ | Description |
|---|---|
| **Heure de correspondance** | L'heure à laquelle l'objet de corrélation a déclenché une correspondance. |
| **Heure de mise à jour** | L'heure à laquelle l'événement a été mis à jour pour la dernière fois avec une preuve de la correspondance. Lorsque le pare-feu collecte une preuve sur un modèle ou une séquence d'événements défini dans un objet de corrélation, l'horodatage est mis à jour dans le journal des événements corrélés. |
| **Nom de l'objet** | Le nom de l'objet de corrélation qui a déclenché la correspondance. |
| **Source Address (Adresse source)** | L'adresse IP de l'utilisateur/périphérique sur votre réseau d'où provient le trafic. |
| **Source User (Utilisateur source)** | Les informations sur l'utilisateur et le groupe d'utilisateurs du serveur d'annuaire, si User-id est activé. |
| **Sévérité** | Un classement qui indique l'urgence et l'incidence de la correspondance. Le niveau de gravité indique l'étendue du dommage ou du modèle de remontée observé, ainsi que la fréquence d'occurrence. |

| Champ | Description |
| --- | --- |
| *Pour configurer le pare-feu ou Panorama pour envoyer des alertes par e-mail, SNMP ou des messages Syslog pour un niveau de gravité souhaité, reportez-vous à la section* Utilisation de services externes pour la surveillance. | Les objets de corrélation ciblant principalement la détection de menaces, les événements corrélés visent généralement à identifier les hôtes compromis sur le réseau et le niveau de gravité se traduit comme suit :<br>• **Critical (Critique)** : indique qu'un hôte a été compromis sur la base d'événements corrélés présentant un modèle de remontée. Par exemple, un événement critique est consigné lorsqu'un hôte ayant reçu un fichier avec un verdict malveillant de WildFire présente la même activité de commande et contrôle que celle observée dans le sandbox WildFire pour ce fichier malveillant.<br>• **High (Élevé)** : indique qu'un hôte est très probablement compromis sur la base d'une corrélation entre plusieurs événements de menace, comme un logiciel malveillant détecté à un quelconque endroit du réseau qui correspond à l'activité de commande et contrôle générée par un hôte particulier.<br>• **Medium (Moyen)** : indique qu'un hôte est probablement compromis sur la base de la détection d'un ou plusieurs événements suspects, comme les consultations répétées d'URL malveillantes connues suggérant une activité de commande et contrôle à script.<br>• **Low (Faible)** : indique qu'un hôte est potentiellement compromis sur la base de la détection d'un ou plusieurs événements suspects, comme la consultation d'une URL malveillante ou d'un domaine DNS dynamique.<br>• **Informational (Informations)** : détecte un événement pouvant permettre d'identifier, dans l'agrégation, une activité suspecte ; mais l'événement n'est pas nécessairement important. |
| **Résumé** | Une description qui récapitule les preuves rassemblées sur l'événement corrélé. |

Cliquez sur l'icône pour afficher la vue détaillée du journal, qui inclut toutes les preuves d'une correspondance :

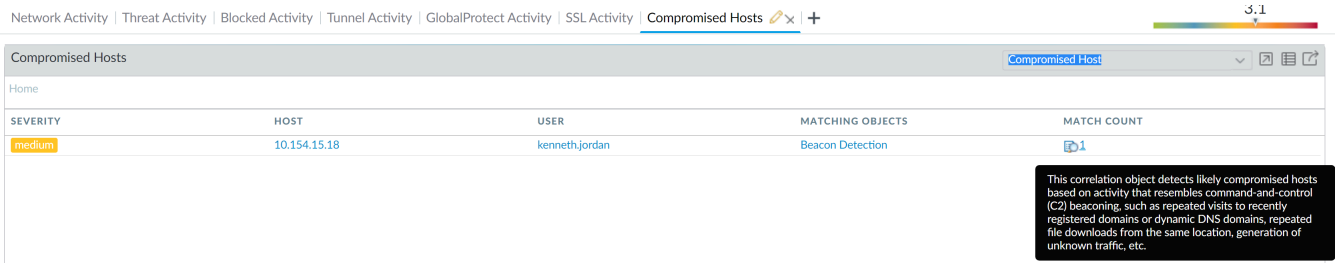



| Onglet | Description |
|---|---|
| **Informations sur la correspondance** | Détails de l'objet : présentent des informations sur l'Objet Corrélation qui a déclenché la correspondance. |
| | Détails de la correspondance : un récapitulatif des détails de la correspondance, notamment l'heure de correspondance, l'heure de la dernière mise à jour selon la preuve de correspondance, le niveau de gravité de l'événement et un récapitulatif des événements. |
| **Preuve de correspondance** | Présente toutes les preuves qui corroborent l'événement corrélé. Il affiche des informations détaillées sur les preuves collectées pour chaque session. |

# Utilisation du widget Hôtes compromis de l'ACC

Le widget Hôtes compromis, dans **ACC (ACC)** > **Threat Activity (Activités des menaces)**, agrège les Événements corrélés et les trie par niveau de gravité. Il affiche l'adresse IP/utilisateur source qui a déclenché l'événement, l'objet de corrélation qui correspondait et le nombre de correspondances de l'objet. Utilisez le lien du nombre de correspondances pour accéder aux détails de la preuve de correspondance.




Pour plus d'informations, reportez-vous à aux sections Utilisation du moteur de corrélation automatique et Utilisation de l'Application Command Center (centre de commande de l'application - ACC).

# Captures de paquets

Tous les pare-feu Palo Alto Networks vous permettent de prendre des captures de paquets (pcaps) du trafic qui traverse l'interface de gestion et les interfaces réseau sur le pare-feu. Lorsque vous capturez des paquets sur le plan de données, une Désactivation du délestage matériel peut être nécessaire pour s'assurer que le pare-feu capture tout le trafic.

***La capture de paquets peut être très gourmande en ressources processeur et réduire les performances du pare-feu. N'utilisez cette fonctionnalité que lorsque cela est nécessaire et assurez-vous de la désactiver après avoir collecté les paquets requis.***

- Types de captures de paquets
- Désactivation du délestage matériel
- Capture de paquets personnalisée
- Capture de paquets de menaces
- Capture de paquets d'application
- Capture de paquets sur l'interface de gestion

## Types de captures de paquets

Vous pouvez activer différents types de captures de paquets différents, en fonction de ce que vous devez faire :

- **Capture de paquets personnalisée** : le pare-feu capture des paquets pour l'ensemble du trafic ou du trafic spécifique en fonction des filtres définis. Par exemple, vous pouvez configurer le pare-feu pour capturer uniquement les paquets depuis et vers une adresse IP source et de destination ou un port spécifique. Vous pouvez ensuite utiliser les captures de paquets pour résoudre des problèmes liés au réseau ou pour collecter des attributs d'application vous permettant d'écrire des signatures d'applications personnalisées ou pour demander une signature d'application à Palo Alto Networks. Reportez-vous à la section Capture de paquets personnalisée.
- **Capture de paquets de menace** : le pare-feu capture des paquets lorsqu'il détecte un virus, un logiciel espion ou une vulnérabilité. Vous pouvez activer cette fonctionnalité dans les profils de sécurité Antivirus, Antispyware et Protection contre les vulnérabilités. Un lien permettant d'afficher ou d'exporter les captures de paquets s'affiche dans la deuxième colonne du journal des menaces. Ces captures de paquets fournissent le contexte d'une menace qui vous permet de déterminer si une attaque est réussie ou d'en savoir plus sur les méthodes utilisées par une personne malveillante. Vous pouvez également envoyer ce type de pcap à Palo Alto Networks pour qu'une menace soit de nouveau analysée si vous pensez qu'il s'agit d'un faux positif (false-positive) ou faux négatif (false-negative). Reportez-vous à la section Capture de paquets de menaces.
- **Capture de paquets d'application** : le pare-feu capture des paquets en fonction d'une application spécifique ou des filtres définis. Un lien permettant d'afficher ou d'exporter les captures de paquets s'affiche dans la deuxième colonne des journaux du trafic pour le trafic correspondant à la règle de capture de paquets. Reportez-vous à la section Capture de paquets d'application.
- **Capture de paquets d'interface de gestion** : le pare-feu capture des paquets sur l'interface de gestion (MGT). Les captures de paquets sont utiles lors du dépannage de services qui traversent

l'interface, comme l'authentification de gestion de pare-feu vers Services d'authentification externes, les mises à jour logicielles et du contenu, le transfert des journaux, la communication avec des serveurs SNMP, et les requêtes d'authentification pour GlobalProtect et le portail d'authentification. Reportez-vous à la section Capture de paquets sur l'interface de gestion.

- **Capture de paquets d'événements GTP** : le pare-feu capture un seul événement GTP, comme GTP dans GTP, usurpation de l'adresse IP de l'utilisateur final et messages GTP anormaux pour faciliter la résolution des problèmes de GTP pour les opérateurs de réseaux mobiles. Activez la capture des paquets dans un profil de protection de réseau mobile.

## Désactivation du délestage matériel

Les captures de paquets pour le trafic qui passe par les ports de données du réseau sur un pare-feu Palo Alto Networks sont effectuées par le CPU du plan de données. Pour capture le trafic qui passe par l'interface de gestion, vous devez procéder à une Capture de paquets sur l'interface de gestion. Dans ce cas, la capture de paquets est menée sur le plan de gestion.

Lorsqu'une capture de paquets est menée sur le plan de données, le filtre de capture des paquets est utilisé différemment par l'étape d'entrée, comparativement aux étapes de capture de pare-feu, de l'abandon et de la sortie. L'étape d'entrée utilise le filtre de capture des paquets pour copier les paquets individuels qui correspondent au filtre afin de capturer le fichier. En cas d'échec de l'analyse syntaxique, les paquets sont abandonnés avant d'être saisis. Les étapes de capture du pare-feu, de l'abandon et de la sortie utilisent le même filtre de capture des paquets pour marquer toutes les nouvelles sessions qui sont associées au filtre. Comme chaque session (consignée dans les tables de sessions) identifie tant des connexions client vers serveur que des connexions serveur vers client, tout trafic, peu importe son sens, qui correspond à la session marquée sera copié dans les fichiers de capture de l'étape pare-feu et de l'étape transmission. De même, tout trafic abandonné (étape après la réception), peu importe le sens, qui correspond à une session marquée sera copié dans un fichier de capture de l'étape d'abandon.

Sur les modèles de pare-feu qui comprennent un processeur réseau, le trafic qui correspond à des critères prédéterminés par Palo Alto Networks peut être délesté aux fins de traitement par le processeur réseau. Un tel trafic délesté n'atteindra pas le CPU du plan de données et, par conséquent, ne sera pas capturé. Pour capturer le trafic délesté, vous devez utiliser la CLI pour désactiver la fonction de délestage du matériel.

Les types courants de trafic qui peuvent faire l'objet d'un délestage comprennent le trafic SSH et SSL non déchiffré (qui, en raison du chiffrement, ne peut être inspecté utilement au-delà de la configuration de session SSL/SSH initiale), les protocoles réseau (comme OSPF, BGP, RIP) et le trafic qui correspond à une politique de contrôle prioritaire sur l'application. Certains types de trafic ne seront jamais délestés, tels qu'ARP, l'ensemble du trafic non IP, IPSec et les sessions VPN. Les paquets SYN, FIN et RST individuels, même pour le trafic de session qui a été délesté, ne seront jamais délestés et seront toujours transmis via le CPU du plan de données, une fois qu'ils auront été reconnus en tant que tel par le processeur réseau.

*Le délestage matériel est pris en charge sur les pare-feu suivants : Pare-feu PA-3200 Series, PA-5200 Series et PA-7000 Series.*

*La désactivation du délestage matériel pourrait augmenter l'utilisation du processeur du plan de données. Si l'utilisation du processeur du plan de données est déjà élevée, vous souhaiterez peut-être planifier une fenêtre de maintenance avant de désactiver le délestage matériel.*

**STEP 1 |** Désactivez le délestage matériel en exécutant la commande CLI suivante :

```
admin@PA-7050>set session offload no
```

**STEP 2 |** Une fois que le pare-feu a capturé le trafic requis, activez le délestage matériel en exécutant la commande CLI suivante :

```
admin@PA-7050>set session offload yes
```

## Capture de paquets personnalisée

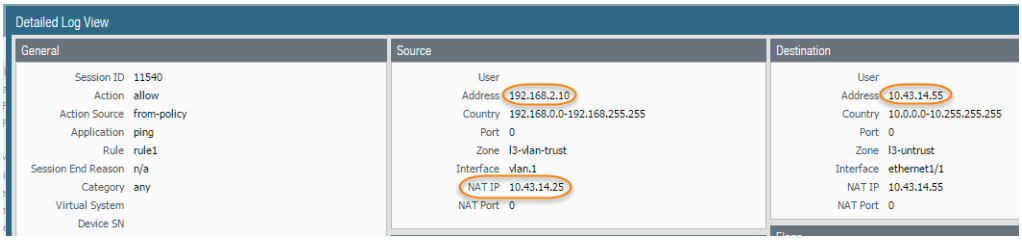
La capture de paquets personnalisée vous permet de définir le trafic capturé par le pare-feu. Pour vous assurer de capturer l'ensemble du trafic, une Désactivation du délestage matériel peut être nécessaire.

**STEP 1 |** Avant de commencer une capture de paquets, identifiez les attributs du trafic que vous souhaitez capturer.

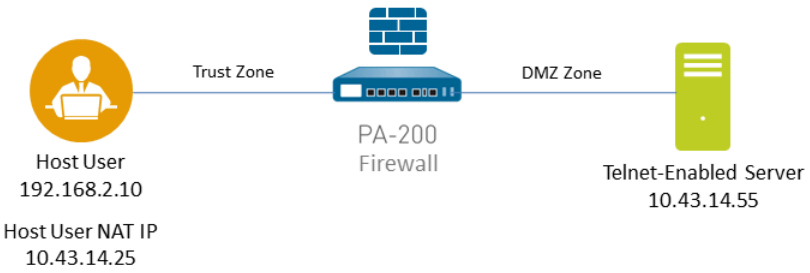
Par exemple, pour déterminer l'adresse IP source, l'adresse IP NAT source et l'adresse IP de destination du trafic entre deux systèmes, exécutez une commande ping du système source vers le système de destination. Une fois la commande ping exécutée, accédez à **Monitor (Surveillance)** > **Traffic (Trafic)** et recherchez le journal du trafic des deux systèmes. Cliquez sur

l'icône **Detailed Log View (Vue détaillée du journal)** située dans la première colonne du journal et notez l'adresse source, l'adresse IP NAT source et l'adresse de destination.




Dans l'exemple suivant, nous utiliserons une capture de paquets pour résoudre un problème de connectivité Telnet entre un utilisateur de la zone approuvée et un serveur de la zone DMZ.




**STEP 2 |** Définissez des filtres de capture de paquets pour que le pare-feu ne capture que le trafic pertinent pour vous.

L'utilisation de filtres vous permet de retrouver plus facilement les informations dont vous avez besoin dans la capture de paquets et réduit la puissance de traitement requise par le pare-feu

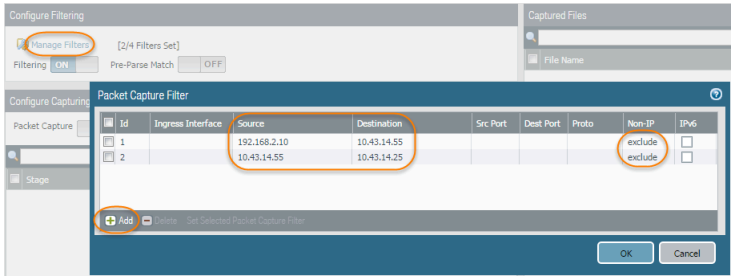
pour effectuer la capture de paquets. Pour capturer l'ensemble du trafic, ne définissez pas de filtres et conservez l'option de filtre désactivée.

Par exemple, si vous avez configuré NAT sur le pare-feu, vous devrez appliquer deux filtres. Le premier filtrant sur l'adresse IP source pré-NAT vers l'adresse IP de destination et le second filtrant du serveur de destination vers l'adresse IP NAT source.

1. Sélectionnez **Monitor (Surveillance)** > **Packet Capture (Capture de paquets)**.
2. Cliquez sur **Clear All Settings (Effacer tous les paramètres)** au bas de la fenêtre pour effacer tous les paramètres de capture existants.
3. Cliquez sur **Manage Filters (Gérer les filtres)**, puis sur **Add (Ajouter)**.
4. Sélectionnez **Id** 1 puis, dans le champ **Source**, saisissez l'adresse IP source qui vous intéresse et, dans le champ **Destination**, saisissez une adresse IP de destination.

   Par exemple, saisissez l'adresse IP source **`192.168.2.10`** et l'adresse IP de destination **`10.43.14.55`**. Pour filtrer davantage la capture, définissez **Non-IP** sur **exclude (Exclure)** pour exclure le trafic non IP, le trafic de diffusion par exemple.
5. Cliquez sur **Add (Ajouter)** pour ajouter le deuxième filtre et sélectionnez **Id** 2.

   Par exemple, dans le champ **Source**, saisissez **`10.43.14.55`** et dans le champ **Destination**, saisissez **`10.43.14.25`**. Dans le menu déroulant **Non-IP**, sélectionnez **exclude (Exclure)**.




6. Cliquez sur **OK**.

**STEP 3 |** Définissez l'option **Filtering (Filtrage)** sur **On (Activé)**.

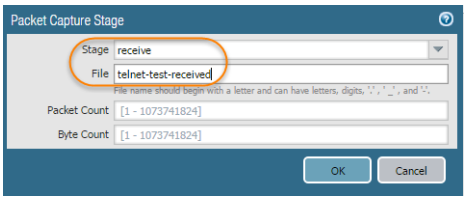
 

**STEP 4 |** Spécifiez la ou les étapes du trafic qui déclenchent la capture de paquets, ainsi que le ou les noms de fichiers à utiliser pour stocker le contenu capturé. Pour obtenir une définition de chaque étape, cliquez sur l'icône **Help (Aide)** dans la page de capture de paquets.

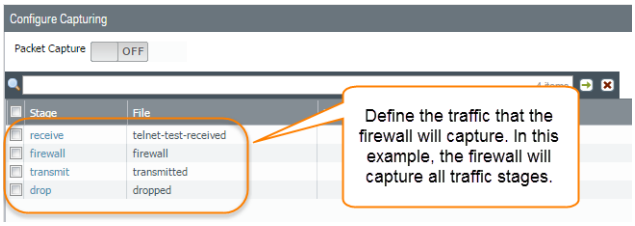
Par exemple, pour configurer toutes les étapes de capture de paquets et définir un nom de fichier pour chaque étape, procédez comme suit :

1. Cliquez sur **Add (Ajouter)** pour ajouter une **Stage (Étape)** à la configuration de la capture de paquets et définissez un nom de **File (Fichiers)** pour la capture de paquets obtenue.

   Par exemple, sélectionnez **receive (Recevoir)** comme **Stage (Étape)** et définissez le nom de **File (Fichier)** sur telnet-test-received.

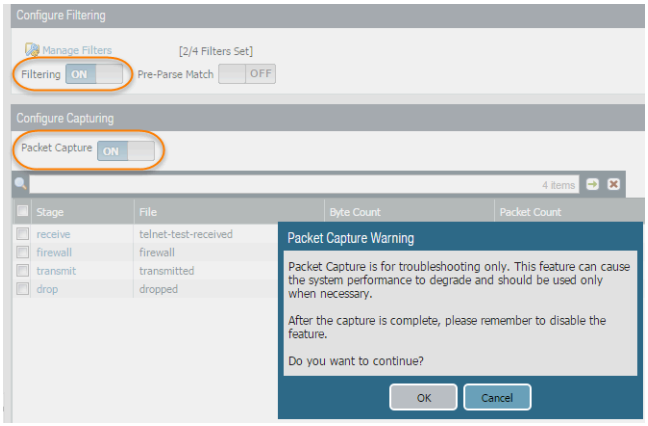



2. Ensuite, cliquez sur **Add (Ajouter)** pour ajouter chaque **Stage (Étape)** à capturer (**firewall (Pare-feu)**, **transmit (Transmettre)** et **drop (Abandonner)**), puis définissez un nom de **File (Fichier)** pour chaque étape.




**STEP 5 |** Définissez l'option **Packet Capture (Capture de paquets)** sur **On (Activé)**.

Le pare-feu ou l'appareil vous prévient que des ralentissements de performance sont à prévoir ; acceptez l'avertissement en cliquant sur **OK**. Si vous définissez des filtres, la capture de paquets ne doit avoir qu'un faible impact sur les performances, mais vous devez toujours définir la capture de paquets sur **Off (Désactivé)** lorsque le pare-feu a capturé les données que vous souhaitez analyser.



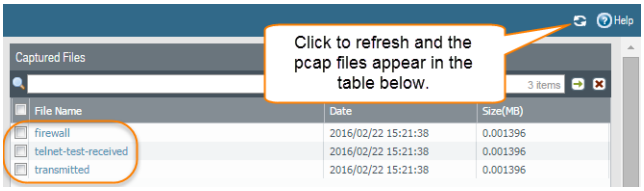

 

**STEP 6 |** Générez du trafic correspondant aux filtres que vous avez définis.

Pour cet exemple, générez du trafic du système source vers le serveur Telnet en exécutant la commande suivante sur le système source (192.168.2.10) :

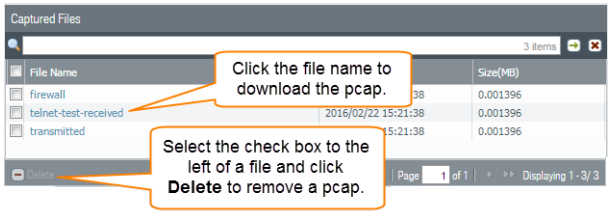
```
telnet 10.43.14.55
```

**STEP 7 |** Définissez la capture de paquets sur **OFF (Désactivé)**, puis cliquez sur l'icône d'actualisation pour afficher les fichiers de capture de paquets.



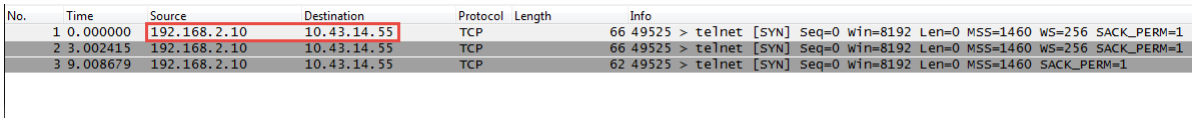

Notez que, dans cet exemple, aucun paquet n'a été abandonné ; le pare-feu n'a donc pas créé de fichier pour l'étape d'abandon.

**STEP 8 |** Téléchargez les captures de paquets en cliquant sur le nom de fichier dans la colonne Nom du fichier.




**STEP 9 |** Affichez les fichiers de capture de paquets à l'aide d'un analyseur de paquets réseau.

Dans cet exemple, le fichier de capture de paquets received.pcap indique un échec de session Telnet entre le système source à l'adresse 192.168.2.10 et le serveur Telnet à l'adresse 10.43.14.55. Le système source a envoyé la requête Telnet au serveur, mais le serveur n'a pas répondu. Dans cet exemple, Telnet n'est peut-être pas activé sur le serveur. Vérifiez le serveur.




**STEP 10 |** Activez le service Telnet sur le serveur de destination (10.43.14.55) et activez la capture de paquets pour effectuer une nouvelle capture.

**STEP 11 |** Générez du trafic qui déclenchera la capture de paquets.

Rétablissez la session Telnet entre le système source et le serveur Telnet.

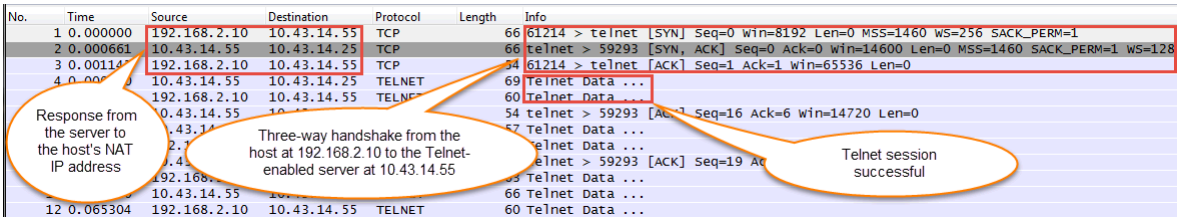
```
telnet 10.43.14.55
```

**STEP 12 |** Téléchargez et ouvrez le fichier received.pcap et affichez-le dans un analyseur de paquets réseau.

La capture de paquets suivante indique maintenant la réussite d'une session Telnet entre l'utilisateur hôte à l'adresse 192.168.2.10 et le serveur Telnet à l'adresse 10.43.14.55.

*L'adresse NAT (10.43.14.25) apparaît également. Lorsque le serveur répond, il le fait vers l'adresse NAT. Vous pouvez constater que la session a réussi, comme indiqué par l'établissement de la connexion en 3 étapes entre l'hôte et le serveur. Vous voyez ensuite les données Telnet.*




# Capture de paquets de menaces

Pour configurer le pare-feu afin qu'il effectue une capture de paquets (pcap) lorsqu'il détecte une menace, activez l'option de capture de paquets dans les profils de sécurité Antivirus, Antispyware et Protection contre les vulnérabilités.

**STEP 1 |** Activez l'option de capture de paquets dans le profil de sécurité.

Certains profils de sécurité vous permettent de définir une capture d'un paquet ou une capture étendue. Si vous choisissez Capture étendue, définissez la longueur de capture. Ceci permet au pare-feu de capturer plus de paquets pour fournir plus de contexte lié à la menace.

*Si l'action d'une menace donnée est autorisé, le pare-feu ne déclenche pas de journal des menaces et ne capture pas de paquets. Si l'action est une alerte, vous pouvez régler la capture de paquets sur un seul paquet ou capture étendue. Toutes les actions de blocage (abandon, blocage et redémarrage) capturent un seul paquet. Le package de contenu sur le périphérique détermine l'action par défaut.*

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)**, puis activez l'option de capture de paquets pour les profils pris en charge comme suit :
   - **Antivirus** : sélectionnez un profil Antivirus personnalisé puis, dans l'onglet **Antivirus**, cochez la case **Packet Capture (Capture de paquets)**.
   - **Anti-Spyware (Antispyware)** : sélectionnez un profil Antispyware personnalisé, cliquez sur l'onglet **DNS Signatures (Signatures DNS)** puis, dans la liste déroulante **Packet Capture (Capture de paquets)**, sélectionnez **single-packet (Un paquet)** ou **extended-capture (Capture étendue)**.
   - **Vulnerability Protection (Protection contre les vulnérabilités)** : sélectionnez un profil Protection contre les vulnérabilités puis, dans l'onglet **Rules (Règles)**, cliquez sur **Add (Ajouter)** pour ajouter une nouvelle règle ou choisissez-en une existante. Définissez

**Packet Capture (Capture de paquets)** sur **single-packet (Un paquet)** ou sur **extended-capture (Capture étendue)**.

*Notez que si des exceptions de signatures sont définies dans le profil, cliquez sur l'onglet **Exceptions** puis, dans la colonne **Packet Capture (Capture de paquets)** d'une signature, définissez **single-packet (Un paquet)** ou **extended-capture (Capture étendue)**.*

2. (Facultatif) Si vous avez sélectionné **extended-capture (Capture étendue)** pour l'un des profils, définissez la longueur de capture de paquets étendue.
   1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Content-ID (Content-ID)** et modifiez les paramètres de Content-ID.
   2. Dans la section **Extended Packet Capture Length (packets) (Longueur de capture de paquets étendue (paquets)**), spécifiez le nombre de paquets que le pare-feu capturera (plage de 1 à 50, par défaut 5).
   3. Cliquez sur **OK**.

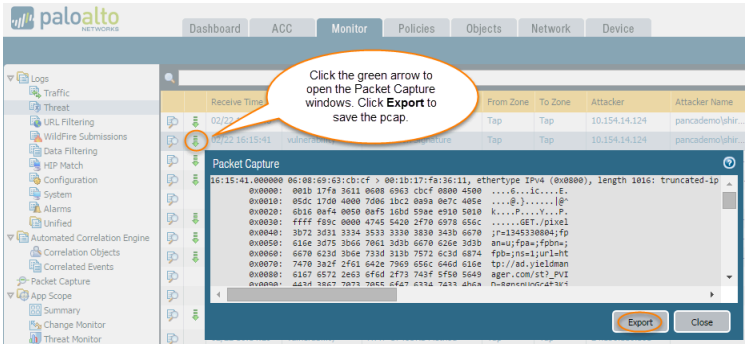
**STEP 2 |** Ajoutez le profil de sécurité (avec la capture de paquets activée) à une règle de Politique de sécurité.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis choisissez une règle.
2. Sélectionnez l'onglet **Actions (Actions)**.
3. Dans la section Profile Settings (Paramètres de profil), sélectionnez un profil dans lequel la capture de paquets est activée.

   Par exemple, cliquez sur la liste déroulante **Antivirus** et sélectionnez un profil dans lequel la capture de paquets est activée.

**STEP 3 |** Affichez/exportez la capture de paquets du journal des menaces.

1. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menace)**.
2. Dans l'entrée de journal qui vous intéresse, cliquez sur l'icône de capture de paquets verte dans la deuxième colonne. Affichez directement la capture de paquets ou **Export (Exporter)** la capture de paquets vers votre système.




# Capture de paquets d'application

Les rubriques suivantes décrivent les deux manières vous permettant de configurer le pare-feu pour capturer des paquets d'application :

- Capture de paquets pour des applications inconnues

- Capture de paquets d'application personnalisée

## Capture de paquets pour des applications inconnues

Les pare-feu Palo Alto Networks génèrent automatiquement une capture de paquets pour des sessions contenant une application que le pare-feu ne parvient pas à identifier. Normalement, les seules applications qui sont classées dans le trafic inconnu (tcp, udp ou non-syn-tcp) sont des applications disponibles dans le commerce qui n'ont pas encore de signatures App-ID, des applications internes ou personnalisées sur votre réseau, ou des menaces potentielles. Vous pouvez utiliser ces captures de paquets pour collecter plus de contexte lié à l'application inconnue ou utiliser les informations pour rechercher d'éventuelles menaces dans le trafic. Vous pouvez également gérer des applications personnalisées ou inconnues en les contrôlant à l'aide d'une politique de sécurité ou en écrivant une signature d'application personnalisée puis en créant une règle de sécurité basée sur la signature personnalisée. Si l'application est une application commerciale, vous pouvez envoyer la capture de paquets à Palo Alto Networks pour la création d'une signature App-ID.

**STEP 1 |** Vérifiez que la capture de paquets d'application inconnue est activée (cette option est activée par défaut).

1. Pour afficher le paramètre de capture d'application inconnue, exécutez la commande CLI suivante :

```
admin@PA-220>show running application setting | match “Unknown
 capture”
```

2. Si l'option de capture de paquets inconnus est désactivée, activez-la :

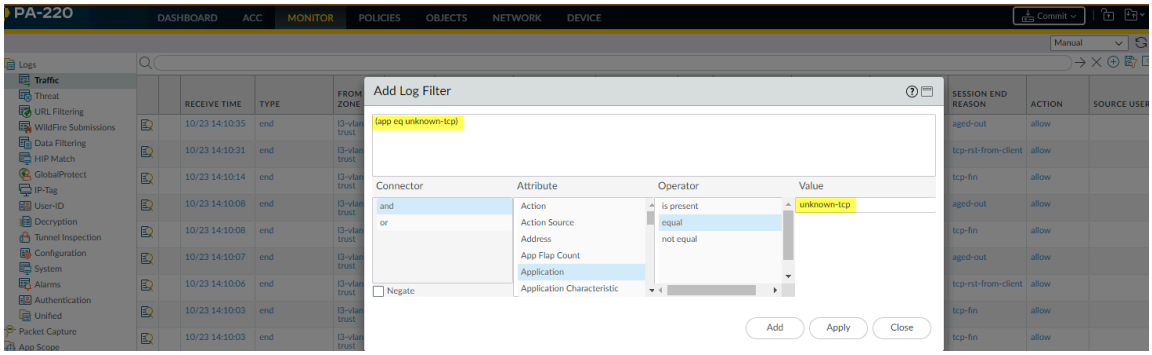
```
admin@PA-220>set application dump-unknown yes
```

**STEP 2 |** Recherchez des application TCP et UDP inconnues en filtrant les journaux du trafic.

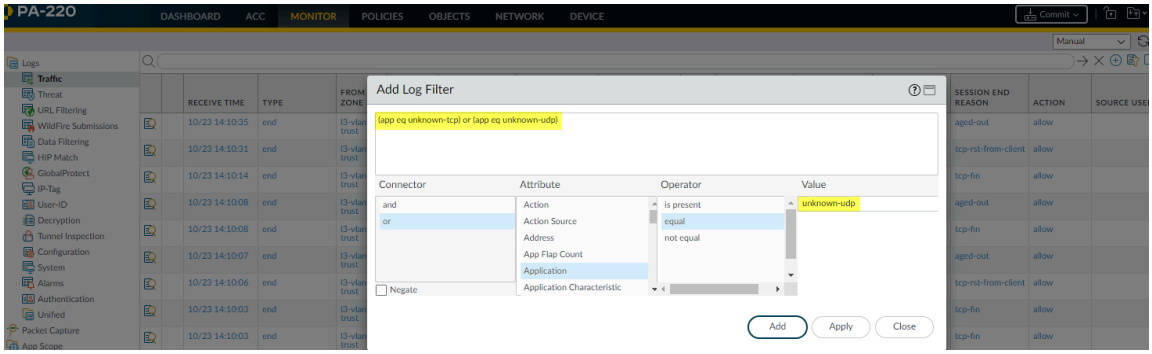
1. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menace)**.
2. Cliquez sur **Add Filter (Ajouter un filtre)**, créez la portion TCP inconnue du filtre (**Connector (Connecteur)** = « and », **Attribute (Attribut)** = « Application », **Operator**

**(Opérateur)** = « equal », et saisissez « unknown-tcp » comme **Value (Valeur)**), puis cliquez sur **Add (Ajouter)** pour ajouter la requête au filtre.

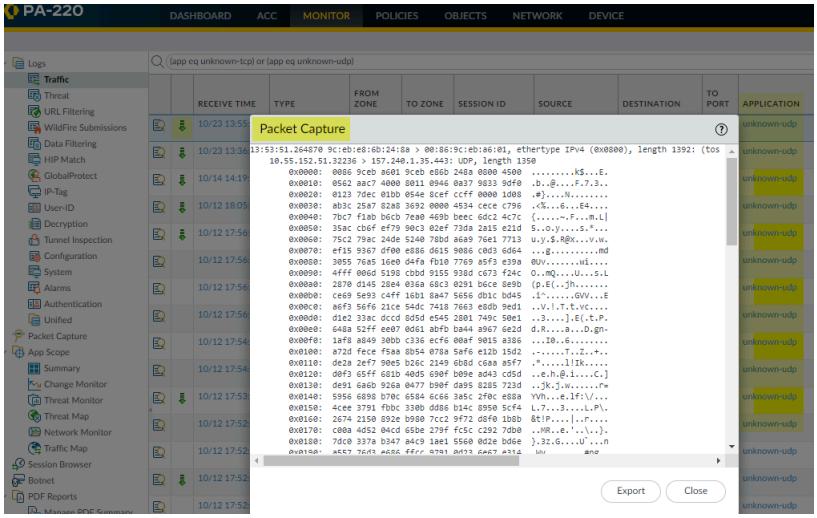



3. Créez la portion UDP inconnue du filtre (**Connector (Connecteur)** = « or », **Attribute (Attribut)** = « Application », **Operator (Opérateur)** = « equal », et saisissez « unknown-udp » comme **Value (Valeur)**), puis cliquez sur **Add (Ajouter)** pour ajouter la requête au filtre.




4. Cliquez sur **Apply (Appliquer)** pour placer le filtre dans le champ de requête de l'écran de journal.

**STEP 3 |** Cliquez sur la flèche **Apply Filter (Appliquer le filtre)** à côté du champ de requête pour exécuter le filtre, puis cliquez sur l'icône de capture de paquets pour afficher la capture de paquets ou **Export (Exporter)** la capture vers votre système local.



## Capture de paquets d'application personnalisée

Vous pouvez configurer un pare-feu Palo Alto Networks pour effectuer une capture de paquets en fonction d'un nom d'application ou de filtres définis. Vous pouvez ensuite utiliser la capture de paquets pour résoudre les problèmes de contrôle d'une application. Lorsque vous configurez une capture de paquets d'application, utilisez le nom d'application défini dans la base de données App-ID. Vous pouvez afficher une liste de toutes les applications App-ID à l'aide d'Applipedia ou à partir de l'interface Web sur le pare-feu dans **Objects (Objets)** > **Applications**.

**STEP 1 |** À l'aide d'une application d'émulation de terminal, telle que PuTTY, lancez une session SSH sur le pare-feu.

**STEP 2 |** Activez la capture de paquets d'application et définissez des filtres.

```
admin@PA-220>set application dump on application <application-name>
 règle <nom-de-la-règle>
```

Par exemple, pour capturer des paquets pour l'application linkedin-base qui correspond à la règle de sécurité nommée Social Networking Apps, exécutez la commande CLI suivante :

```
admin@PA-220>set application dump on application linkedin-base rule
 "Social Networking Apps"
```

*Vous pouvez également appliquer d'autres filtres, comme l'adresse IP source et l'adresse IP de destination.*

**STEP 3 |** Affichez le résultat de capture de paquets pour vous assurer que les filtres appropriés sont appliqués. Le résultat s'affiche après que vous ayez activé la capture de paquets.

Le résultat suivant confirme que le filtrage de capture d'application est maintenant basé sur l'application linkedin-base pour le trafic qui correspond à la règle Social Networking Apps.

```
Application setting:
Application cache             : yes
Supernode                     : yes
Heuristics                    : yes
Cache Threshold               : 16
Bypass when exceeds queue limit: no
Traceroute appid              : yes
Traceroute TTL threshold      : 30
Use cache for appid           : no
Use simple appsigs for ident  : yes
Use AppID cache on SSL/SNI    : no
Unknown capture               : on
Max. unknown sessions         : 5000
Current unknown sessions      : 7
Application capture           : on
Max. application sessions     : 5000
Current application sessions  : 0
Application filter setting:
    Rule                      : Social Networking Apps
    From                      : any
    To                        : any
    Source                    : any
    Destination               : any
    Protocol                  : any
    Source Port               : any
    Dest. Port                : any
    Application               : linkedin-base

Current APPID Signature
   Memory Usage               : 16768  KB (Actual 16440  KB)
      TCP 1 C2S               : regex 11898  states
      TCP 1 S2C               : regex 4549   states
      UDP 1 C2S               : regex 4234   states
      UDP 1 S2C               : regex 1605   states

Alternate APPID Signature
   Memory Usage               : 16768  KB (Actual 16425  KB)
      TCP 1 C2S               : regex 11878  states
      TCP 1 S2C               : regex 4549   states
      UDP 1 C2S               : regex 4233   states
      UDP 1 S2C               : regex 1604   states
```

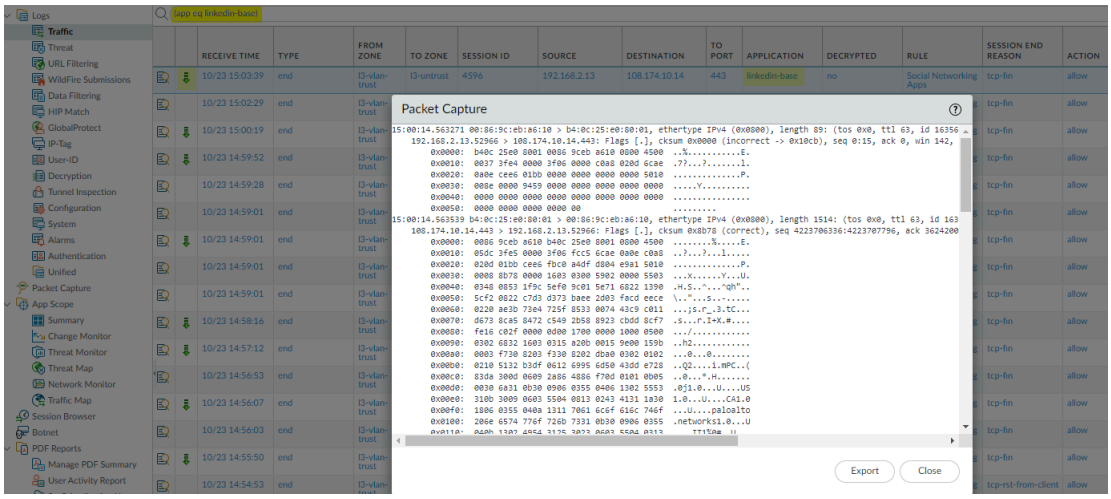
 

**STEP 4 |** Accédez à linkedin.com depuis un navigateur web et effectuez certaines tâches LinkedIn pour générer du trafic LinkedIn, puis exécutez la commande CLI suivante pour désactiver la capture de paquets d'application :

```
admin@PA-220>set application dump off
```

**STEP 5 |** Affichez/exportez la capture de paquets.

1. Connectez-vous à l'interface Web sur le pare-feu, puis sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)**.
2. Dans l'entrée de journal qui vous intéresse, cliquez sur l'icône de capture de paquets verte .
3. Affichez directement la capture de paquets ou **Export (Exportez)**-la vers votre ordinateur. La capture d'écran suivante illustre la capture de paquets linkedin-base.




# Capture de paquets sur l'interface de gestion

La commande CLI **tcpdump** vous permet de capture des paquets qui traversent l'interface de gestion (MGT) sur un pare-feu Palo Alto Networks.

*Chaque plate-forme dispose d'un nombre d'octets par défaut capturés par **tcpdump**. Les pare-feu PA-220 Series capturent 68 octets de données de chaque paquet ; les octets restants sont tronqués. Les pare-feux PA-7000 et VM-Series capturent 96 octets de données de chaque paquet. Pour définir le nombre de paquets capturés par **tcpdump**, utilisez l'option **snaplen** (snap length) (plage de 0 à 65 535). Définissez l'option **snaplen** sur 0 pour que le pare-feu utilise la longueur maximale requise pour capturer tous les paquets.*

**STEP 1 |** À l'aide d'une application d'émulation de terminal, telle que PuTTY, lancez une session SSH sur le pare-feu.

**STEP 2 |** Pour lancer une capture de paquets sur l'interface MGT, exécutez la commande suivante :

```
admin@PA-220>tcpdump filter “<filter-option> <IP-address>” snaplen
 length
```

Par exemple, pour capturer le trafic généré lorsqu'un administrateur s'authentifie sur le pare-feu avec RADIUS, filtrez sur l'adresse IP de destination du serveur RADIUS (10.5.104.99 dans cet exemple) :

```
admin@PA-220>tcpdump filter “dst 10.5.104.99” snaplen 0
```

Vous pouvez également filtrer sur src (adresse IP source), l'hôte, le réseau, et vous pouvez exclure du contenu. Par exemple, pour filtrer sur un sous-réseau et exclure tout le trafic SCP, SFTP et SSH (qui utilise le port 22), exécutez la commande suivante :

```
admin@PA-220>tcpdump filter “net 10.5.104.0/24 and not port 22”
 snaplen 0
```

*Chaque fois que la commande **tcpdump** effectue une capture de paquets, il stocke le contenu dans un fichier nommé mgmt.pcap. Ce fichier est remplacé à chaque exécution de la commande **tcpdump**.*

**STEP 3 |** Lorsque le trafic pertinent pour vous a traversé l'interface MGT, appuyez sur Ctrl + C pour arrêter la capture.

**STEP 4 |** Affichez la capture de paquets en exécutant la commande suivante :

```
admin@PA-220> view-pcap mgmt-pcap mgmt.pcap
```

Le résultat suivant affiche la capture de paquets entre le port MGT (10.5.104.98) et le serveur RADIUS (10.5.104.99) :

```
09:55:29.139394 IP 10.5.104.98.43063 > 10.5.104.99.radius: RADIUS,
 Access Request (1), id: 0x00 length: 89
 09:55:29.144354 arp reply 10.5.104.98 is-at 00:25:90:23:94:98 (oui
 Unknown)
 09:55:29.379290 IP 10.5.104.98.43063 > 10.5.104.99.radius: RADIUS,
 Access Request (1), id: 0x00 length: 70
 09:55:34.379262 arp who-has 10.5.104.99 tell 10.5.104.98
```

**STEP 5 |** (Facultatif) Exportez la capture de paquets du pare-feu à l'aide de SCP (ou TFTP). Par exemple, pour exporter la capture de paquets à l'aide de SCP, exécutez la commande suivante :

```
admin@PA-220>scp export mgmt-pcap from mgmt.pcap
 to <username@host:path>
```

Par exemple, pour exporter la pcap vers un serveur SCP à l'adresse 10.5.5.20 dans un dossier temporaire nommé temp-SCP, exécutez la commande suivante :

```
admin@PA-220>scp export mgmt-pcap from mgmt.pcap to
 admin@10.5.5.20:c:/temp-SCP
```

Saisissez le nom de connexion et le mot de passe du compte sur le serveur SCP, afin de permettre au pare-feu de copier la capture de paquets dans le dossier c:\temp-SCP sur le serveur SCP.

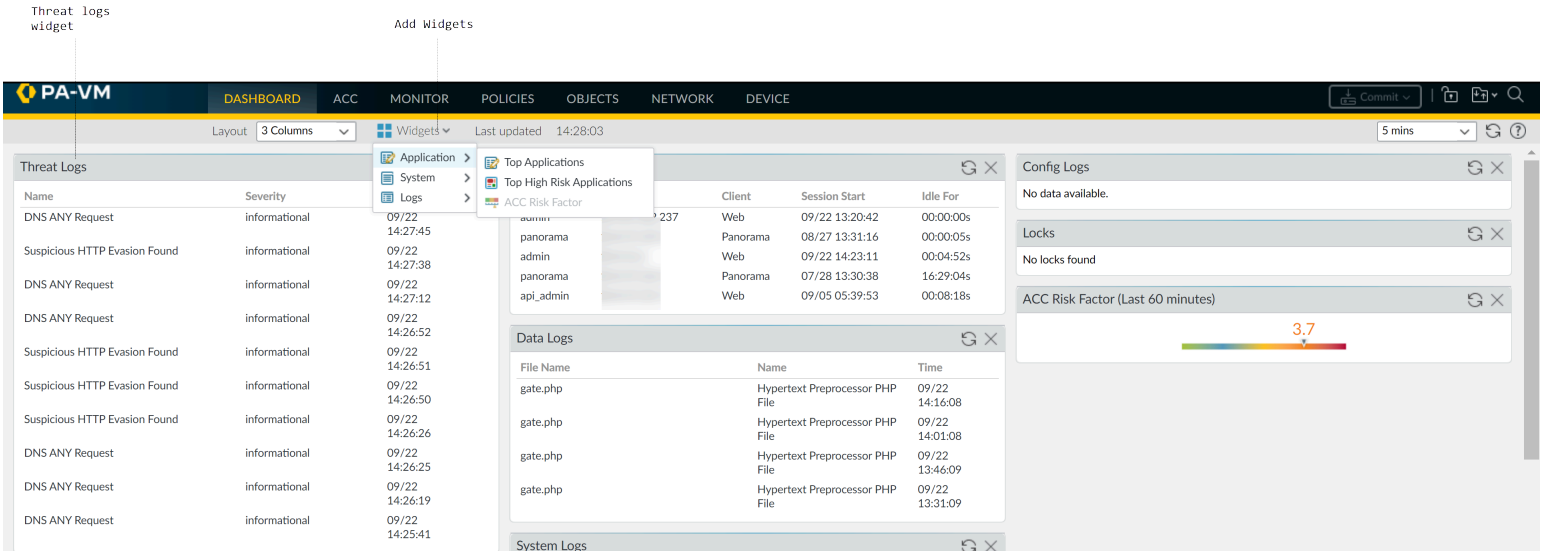
**STEP 6 |** Vous pouvez maintenant afficher les fichiers de capture de paquets à l'aide d'un analyseur de paquets réseau, Wireshark par exemple.

# Surveillance des applications et des menaces

Tous les pare-feu Palo Alto Networks de dernière génération sont équipés de la technologie App-ID, qui identifie les applications traversant votre réseau, quel que soit le protocole, le cryptage ou la tactique évasive. L'Utilisation de l'Application Command Center (centre de commande de l'application - ACC) est alors possible pour surveiller les applications. L'ACC dresse un récapitulatif graphique des données d'une variété de bases de données de journaux afin de mettre en évidence les applications traversant votre réseau, leurs utilisateurs et leur incidence potentielle sur la sécurité. L'ACC est mis à jour de manière dynamique, à l'aide de la classification continue du trafic par App-ID ; si une application change de port ou de comportement, App-ID continue à voir le trafic et affiche les résultats dans l'ACC. Une visibilité supplémentaire des catégories d'URL, des menaces et des données offre une analyse complète et globale de l'activité du réseau. L'ACC vous permet très rapidement d'en savoir plus sur le trafic traversant le réseau et de traduire ensuite ces informations en une politique de sécurité plus avisée.

L' est ensuite possible Utilisation du tableau de bord pour surveiller le réseau.




Passez en revue Content Delivery Network Infrastructure (infrastructure du réseau de diffusion de contenu) pour vérifier si les événements enregistrés sur le pare-feu présentent un risque de sécurité. Le récapitulatif des données de renseignements AutoFocus révèle la présence de propriétés, d'activités ou de comportements associés aux journaux dans votre réseau et à plus grande échelle ainsi que le verdict WildFire et les balises AutoFocus s'y rapportant. En détenant une souscription AutoFocus active, vous pouvez utiliser ces informations pour créer des Alertes AutoFocus spécialisées qui suivent des menaces spécifiques sur votre réseau.

# Afficher et gérer les journaux

Un journal est un fichier horodaté généré automatiquement qui fournit une piste d'audit pour des événements systèmes qui surviennent sur le pare-feu ou pour des événements de trafic réseau que le pare-feu surveille. Les entrées de journal contiennent des ***artefacts***, qui sont des propriétés, des activités ou des comportements associés avec l'événement journalisé, tels que le type d'application ou l'adresse IP d'un pirate. Chaque type de journal enregistre des informations sur un type d'événement distinct. Par exemple, le pare-feu génère un journal des menaces pour y consigner le trafic qui correspond à la signature d'un logiciel espion, d'une vulnérabilité ou d'un virus, ou une attaque DoS qui correspond aux seuils configurés pour le déclenchement d'une analyse de port ou d'une activité de balayage de l'hôte sur le pare-feu.

- Types de journaux et Niveaux de gravité
- Afficher des journaux
- Journaux de filtrage
- Journaux d'exportation
- Configuration de quotas de stockage et de périodes d'expiration des journaux
- Planification des exportations de journaux vers un serveur SCP ou FTP

## Types de journaux et Niveaux de gravité

Vous pouvez voir les types de journaux suivants dans les pages **Monitor (Surveillance)** > **Logs (Journaux)**.

- Journaux du trafic
- Journaux des menaces
- Journaux de filtrage des URL
- Journaux des envois WildFire
- Journaux de filtrage des données
- Journaux de corrélation
- Journaux d'inspection des tunnels
- Journaux de configuration
- Journaux systèmes
- Journaux de correspondance HIP
- Journaux GlobalProtect
- Journaux des indicateurs d'adresse IP
- Journaux User-ID
- Journaux de décryptage
- Journaux des alarmes
- Journaux d'authentification
- Journaux unifiés

## Journaux du trafic

Les journaux de trafic affichent une entrée au début et à la fin de chaque session. Chaque entrée contient les informations suivantes : la date et l'heure, les zones source et de destination, les groupes d'adresses dynamiques source et de destination, des adresses et des ports, le nom de l'application, la règle de sécurité appliquée au flux de trafic, l'action de la règle (autoriser, refuser ou supprimer), l'interface d'entrée et de sortie, ainsi que le nombre d'octets et le motif de fin de session.

***Un groupe d'adresses dynamiques n'apparaît dans un journal que si la règle à laquelle le trafic correspond comprend un groupe d'adresses dynamiques. Si une adresse IP apparaît dans plus d'un groupe d'adresses dynamiques, le pare-feu affiche jusqu'à cinq groupes d'adresses dynamiques dans les journaux avec l'adresse IP source***

La colonne Type (Type) indique si l'entrée correspond au début ou à la fin de la session. La colonne Action (Action) indique si le pare-feu a autorisé, refusé ou supprimé la session. Une suppression indique que la règle de sécurité qui bloquait le trafic a spécifié n'importe quelle application, alors qu'un refus indique que la règle a identifié une application spécifique. Si le pare-feu supprime le trafic avant d'identifier l'application, comme lorsqu'une règle supprime l'ensemble du trafic d'un service spécifique, la colonne Application (Application) affiche non-applicable.

Cliquez sur en regard d'une entrée pour afficher des détails supplémentaires concernant une session, à savoir si une entrée ICMP regroupe plusieurs sessions entre une même source et destination (dans ce cas la valeur de la colonne Count (Nombre) sera supérieure à 1).

***Lorsque le journal de décryptage introduit dans PAN-OS 10.1 est désactivé, le pare-feu envoie des journaux HTTP/2 en tant que journaux de trafic. Toutefois, lorsque les journaux de décryptage sont activés, le pare-feu envoie des journaux HTTP/2 en tant que journaux d'inspection des tunnels (lorsque les journaux de décryptage sont désactivés, les journaux HTTP/2 sont envoyés en tant que journaux de trafic), vous devez donc vérifier les journaux d'inspection des tunnels plutôt que les journaux de trafic pour les événements HTTP/2.***

## Journaux des menaces

Les journaux des menaces affichent des entrées lorsque le trafic correspond à un des profils de sécurité associés à une règle de sécurité définie sur le pare-feu. Chaque entrée inclut les informations suivantes : date et heure ; type de menace (par exemple un virus ou un logiciel espion) ; description de la menace ou de URL (colonne Name (Nom)) ; zones source et de destination, adresses, groupes d'adresses dynamiques source et de destination, et ports ; nom de l'application ; action d'alerte (par exemple autorisation ou blocage) ; et niveau de gravité.

***Un groupe d'adresses dynamiques n'apparaît dans un journal que si la règle à laquelle le trafic correspond comprend un groupe d'adresses dynamiques. Si une adresse IP apparaît dans plus d'un groupe d'adresses dynamiques, le pare-feu affiche jusqu'à cinq groupes d'adresses dynamiques dans les journaux avec l'adresse IP source***

Pour voir plus de détails sur des entrées du journal des menaces données :

- Cliquez sur en regard d'une entrée pour afficher des détails, à savoir si une entrée regroupe plusieurs menaces du même type entre une même source et destination (dans ce cas la valeur de la colonne Count [Nombre] sera supérieure à un).

- Si vous avez configuré le pare-feu pour qu'il prenne des captures de paquets, cliquez sur en regard d'une entrée pour accéder aux paquets capturés.

Le tableau suivant récapitule les niveaux de gravité des menaces :

| Sévérité | Description |
|---|---|
| **Critique** | Menaces graves, telles que celles affectant les installations par défaut des logiciels déployés à grande échelle et menant à la compromission des serveurs, dans lesquelles le code d'exploitation est largement accessible aux pirates. Le pirate n'a généralement pas besoin d'informations d'authentification spéciales ni de connaissances relatives à chaque victime, et la cible n'a pas besoin d'être manipulée au point d'effectuer des fonctions spéciales. |
| **Élevée** | Menaces pouvant devenir critiques mais ayant des facteurs atténuants; par exemple, elles peuvent être difficiles à exploiter, ne mènent pas à des privilèges élevés ou ne ciblent pas un grand nombre de victimes.<br>Les entrées du journal des envois WildFire qui ont reçu un verdict de fichier malveillant et dont l'action est définie sur allow (autoriser) sont journalisées sous le niveau de gravité Élevé. |
| **Moyenne** | Menaces mineures dans lesquelles l'incidence est minimisée, telles que les attaques DoS qui ne compromettent pas la cible ou les exploitations nécessitant qu'un pirate réside sur le même réseau local que la victime, affectent uniquement les configurations non standard ou les applications obscures, ou fournissent un accès très limité.<br>• Les entrées du journal des menaces ayant pour verdict la présence d'un fichier malveillant et une action de blocage ou d'alerte, en fonction de la gravité de la signature WildFire existante, sont journalisées sous le niveau de gravité Moyen. |
| **Faible** | Menaces à surveiller ayant très peu d'incidence sur l'infrastructure de l'entreprise. Celles-ci requièrent généralement un accès au système physique ou local et peuvent entraîner des problèmes DoS ou de confidentialité de la victime, ainsi qu'une fuite des informations.<br>• Les correspondances du profil de filtrage des données sont consignées sous le niveau de gravité Faible.<br>• Les entrées du journal des envois WildFire qui ont reçu un verdict de fichier indésirable, peu importe l'action, sont journalisées sous le niveau de gravité Faible. |
| **Informations** | Événements suspects qui ne constituent pas une menace immédiate, mais qui sont signalés pour attirer l'attention sur l'existence possible de problèmes plus graves.<br>• Les entrées du journal de filtrage des URL sont enregistrées sous le niveau de gravité Informations.<br>• Les entrées du journal des envois WildFire qui ont reçu un verdict de fichier bénin, peu importe l'action, sont journalisées sous le niveau de gravité Informations. |

| Sévérité | Description |
|---|---|
| | • Les entrées du journal des envois WildFire qui ont reçu n'importe quel verdict, et dont l'action est définie sur block (bloquer) et forward (transférer), sont journalisées sous le niveau de gravité Informations.<br>• Les entrées du journal des envois WildFire qui ont reçu un verdict quelconque et dont l'action est définie sur block (bloquer) sont journalisés sous le niveau de gravité Informations. |

## Journaux de filtrage des URL

Filtrage des URL les journaux affichent des entrées pour le trafic qui correspond aux profils de filtrage d'URL attachés aux règles de politique de sécurité ou aux catégories d'URL utilisées comme critères de correspondance dans les règles de politique de sécurité. Par exemple, le pare-feu génère un journal si une règle bloque l'accès à des sites Web ou des catégories de sites Web spécifiques ou si vous avez configuré une règle pour générer une alerte quand un utilisateur accède a un site Web.

## Journaux des envois WildFire

Le pare-feu transmet, pour analyse, des échantillons (liens de fichiers et de courriers électroniques) vers le cloud WildFire en fonction des paramètres du profil d'analyse WildFire (**Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **WildFire Analysis (Analyse WildFire)**). Une fois les analyses statique et dynamique de WildFire terminées, le pare-feu génère des entrées du journal des envois WildFire pour chaque échantillon qu'il transmet Les entrées du journal des envois WildFire comprennent l'action de pare-feu pour l'échantillon (autoriser ou bloquer), le verdict de WildFire pour l'échantillon envoyé et le niveau de gravité de l'échantillon.

Le tableau suivant récapitule les verdicts WildFire :

| Verdict | Description |
|---|---|
| **Benign (Bénin)** | Indique que l'entrée a reçu un verdict d'analyse WildFire « bénin ». Les fichiers classés comme bénins sont sûrs et ne manifestent aucun comportement malveillant. |
| **Grayware (Logiciel indésirable)** | Indique que l'entrée a reçu un verdict d'analyse WildFire « logiciel indésirable ». Les fichiers classés en tant que logiciel indésirable n'entraînent pas une menace de sécurité directe, mais peuvent présenter un comportement indiscret. Les logiciels indésirables peuvent inclure les logiciels publicitaires, les logiciels espions et les Browser Helper Objects (objets de l'assistant du navigateur ; BHO). |
| **Hameçonnage** | Indique que WildFire a attribué un lien à un verdict d'analyse de hameçonnage. Un verdict de hameçonnage indique que le site vers lequel le lien dirige les utilisateurs a affiché une activité de hameçonnage des informations d'identification. |
| **Malicious (Malveillant)** | Indique que l'entrée a reçu un verdict d'analyse WildFire « malveillant ». Les échantillons qui sont classés comme étant malveillant peuvent représenter une menace de sécurité. Les logiciels malveillants peuvent inclure les virus, C2 (commande et contrôle), les vers, les chevaux de Troie, Remote Access Tools (outils à accès distant - RAT), les rootkits et les Botnets. Pour des échantillons qui sont |

| Verdict | Description |
|---|---|
| | identifiés en tant que logiciel malveillant, le cloud WildFire génère et distribue une signature qui empêche toute exposition ultérieure.<br><br>*Les échantillons C2 sont classés comme C2 dans le rapport d'analyse WildFire et d'autres produits Palo Alto Networks qui s'appuient sur les données d'analyse WildFire; cependant, ce verdict est traduit et classé comme malveillant par le pare-feu.* |

## Journaux de filtrage des données

Les journaux de filtrage des données présentent les entrées se rapportant aux politiques de sécurité qui permettent d'empêcher les informations sensibles telles que les numéros de carte de crédit de quitter la zone protégée par le pare-feu. Pour plus d'informations sur la définition de profils de filtrage des données, reportez-vous à la section Filtrage des données.

Ce type de journal affiche également des informations relatives aux profils de blocage des fichiers. Par exemple, si une règle bloque les fichiers .exe, le journal montre les fichiers bloqués.

## Journaux de corrélation

Le pare-feu consigne un événement de corrélation lorsque les modèles et seuils définis dans un Objet Corrélation correspondent aux modèles de trafic sur votre réseau. Pour procéder à l'Interprétation des événements corrélés et pour afficher une vue graphique des événements, reportez-vous à la section Utilisation du widget Hôtes compromis de l'ACC.

Le tableau suivant récapitule les niveaux de gravité des journaux de corrélation :

| Sévérité | Description |
|---|---|
| **Critique** | Indique qu'un hôte a été compromis sur la base d'événements corrélés présentant un modèle de remontée. Par exemple, un événement critique est consigné lorsqu'un hôte ayant reçu un fichier avec un verdict malveillant de WildFire présente la même activité de commande et contrôle que celle observée dans le sandbox WildFire pour ce fichier malveillant. |
| **Élevée** | Indique qu'un hôte est très probablement compromis sur la base d'une corrélation entre plusieurs événements de menace, comme un logiciel malveillant détecté à un quelconque endroit du réseau qui correspond à l'activité de commande et contrôle générée par un hôte particulier. |
| **Moyenne** | Indique qu'un hôte est probablement compromis sur la base de la détection d'un ou plusieurs événements suspects, comme les consultations répétées d'URL malveillantes connues suggérant une activité de commande et contrôle à script. |
| **Faible** | Indique qu'un hôte est potentiellement compromis sur la base de la détection d'un ou plusieurs événements suspects, comme la consultation d'une URL malveillante ou d'un domaine DNS dynamique. |

| Sévérité | Description |
|---|---|
| **Informations** | Détecte un événement pouvant permettre d'identifier, dans l'agrégation, une activité suspecte ; chaque événement n'est pas nécessairement important. |

## Journaux d'inspection des tunnels

Les journaux d'inspection des tunnels sont comme des journaux de trafic pour les sessions de tunnel : ils affichent les entrées des sessions de tunnel non cryptées. Pour empêcher le double comptage, le pare-feu enregistre uniquement les flux internes dans les journaux de trafic, et envoie les sessions de tunnel dans les journaux d'inspection des tunnels. Les entrées du journal d'inspection des tunnels comprennent l'heure de réception (date et heure de réception du journal), l'ID du tunnel, le tag de surveillance, l'ID de session, la règle de sécurité appliquée à la session de tunnel, le nombre d'octets dans la session, l'ID de session parent (ID de session pour la session de tunnel), l'adresse source, l'utilisateur source et la zone source, l'adresse de destination, l'utilisateur de destination et la zone de destination.

***Lorsque les journaux de décryptage introduits dans PAN-OS 10.1 sont activés, le pare-feu envoie des journaux HTTP/2 en tant que journaux d'inspection des tunnels (lorsque les journaux de décryptage sont désactivés, les journaux HTTP/2 sont envoyés en tant que journaux de trafic), vous devez donc vérifier les journaux d'inspection des tunnels plutôt que les journaux de trafic pour les événements HTTP/2. Dans ce cas, vous devez également activer l'***inspection du contenu du tunnel ***pour obtenir l'App-ID pour le trafic HTTP/2.***

Cliquez sur la vue détaillée du journal pour afficher les détails d'une entrée, par exemple le protocole de tunnel utilisé, et l'indicateur précisant si le contenu du tunnel a été inspecté ou non. Seule une session ayant une session parent aura l'indicateur de tunnel inspecté défini, ce qui signifie que la session se trouve dans un tunnel-en-tunnel (deux niveaux d'encapsulation). Le premier en-tête extérieur d'un tunnel n'aura pas d'indicateur de tunnel inspecté défini.

## Journaux de configuration

Les journaux de configuration affichent des entrées pour des changements à la configuration du pare-feu. Chaque entrée inclut la date et l'heure, le nom d'utilisateur de l'administrateur, l'adresse IP correspondant à l'emplacement où l'administrateur a apporté la modification, le type de client (Web, CLI ou Panorama), le type de commande exécutée, l'état de la commande (réussite ou échec), le chemin de la configuration et les valeurs avant et après la modification.

## Journaux systèmes

Les journaux système affichent les entrées de chaque événement système qui est survenu sur le pare-feu. Chaque entrée inclut la date et l'heure, la gravité de l'événement et sa description. Le tableau suivant récapitule les niveaux de gravité des journaux système : Pour obtenir une liste partielle des messages des journaux et de leurs niveaux de gravité correspondants, reportez-vous à la section Événements du journal système.

| Sévérité | Description |
|---|---|
| **Critique** | Défaillances matérielles, notamment les basculements High Availability (haute disponibilité ; HA) et les échecs de liaison. |
| **Élevée** | Problèmes graves, notamment les connexions abandonnées avec des périphériques externes tels que les serveursLDAP et RADIUS. |
| **Moyenne** | Notifications de niveau intermédiaires telles que les mises à niveau du module antivirus. |
| **Faible** | Notifications de gravité mineure telles que les changements de mot de passe utilisateur. |
| **Informations** | Connexion/déconnexion, changement du nom ou du mot de passe administrateur, toute modification apportée à la configuration et tous les autres événements non couverts par les autres niveaux de gravité. |

## Journaux de correspondance HIP

La correspondance GlobalProtect Host Information Profile (profil d'informations sur l'hôte ; HIP) vous permet de recueillir des informations sur l'état de sécurité des périphériques finaux qui accèdent à votre réseau (par exemple, à savoir si le cryptage de disque est activé). Le pare-feu peut autoriser ou refuser l'accès à un hôte donné selon qu'il respecte, ou non, les règles de sécurité HIP que vous définissez. Les journaux de correspondance HIP affichent les flux de trafic qui correspondent à un Objet HIP ou à un Profil HIP que vous avez configuré pour le respect des règles.

## Journaux GlobalProtect

Les journaux GlobalProtect affichent les journaux suivants liés à GlobalProtect:

- Journaux système GlobalProtect

  Les journées d'événement d'authentification GlobalProtect restent dans **Monitor (Moniteur** > **Logs (Journaux)** > **System (Système)** ; cependant la colonne **Auth Method (Méthode d'authentification)** dans les journaux GlobalProtect affiche la méthode d'authentification utilisés pour les connexions.
- LSVPN/SATELLITE événements
- Journaux du portail et passerelles GlobalProtect
- Journaux du VPN sans client

## Journaux des indicateurs d'adresse IP

Les journaux des indicateurs d'adresse IP affichent comment et quant une adresse IP source est enregistrée ou désenregistrée sur le pare-feu et l'étiquette que le pare-feu a appliqué à l'adresse. De plus, chaque entrée de journal affiche le délai configuré (lorsqu'il est configuré) et la source des informations de mappage adresse IP/étiquette, comme les sources d'information VM de l'agent User-ID et l'auto-étiquetage. Voyez comment procéder à l'enregistrement dynamique des adresses IP et des étiquettes pour obtenir de plus amples renseignements.

## Journaux User-ID

User-id : les journaux affichent des informations sur les mappages d'adresse IP sur nom d'utilisateur et Horodatages d'authentification, comme les sources des informations de mappage et les différentes authentifications des utilisateurs. Vous pouvez utiliser ces informations pour résoudre les problèmes d'User-ID et les erreurs d'authentification. Par exemple, si le pare-feu applique la mauvaise règle de politique pour un utilisateur, vous pouvez afficher les journaux pour vérifier si cet utilisateur est mappé à la bonne adresse IP et si les associations de groupe sont correctes.

## Journaux de décryptage

Les Decryption Logs (Journaux de décryptage) affichent par défaut les entrées pour les communications TLS avortées et peuvent afficher les entrées pour les communications TLS réussies si vous les activez dans la politique de décryptage. Si vous autorisez les entrées pour les communications réussies, assurez-vous que vous disposez des ressources système (espace de journalisation) pour les journaux.

Les journaux de décryptage contiennent une grande quantité d'informations pour vous aider à Dépannage et surveillance du décryptage puis à résoudre les problèmes. Il y a 62 colonnes de différents types d'informations que vous pouvez activer dans les journaux, et vous pouvez sélectionner n'importe quel journal individuel ( , la loupe) et voir les informations dans une seule vue détaillée. Vous pouvez afficher le certificat, la suite de chiffrement et les informations sur les erreurs telles que : nom commun du sujet, nom commun de l'émetteur, nom commun de la racine, état de la racine, type et taille de la clé du certificat, date de début et de fin du certificat, numéro de série du certificat, empreinte digitale du certificat, version TLS, algorithme d'échange de clés, algorithme de cryptage, courbe négociée EC, algorithme d'authentification, SNI, type de proxy, informations sur les erreurs (chiffrement, HSM, ressource, reprise, protocole, caractéristique, certificat, version) et index d'erreurs (codes que vous pouvez consulter pour obtenir plus d'informations sur les erreurs).

## Journaux des alarmes

Une alarme est un message généré par le pare-feu indiquant que le nombre d'événements d'un certain type (par exemple, les erreurs de cryptage et de déchiffrement) a dépassé le seuil configuré pour ce type d'événement. Pour activer les alarmes et configurer des seuils d'alertes, sélectionnez **Device (Périphérique)** > **Log Settings (Paramètres des journaux)** et modifiez les Alarm Settings (Paramètres d'alertes).

Lorsqu'il génère une alarme, le pare-feu crée un Journal des alarmes et ouvre la boîte de dialogue Alarmes du système pour afficher l'alarme en question. Après avoir **Close (Fermé)** le dialogue, vous pouvez l'ouvrir à nouveau, à tout moment, en cliquant sur **Alarms (Alarmes)** ( ) au bas de l'interface Web. Pour éviter que le pare-feu ouvre automatiquement la boîte de dialogue d'une alarme en particulier, sélectionnez l'alarme dans la liste Unacknowledged Alarmes (Alarmes non acquittées), puis cliquez sur **Acknowledge (Acquitter)** l'alerte.

## Journaux d'authentification

Les journaux d'authentification affichent des informations à propos des événements d'authentification qui se produisent lorsque les utilisateurs finaux essaient d'accéder aux ressources du réseau pour lesquelles l'accès est contrôlé par les règles Politique d'authentification. Vous pouvez utiliser ces informations pour résoudre les problèmes d'accès et pour adapter votre Politique d'authentification si nécessaire. En parallèle des objets de corrélation, vous pouvez également utiliser

les Journaux d'authentification pour identifier les activités suspectes sur votre réseau, telles que les attaques par force brute.

Vous pouvez éventuellement configurer les Règles d'authentification pour journaliser les événements de temporisation. Ces délais d'expiration font référence à la période pendant laquelle un utilisateur doit s'authentifier une seule fois pour une ressource, mais qu'il peut y accéder à plusieurs reprises. Consulter les informations à propos de ces délais d'expiration vous aide à décider s'il est nécessaire de les régler, et comment le faire (pour obtenir de plus amples précisions, reportez-vous à la section Horodatages d'authentification).

***Les journaux système enregistrent les événements d'authentification liés à GlobalProtect et à l'accès administrateur à l'interface Web.***

### Journaux unifiés

Les journaux unifiés sont des entrées de journal relatives au trafic, aux menaces, au filtrage des URL, aux envois WildFire et au filtrage des données en une vue unifiée. La vue des journaux unifiés vous permet d'examiner et de filtrer les dernières entrées de divers types de journaux en un seul endroit, plutôt que d'effectuer une recherche dans chacun des types de journal séparément. Cliquez sur Effective Queries (Requêtes effective) ( ) dans la zone de filtrage pour sélectionner les types de journal d'où proviendront les entrées qui s'afficheront dans la vue des journaux unifiés.

La vue des journaux unifiés ne présente que les entrées de journaux que vous êtes autorisé à visualiser. Par exemple, un administrateur qui n'est pas autorisé à visualiser les journaux des envois WildFire ne verra pas les entrées des journaux des envois WildFire lorsqu'il visualisera les journaux unifiés. Types de rôles administrateur définit ces permissions.

***Lorsque vous Configurez la recherche à distance dans AutoFocus pour effectuer une recherche ciblée sur le pare-feu, les résultats de recherche sont affichés dans une vue de journaux unifiée.***

## Afficher des journaux

Vous pouvez visualiser les divers types de journaux du pare-feu sous la forme de tableaux. Le pare-feu stocke localement tous les fichiers des journaux et génère automatiquement des journaux de configuration et de système par défaut. Pour en savoir davantage sur les politiques de sécurité qui déclenchent la création d'entrées pour les autres types de journaux, reportez-vous à la section Types de journaux et Niveaux de gravité.

Pour configurer la transmission, par le pare-feu, de journax sous forme de messages syslog, de notifications par e-mail ou de pièges Simple Network Management Protocol (protocole simple de gestion réseau ; SNMP), procédez à l'Utilisation de services externes pour la surveillance.

**STEP 1 |** Sélectionnez un type de journal à afficher.

1. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)**.
2. Sélectionnez un type de journal dans la liste.

   *Le pare-feu affiche uniquement les journaux que êtes autorisé à visualiser. Par exemple, si votre compte administratif n'est pas autorisé à visualiser des journaux d'envois WildFire, le pare-feu n'affiche pas ce type de journaux lorsque vous accédez aux pages de journaux.* Types de rôles administrateur *définit les permissions.*

**STEP 2 |** **(**Facultatif**)**Personnalisez l'affichage des colonnes des journaux.

1. Cliquez sur la flèche qui se trouve à la droite des en-têtes des colonnes, puis sélectionnez **Columns (Colonnes)** .
2. Sélectionnez les colonnes à afficher dans la liste. Le journal se met à jour automatiquement pour correspondre à vos sélections.

**STEP 3 |** Visualisez d'autres détails sur les entrées de journaux.

- Cliquez sur la longue-vue ( ) pour consulter une entrée de journal spécifique. La Detailed Log View (Vue détaillée du journal) contient plus d'informations sur la source et la destination de la session ainsi qu'une liste de sessions associée à l'entrée du journal.
- (Journal des menaces uniquement) Cliquez sur à côté d'une entrée pour accéder aux captures de paquets locaux de la menace. Pour activer les captures de paquets locaux, reportez-vous à la section Captures de paquets.
- (Trafic, Menace, Filtrage des URL, Envois WildFire, Filtrage des données et Journaux unifiés uniquement) Affichez les données de menace AutoFocus pour une entrée du journal.

  1. Activation des données de renseignement sur les menaces AutoFocus.

     *Activez AutoFocus dans Panorama afin de visualiser des données de menace AutoFocus pour toutes les entrées de journal Panorama, y compris celles des pare-feu qui ne sont pas connectés à AutoFocus et/ou celles qui exécutent PAN-OS 7.0 ou des versions antérieures (**Panorama (Panorama) > Setup (Configuration) > Management (Gestion) > AutoFocus (AutoFocus)**).*
  2. Survolez une adresse IP, une URL, un agent utilisateur, un nom de menace (sous-type : virus et virus-WildFire uniquement), un nom de fichier ou un hachage SHA-256.
  3. Cliquez sur le menu déroulant ( ) et sélectionnez **AutoFocus (AutoFocus)**.
  4. Content Delivery Network Infrastructure (Infrastructure réseau de distribution de contenu)

Étapes suivantes…

- Journaux de filtrage.
- Journaux d'exportation.
- Configuration de quotas de stockage et de périodes d'expiration des journaux.

# Journaux de filtrage

Chaque journal possède une zone de filtrage qui vous permet d'établir un critère pour l'affichage des entrées de journaux. Le filtrage des journaux s'avère fort utilise afin se concentrer sur des événements survenus sur votre pare-feu qui possèdent des propriétés ou des attributs particuliers. Filtrez les journaux par artefacts qui sont associés aux entrées individuelles.

Par exemple, le filtrage par l'UUID de la règle facilite le l'identification de la règle spécifique que vous souhaitez trouver, même parmi de nombreuses règles portant des noms similaires. Si votre ensemble de règles est très grand et qu'il contient de nombreuses règles, l'utilisation de l'UUID de la règle en tant que filtre met en lumière la règle particulière que vous devez trouver sans avoir à parcourir de nombreuses pages de résultats.



**STEP 1 |** (Journaux unifiés uniquement) Sélectionnez les types de journaux à inclure dans l'affichage des journaux unifiés.

1. Cliquez sur Effective Queries (Requêtes effectives) ( ).
2. Sélectionnez un ou plusieurs types de journaux dans la liste (**traffic (trafic)**, **threat (menace)**, **url (url)**, **data (données)** et **wildfire (wildfire)**).
3. Cliquez sur **OK**. Le journal unifié se met à jour pour afficher uniquement les entrées qui proviennent des types de journaux que vous avez sélectionnés.

**STEP 2 |** Ajoutez un filtre dans le champ des filtres.

> ***Si la valeur de l'artefact correspond à l'opérateur (tel que **has (a)** ou **in (dans)**), insérez la valeur entre guillemets afin d'éviter une erreur de syntaxe. Par exemple, si vous filtrez par pays de destination et utilisez la Valeur IN pour préciser INDE, saisissez le filtre comme suit : `( dstloc eq "IN" )`.***

- Cliquez sur un ou plusieurs artefacts (comme le type d'application associé au trafic et à l'adresse IP du pirate) dans l'entrée du journal. Par exemple, cliquez sur la Source (Source) **10.0.0.25 (10.0.0.25)** et sur l'Application (Application) **web-browsing (navigation Web)** d'une entrée de journal afin d'afficher uniquement des entrées qui contiennent les deux artefacts (recherche AND (ET)).
- Afin de spécifier des artefacts à ajouter au champ de filtrage, cliquez sur Add Filter ( ) (Ajouter un filtre).
- Afin d'ajouter un filtre précédemment enregistré, cliquez sur Load Filter ( ) (Charger un filtre).

**STEP 3 |** Appliquez le filtre au journal.

Cliquez sur Apply Filter ( ) (Appliquer le filtre). Le journal se met à jour ; seules les entrées de journal qui correspondent au filtre actuel s'affichent.

**STEP 4 |** (Facultatif) Enregistrez les filtres qui sont utilisés fréquemment.

1. Cliquez sur Save Filter ( ) (Enregistrer le filtre).
2. Saisissez un **Name (Nom)** à donner au filtre.
3. Cliquez sur **OK**. Vous pouvez visualiser les filtres que vous avez enregistrés en cliquant sur Load Filter ( ) (Charger le filtre).

Étapes suivantes...

- Affichage des journaux.
- Exportation des journaux.

## Journaux d'exportation

Vous pouvez exporter le contenu d'un type de journal vers un rapport au format Comma-Separated Value (Valeur séparée par des virgules ; CSV). Par défaut, le rapport comprend un maximum de 2 000 lignes d'entrées de journal.

**STEP 1 |** Indiquez le nombre de lignes à afficher dans le rapport.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez la section Logging and Reporting Settings (Paramètres de journalisation et de génération de rapports).
2. Cliquez sur l'onglet **Log Export and Reporting (Exportation et génération de rapports de journaux)**.
3. Modifiez le nombre de **Max Rows in CSV Export (lignes maximales du fichier d'exportation CSV)** (maximum de 1048576 lignes).
4. Cliquez sur **OK**.

**STEP 2 |** Téléchargez le journal.

1. Cliquez sur Export to CSV ( ) (Exporter vers un fichier CSV). Une barre de progression apparaît et indique l'état d'avancement du téléchargement.
2. Une fois le téléchargement terminé, cliquez sur **Download file (Télécharger le fichier)** afin d'enregistrer une copie du journal dans un dossier local. Pour obtenir la description des en-têtes de colonne d'un journal téléchargé, reportez-vous à la section Descriptions des champs Syslog.

Étapes suivantes...

Planification des exportations de journaux vers un serveur SCP ou FTP.

## Configuration de quotas de stockage et de périodes d'expiration des journaux

Le pare-feu supprime automatiquement les journaux qui ont atteint la période d'expiration. Lorsque le pare-feu atteint le quota de stockage d'un type de journal, il supprime automatiquement les journaux antérieurs de ce type pour libérer de l'espace, même si vous ne définissez pas de période d'expiration.

*Pour supprimer manuellement des journaux, sélectionnez **Device (Périphérique) > Log Settings (Paramètres des journaux)** puis, dans la section Manage Logs (Gestion des journaux), cliquez sur les liens pour effacer des journaux par type.*

**STEP 1 |** Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Logging and Reporting Settings (paramètres de journalisation et de génération de rapports).

**STEP 2 |** Sélectionnez **Log Storage (Stockage des journaux)** et saisissez un **Quota (%) (Quota (%))** pour chaque type de journal. Lorsque vous modifiez la valeur de pourcentage, la boîte de dialogue est actualisée pour afficher la valeur absolue correspondante (colonne Quota Go/Mo).

**STEP 3 |** Entrez les **Max Days (Jours maximum)** pour chaque type de journal (plage de 1 à 2 000). Les champs sont vides par défaut, ce qui signifie que les journaux n'expirent jamais.

*Le pare-feu synchronise les périodes d'expiration sur les homologues haute disponible (HA). Étant donné que seul l'homologue HA génère des journaux, l'homologue passif n'a aucun journal à supprimer, sauf en cas de basculement et s'il commence à générer des journaux.*

**STEP 4 |** Cliquez sur **OK**, puis sur **Commit (Valider)**.

## Planification des exportations de journaux vers un serveur SCP ou FTP

Vous pouvez planifier des exportations des journaux du trafic, des menaces, de filtrage des URL, de filtrage des données, de correspondance HIP et d'envois WildFire vers un serveur Secure Copy (copie sécurisée ; SCP) ou un serveur File Transfer Protocol (protocole de transfert de fichiers ; FTP). Effectuez cette tâche pour chaque type de journal que vous souhaitez exporter :

*Vous pouvez utiliser des commandes Secure Copy (SCP) de la CLI pour exporter l'ensemble de la base de données de journaux vers un serveur SCP et l'importer sur un autre pare-feu. La base de données de journaux étant trop volumineuse pour que l'exportation ou l'importation soit pratique sur les plates-formes suivantes, celles-ci ne prennent pas en charge ces options : Pare-feu PA-7000 Series (toutes les versions de PAN-OS), appareil virtuel Panorama exécutant Panorama 6.0 ou versions ultérieures, et appareils Panorama M-Series (toutes les versions de Panorama).*

**STEP 1 |** Sélectionnez **Device (Périphérique)** > **Scheduled Log Export (Exportation planifiée des journaux)**, puis cliquez sur **Add (Ajoutez)**.

**STEP 2 |** Saisissez un **Name (Nom)** pour l'exportation programmée des journaux et **Enable (Activez)**-le.

**STEP 3 |** Sélectionnez le **Type de journal** à exporter.

**STEP 4 |** Sélectionnez la valeur quotidienne pour **Scheduled Export Start Time (Heure de début de l'exportation planifiée)**. Les options sont des incréments de 15 minutes pour un format sur 24 heures (00:00 - 23:59).

**STEP 5 |** Sélectionnez le **Protocol (Protocole)** pour exporter les journaux : **SCP** (sécurisé) ou **FTP**.

**STEP 6 |** Saisissez le **Nom d'hôte** ou l'adresse IP du serveur.

**STEP 7 |** Saisissez le numéro du **Port**. Par défaut, FTP utilise le port 21 et SCP utilise le port 22.

**STEP 8 |** Saisissez le **Path (Chemin)** ou le répertoire dans lequel enregistrer les journaux exportés.

**STEP 9 |** Saisissez le **Username (Nom d'utilisateur)** et, si nécessaire, le **Password (Mot de passe)** (et **Confirm Password (Confirmez le mot de passe)**) d'accès au serveur.

**STEP 10 |** **(**FTP uniquement**)** Sélectionnez **Enable FTP Passive Mode (Activer le mode passif FTP)** si vous souhaitez utiliser le mode passif FTP, dans lequel le pare-feu établit une connexion de données avec le serveur FTP. Par défaut, le pare-feu utilise le mode actif FTP, dans lequel c'est le serveur FTP qui établit une connexion de données avec le pare-feu. Choisissez le mode en fonction des options prises en charge par votre serveur FTP et des exigences relatives à votre réseau.

**STEP 11 |** **(**SCP uniquement**)** Cliquez sur **Test SCP server connection (Tester la connexion au serveur SCP)**. La connexion n'est pas établie jusqu'à ce que le pare-feu accepte la clé hôte pour le serveur SCP.

> *Si vous utilisez un modèle Panorama pour configurer la planification de l'exportation de journal, vous devez réaliser cette étape après avoir validé la configuration du modèle sur les pare-feu. Une fois le modèle validé, connectez-vous à chaque pare-feu, ouvrez la planification de l'exportation des journaux et cliquez sur **Test SCP server connection (Testez la connexion au serveur SCP)**.*

**STEP 12 |** Cliquez sur **OK**, puis sur **Commit (Valider)**.

# Surveiller la liste d'interdiction

Vous pouvez faire en sorte que le pare-feu place une adresse IP sur la liste d'interdiction de deux manières :

- Configurez un profil de protection contre les vulnérabilités avec une règle pour bloquer les connexions IP et appliquez le profil à une politique de sécurité que vous appliquez à une zone.
- Configurez une règle de stratégie DoS Protection avec l'action Protect et un profil Classified DoS Protection, qui spécifie un taux maximal de connexions par seconde autorisé. Lorsque les paquets entrants correspondent à la stratégie de protection DoS et dépassent le taux maximal, et si vous avez spécifié une règle de durée de bloc et une règle de politique classifiée pour inclure l'adresse IP source, le pare-feu place l'adresse IP source incriminée dans la liste de blocage.

Dans les cas décrits ci-dessus, le pare-feu bloque automatiquement ce trafic dans le matériel avant que ces paquets n'utilisent des ressources de processeur ou de tampon de paquets. Si le trafic d'attaque dépasse la capacité de blocage du matériel, le pare-feu utilise des mécanismes de blocage IP dans le logiciel pour bloquer le trafic.

Le pare-feu crée automatiquement une entrée de liste d'interdiction matérielle en fonction de votre profil de protection contre les vulnérabilités ou de la règle de politique de Protection DoS ; l'adresse source de la règle est l'adresse IP source dans la liste d'interdiction matérielle.

Les entrées de la liste d'interdiction indiquent dans la colonne Type si elles ont été bloquées par le matériel (hw) ou le logiciel (sw). Le bas de l'écran affiche :

- Le nombre **Total Blocked IPs (Total des adresses IP bloquées)** sur le nombre d'adresses IP bloquées prises en charge par le pare-feu.
- Pourcentage de la liste d'interdiction utilisée par le pare-feu.

Pour afficher les détails d'une adresse dans la liste des blocs, passez la souris sur une adresse IP source et cliquez sur le lien vers le bas. Cliquez sur le lien Who is (Qui est...) qui affiche la fonctionnalité Network Solutions Who Is Solutions réseau qui est) fournissant des informations sur l'adresse.

Pour plus d'informations sur la configuration d'un profil de protection contre les vulnérabilités, voir Personnaliser les conditions Action et Déclenchement pour une signature de force brute. Pour plus d'informations sur la liste et les profils de verrouillage de protection DoS, consultez la section Protection DoS contre l'inondation de nouvelles sessions.

# Afficher et gérer les rapports

Les fonctions de génération de rapports sur le pare-feu vous permettent de conserver une impulsion sur votre réseau, de valider vos politiques et de cibler vos efforts sur la gestion de la sécurité du réseau pour préserver la sécurité et la productivité de vos utilisateurs.



## Types de rapports

Le pare-feu inclut des rapports prédéfinis que vous pouvez utiliser tels quels. Vous pouvez également générer des rapports personnalisés répondant à vos besoins de données spécifiques et de tâches, ou combiner des rapports prédéfinis et personnalisés pour compiler les informations dont vous avez besoin. Le pare-feu fournit les types de rapports suivants :

- **Rapports prédéfinis** : vous permettent d'afficher un bref récapitulatif du trafic sur votre réseau. Une suite de rapports prédéfinis est disponible dans quatre catégories : Applications, Trafic, Menaces et Filtrage des URL. Reportez-vous à la section Affichage des rapports.
- **Rapports d'activités des utilisateurs/groupes** : vous permettent de programmer ou de créer un rapport sur demande sur l'utilisation de l'application et les activités d'URL pour un utilisateur ou un groupe d'utilisateurs spécifique. Le rapport inclut les catégories d'URL et une estimation de la durée de navigation pour chaque utilisateur. Reportez-vous à la section Génération de rapports d'activités des utilisateurs/groupes.
- **Rapports personnalisés** : créez et planifiez des rapports personnalisés qui indiquent avec précision les informations que vous souhaitez voir en appliquant un filtre sur les conditions et les colonnes à inclure. Vous pouvez également inclure des générateurs de requêtes pour une consultation plus spécifique des données du rapport. Reportez-vous à la section Génération de rapports personnalisés.
- **Rapports récapitulatifs au format PDF** : agrégez jusqu'à 18 rapports/graphiques prédéfinis ou personnalisés des catégories Menaces, Applications, Tendance, Trafic et Filtrage des URL dans un même document PDF. Reportez-vous à la section Gestion de rapports récapitulatifs au format PDF.

- **Rapports du Botnet** : vous permettent d'utiliser des mécanismes comportementaux pour identifier d'éventuels hôtes infectés par un Botnet dans le réseau. Reportez-vous à la section Génération de rapports du Botnet.
- **Groupes de rapports** : combinez des rapports prédéfinis et personnalisés dans des groupes de rapports et compilez un PDF qui est envoyé par e-mail à un ou plusieurs destinataires. Reportez-vous à la section Gestion des groupes de rapports.

Les rapports peuvent être générés sur demande, selon un schéma récurrent, et peuvent être planifiés pour être distribués par e-mail.

## Affichage des rapports

Le pare-feu propose un ensemble de plus de 40 rapports prédéfinis qu'il génère quotidiennement. Vous pouvez afficher ces rapports directement sur le pare-feu. Vous pouvez également afficher des rapports personnalisés et des rapports récapitulatifs.

200 Mo de stockage environ sont réservés à l'enregistrement des rapports sur le pare-feu. Cette limite peut être reconfigurée pour les pare-feu PA-7000 Series et PA-5200 Series uniquement. Pour tous les autres modèles de pare-feu, vous pouvez Configuration de la période d'expiration et du délai d'exécution des rapports pour autoriser le pare-feu à supprimer les rapports dépassant la période. N'oubliez pas que lorsque le pare-feu atteint sa limite de stockage, il supprime automatiquement les rapports antérieurs pour libérer de l'espace, même si vous ne définissez pas de période d'expiration. Une autre méthode pour préserver les ressources système sur le pare-feu est la Désactiver les rapports prédéfinis. Pour conserver des rapports sur le long terme, vous pouvez exporter les rapports (comme décrit ci-dessous) ou procéder à une Planification des rapports pour la distribution par e-mail.

***Contrairement aux autres rapports, vous ne pouvez pas enregistrer les rapports d'activité des utilisateurs/groupes sur le pare-feu. Une** Génération de rapports d'activités des utilisateurs/groupes **sur demande est nécessaire ou vous devez les planifier pour être distribués par e-mail.***

**STEP 1 |** (Pare-feu VM-50, VM-50 Lite et PA-200 uniquement) Activez la génération de rapports prédéfinis.

*Par défaut, les rapports prédéfinis sont désactivés sur les pare-feu VM-50, VM-50 Lite et PA-200 pour économiser les ressources.*

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez **Logging and Reporting (Journalisation et création de rapports)**.
2. Sélectionnez **Pre-Defined Reports (Rapports prédéfinis)** et activez (cochez) **Pre-Defined Reports (Rapports prédéfinis)**.
3. Cochez (activez) les rapports prédéfinis que vous voulez générer et cliquez sur **OK**
4. **Commit (validez)** vos modifications de configuration.
5. Access the firewall CLI (Accédez à la CLI du pare-feu) pour activer les rapports prédéfinis.

   Cette étape est nécessaire pour les rapports locaux prédéfinis et les rapports prédéfinis poussés à partir d'un serveur de gestion Panorama™.

```
admin> debug predefined-default enable
```

**STEP 2 |** Sélectionnez **Monitor (Surveillance)** > **Reports (Rapports)**.

Les rapports sont regroupés en sections (types) à droite de la page : **Custom Reports (Rapports personnalisés)**, **Application Reports (Rapports d'application)**, **Traffic Reports (Rapports du trafic)**, **Threat Reports (Rapports des menaces)**, **URL Filtering Reports (Rapports de filtrage des URL)** et **PDF Summary Reports (Rapports récapitulatifs au format PDF)**.

**STEP 3 |** Sélectionnez le rapport à afficher. Ensuite, la page de rapports affiche le rapport de la veille.

Pour afficher les rapports d'autres jours, sélectionnez une date dans le calendrier en bas à droite de la page, puis sélectionnez un rapport. Si vous sélectionnez un rapport dans une autre section, la sélection de date est rétablie à la date d'aujourd'hui.

**STEP 4 |** Pour afficher un rapport hors ligne, vous pouvez exporter le rapport au format PDF, CSV ou XML. Cliquez sur **Export to PDF (Exporter au format PDF)** , **Export to CSV (Exporter au format CSV)**, ou **Export to XML (Exporter au format XML)** en bas de la page, puis imprimez ou enregistrez le fichier.

## Configuration de la période d'expiration et du délai d'exécution des rapports

La période d'expiration et le délai d'exécution sont des paramètres globaux qui s'appliquent à tous les Types de rapports. À l'issue de l'exécution de nouveaux rapports, le pare-feu supprime automatiquement les rapports qui ont atteint la période d'expiration.

**STEP 1 |** Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)**, modifiez les Logging and Reporting Settings (Paramètres de journalisation et de génération de rapports), puis sélectionnez l'onglet **Log Export and Reporting (Exportation de journaux et génération de rapports)**.

**STEP 2 |** Définissez le **Report Runtime (Délai d'exécution de rapport)** sur une heure en utilisant le format d'horloge 24 heures (02:00 par défaut ; plage comprise entre 00:00 [minuit] et 23:00).

**STEP 3 |** Entrez la **Report Expiration Period (Période d'expiration de rapport)** en jours (défaut : aucune expiration ; plage comprise entre 1 et 2 000).

> *Vous ne pouvez pas modifier le stockage alloué par le pare-feu pour l'enregistrement des rapports : il est prédéfini sur 200 Mo environ. Lorsque le pare-feu atteint le stockage maximum, il supprime automatiquement les rapports antérieurs pour libérer de l'espace, même si vous ne définissez pas de **Report Expiration Period (Période d'expiration du rapport)**.*

**STEP 4 |** Cliquez sur **OK**, puis sur **Commit (Valider)**.

## Désactiver les rapports prédéfinis

Le pare-feu inclut 40 rapports prédéfinis environ qu'il génère automatiquement chaque jour. Si vous n'utilisez pas certains ou tous ceux-ci, vous pouvez désactiver des rapports sélectionnés pour préserver les ressources système sur le pare-feu.

Vérifiez qu'aucun groupe de rapports ou rapport récapitulatif au format PDF n'inclut les rapports prédéfinis que vous souhaitez désactiver. Sinon, le pare-feu génèrera un rapport récapitulatif au format PDF ou un groupe de rapports sans données.

**STEP 1 |** Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Logging and Reporting Settings (paramètres de journalisation et de génération de rapports).

**STEP 2 |** Sélectionnez l'onglet **Pre-Defined Reports (Rapports prédéfinis)**, puis décochez la case de chaque rapport que vous souhaitez désactiver. Pour désactiver tous les rapports prédéfinis, cliquez sur **Deselect All (Désélectionner tout)**.

**STEP 3 |** Cliquez sur **OK**, puis sur **Commit (Valider)**.

## Rapports personnalisés

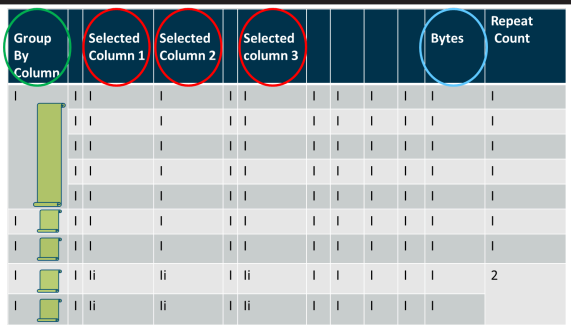
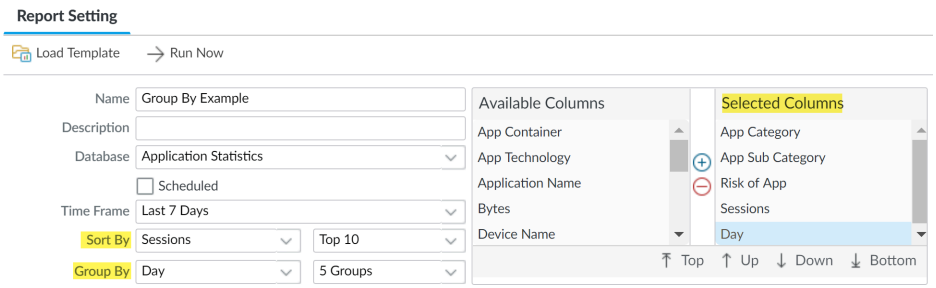
Pour pouvoir créer des rapports personnalisés utiles, vous devez prendre en compte les attributs ou éléments d'informations clés que vous souhaitez récupérer et analyser, comme les menaces, ainsi que la meilleur façon de catégoriser les informations, comme le regroupement par l'UUID de la règle, qui vous permettra de voir la règle qui s'applique à chaque type de menace. Les informations ci-dessous vous guident dans les sélections suivantes dans un rapport personnalisé :

| Sélection | Description |
|---|---|
| **Base de données** | Vous pouvez fonder le rapport sur l'un des types de base de données suivants :<br>• **Bases de données récapitulatives** : ces bases de données sont disponibles pour les journaux relatifs aux statistiques d'application, au trafic, aux menaces, au filtrage des URL et à l'inspection des tunnels. Le pare-feu agrège les journaux détaillés toutes les 15 minutes. Pour |

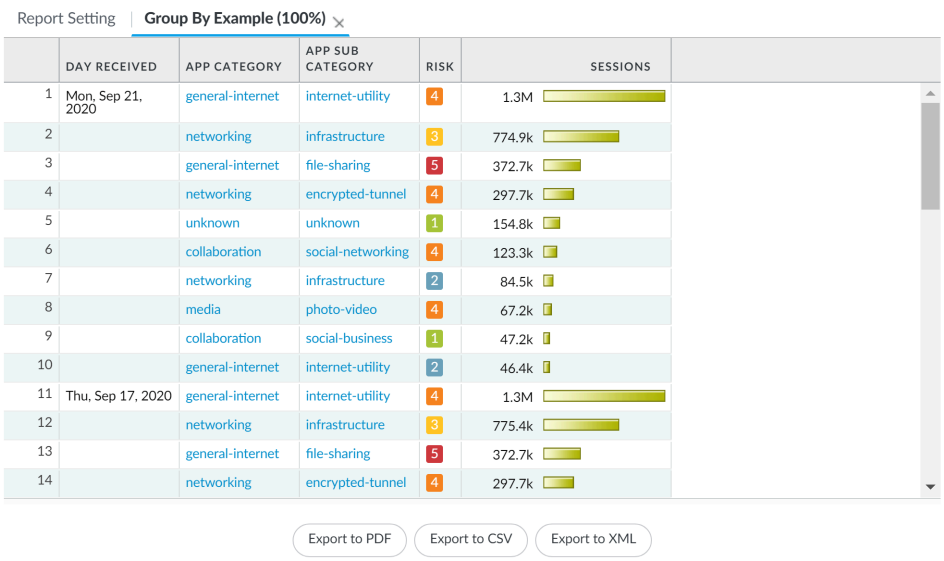
 

| Sélection | Description |
|---|---|
| | assurer un temps de réponse plus rapide lors de la génération de rapports, le pare-feu condense les données : les sessions en double sont regroupées et incrémentées dans un compteur de répétition, et certains attributs (ou colonnes) sont exclus du récapitulatif.<br>• **Journaux détaillés** : ces bases de données énumèrent les journaux et présentent une liste de tous les attributs (ou colonnes) contenus dans chaque entrée du journal.<br>  *L'exécution de rapports basés sur des journaux détaillés est plus longue et n'est recommandée qu'en cas d'absolue nécessité.* |
| **Attributs** | Les colonnes que vous souhaitez utiliser comme critères de correspondance. Les attributs correspondent aux colonnes pouvant être sélectionnées dans un rapport. Dans la liste **Available Columns (Colonnes disponibles)**, vous pouvez ajouter des critères de sélection de correspondance des données et d'agrégation des détails (**Selected Columns (Colonnes sélectionnées)**). |
| **Trier par/Regrouper par** | Les critères **Sort By (Trier par)** et **Group By (Regrouper par)** vous permettent d'organiser/de segmenter les données dans le rapport ; les attributs de tri et de regroupement disponibles varient en fonction de la source de données sélectionnée.<br>L'option Sort By (Trier par) indique l'attribut utilisé pour l'agrégation. Si vous ne sélectionnez pas d'attribut pour le tri, le rapport renvoie les N premiers résultats sans agrégation.<br>L'option Group By (Regrouper par) vous permet de sélectionner un attribut et de l'utiliser comme ancrage pour regrouper des données; toutes les données du rapport sont alors présentées sous la forme d'un ensemble de 5, 10, 25 ou 50 groupes principaux. Par exemple, vous sélectionnez Hour (Heure) comme critère Group By (Regrouper par) et vous souhaitez obtenir les 25 premiers groupes sur une période de 24 heures. Les résultats du rapport seront générés par heure sur une période de 24 heures. La première colonne du rapport indique l'heure et les autres colonnes correspondent aux colonnes du rapport sélectionné. |
| | L'exemple suivant illustre le fonctionnement des critères **Selected Columns (Colonnes sélectionnées)** et **Sort By**/**Group By (Trier par/ Regrouper par)** lors de la génération de rapports : |

| Sélection | Description |
|---|---|
| |  <br>Les colonnes encerclées de rouge (ci-dessous) correspondent aux colonnes sélectionnées, à savoir les attributs de correspondance pour la génération du rapport. Chaque entrée du journal de la source de données est analysée, et ces colonnes sont mises en correspondance. Si plusieurs sessions incluent les mêmes valeurs que les colonnes sélectionnées, les sessions sont agrégées et le nombre de répétitions (ou de sessions) est incrémenté.<br>La colonne encerclée de bleu indique l'ordre de tri choisi. Lorsque l'ordre de tri (**Sort By (Trier par)**) est spécifié, les données sont triées (et agrégées) par l'attribut sélectionné.<br>La colonne encerclée de vert indique la sélection **Group By (Regrouper par)**, qui sert d'ancrage au rapport. La colonne **Group By (Regrouper par)** est utilisée comme critère de correspondance pour filtrer les N premiers groupes. Ensuite, pour chacun des N premiers groupes, le rapport énumère les valeurs de toutes les autres colonnes sélectionnées. |
| | Par exemple, si un rapport inclut les sélections suivantes :<br>  <br>Le résultat affiché sera semblable à ci-dessous : |

| Sélection | Description |
|---|---|
| |  <br>Le rapport est ancré par **Day (Jour)** et trié par **Sessions (Sessions)**. Il répertorie les 5 jours (**5 Groups (5 groupes)**) avec le trafic maximum dans le délai **Last 7 Days (7 derniers jours)**. Les données sont énumérées selon les **Top 5 (5 premières)** sessions pour chaque jour et les colonnes sélectionnées : **App Category (Catégorie d'application)**, **App Subcategory (Sous-catégorie d'application)** et **Risk (Risque)**. |
| **Intervalle de temps** | La plage de dates sur laquelle vous souhaitez analyser les données. Vous pouvez définir une plage personnalisée ou sélectionner une période de temps allant des 15 dernières minutes aux 30 derniers jours. Les rapports peuvent être exécutés sur demande ou planifiés pour s'exécuter à une fréquence quotidienne ou hebdomadaire. |
| **Générateur de requêtes** | Le générateur de requêtes vous permet de définir des requêtes spécifiques afin d'affiner les attributs sélectionnés. Il vous permet d'afficher uniquement les éléments souhaités dans votre rapport à l'aide des opérateurs **and (et)** et **or (ou)** et d'un critère de correspondance, puis d'inclure ou d'exclure du rapport des données qui correspondent ou non à la requête. Les requêtes vous permettent de générer un ensemble d'informations plus ciblé dans un rapport. |

## Génération de rapports personnalisés

Vous pouvez configurer des rapports personnalisés que le pare-feu génère immédiatement (sur demande) ou selon la planification (chaque nuit). Pour comprendre les options qui s'offrent à vous pour créer un rapport personnalisé utile, reportez-vous à la section Rapports personnalisés.

*Une fois que le pare-feu a généré un rapport personnalisé planifié, vous risquez d'invalider les résultats antérieurs du rapport si vous modifiez sa configuration pour changer les résultats ultérieurs. Si vous devez modifier la configuration d'un rapport planifié, il est recommandé de créer un nouveau rapport.*

**STEP 1 |** Sélectionnez **Monitor (Surveillance)** > **Manage Custom Reports (Gérer les rapports personnalisés)**.

**STEP 2 |** Cliquez sur **Add (Ajouter)**, puis saisissez un **Name (Nom)** pour le rapport.

*Pour qu'un rapport se base sur un modèle prédéfini, cliquez sur **Load Template (Charger un modèle)** et sélectionnez un modèle. Vous pouvez ensuite modifier le modèle et l'enregistrer sous un rapport personnalisé.*

**STEP 3 |** Sélectionnez la **Database (Base de données)** à utiliser pour le rapport.

*Chaque fois que vous créez un rapport personnalisé, un rapport aperçu du journal est automatiquement créé. Ce rapport affiche les journaux qui ont été utilisés pour générer le rapport personnalisé. Le rapport d'aperçu du journal porte le même nom que le rapport personnalisé mais en ajoutant la phrase (Log View) au nom du rapport.*

Lors de la création d'un groupe de rapports, vous pouvez inclure le rapport d'aperçu du journal au rapport personnalisé. Pour plus d'informations, reportez-vous à la section Gestion des groupes de rapports.

**STEP 4 |** Cochez la case **Scheduled (Planifié)** pour exécuter le rapport de nuit. Le rapport peut alors être affiché dans la colonne **Reports (Rapports)** située sur le côté.

**STEP 5 |** Définissez les critères de filtrage. Sélectionnez le **Time Frame (Calendrier)**, l'ordre **Sort By (Trier par)**, **la préférence Group By (Regrouper par)**, puis sélectionnez les colonnes qui doivent s'afficher dans le rapport.

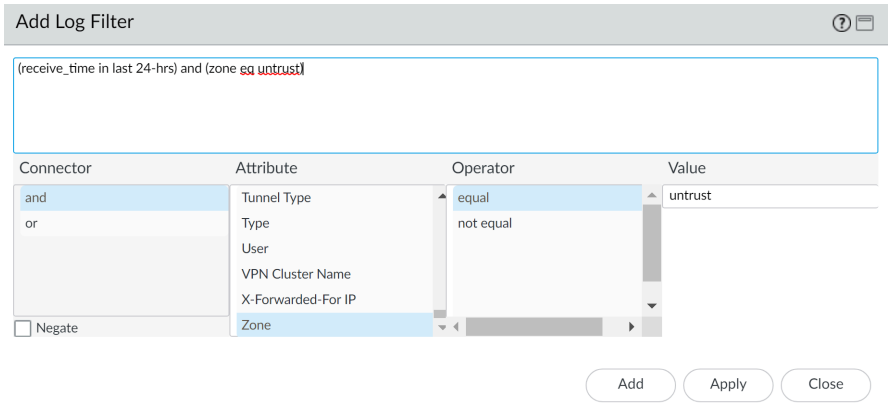
**STEP 6 |** **(**Facultatif**)** Sélectionnez les attributs **Query Builder (Générateur de requêtes)**, si vous souhaitez encore affiner les critères de sélection. Pour générer une requête de rapport, indiquez les options suivantes et cliquez sur **Add (Ajouter)**. Répétez ces différentes étapes, le cas échéant, pour formuler une requête complète.

- **Connector (Connecteur)** : sélectionnez le connecteur (et/ou) devant précéder l'expression que vous ajoutez.
- **Negate (Refuser)** : cochez cette case pour interpréter la requête en tant que refus. Si, par exemple, vous avez choisi de mettre en correspondance les entrées des 24 dernières heures et/ou provenant de la zone non approuvée, l'option de refus renvoie des entrées en dehors des 24 dernières heures et/ou ne provenant pas de la zone non approuvée.
- **Attribute (Attribut)** : sélectionnez un élément de donnée. Les options disponibles dépendent du choix de base de données.
- **Operator (Opérateur)** : sélectionnez des critères pour déterminer si un attribut s'applique (comme =). Les options disponibles dépendent du choix de base de données.

- **Value (Valeur)** : indiquez la valeur de l'attribut à faire correspondre.

Par exemple, la figure suivante (basée sur la base de données `Traffic Log`) montre une requête qui correspond, à condition que l'entrée du journal du trafic ait été reçue au cours des dernières 24 heures et qu'elle provienne d'une zone « non approuvée ».




**STEP 7 |** Pour tester les paramètres de rapport, sélectionnez **Run Now (Lancer l'exécution)**. Modifiez les paramètres si nécessaire pour modifier les informations qui figurent dans le rapport.

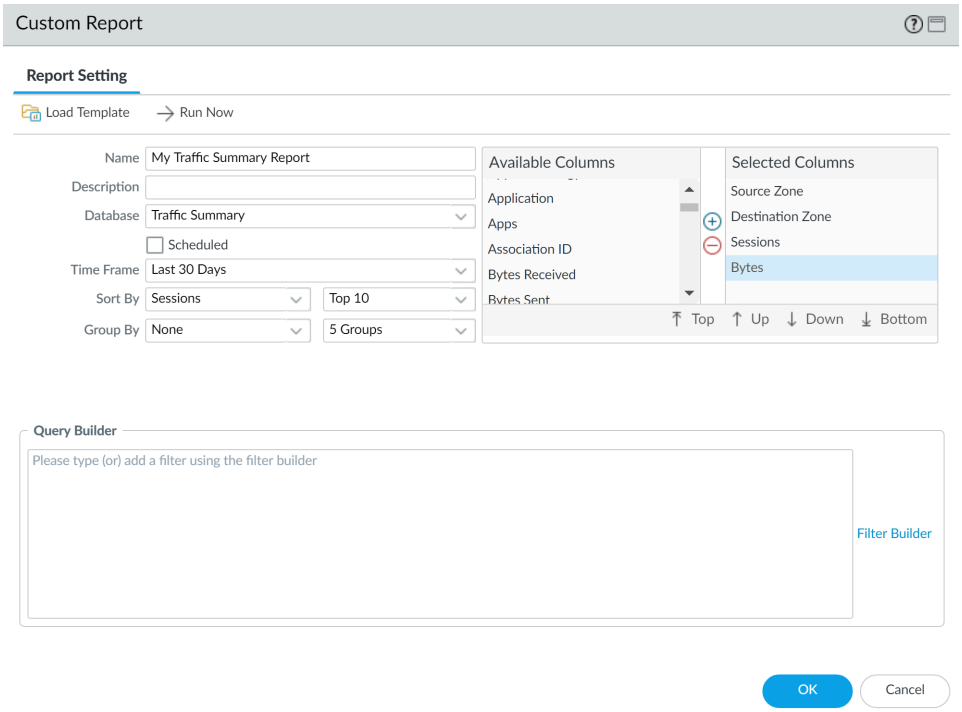
**STEP 8 |** Cliquez sur **OK** pour enregistrer le rapport personnalisé.

### Exemples de rapports personnalisés

Si vous souhaitez configurer un rapport simple dans lequel vous utilisez la base de données récapitulative du trafic des 30 derniers jours, que vous triez les données selon les 10 premières

sessions et que ces sessions sont regroupées dans 5 groupes par jour de la semaine. Vous devriez configurer le rapport personnalisé pour qu'il soit semblable à ci-dessous :




Et le résultat au format PDF du rapport sera semblable à ci-dessous :

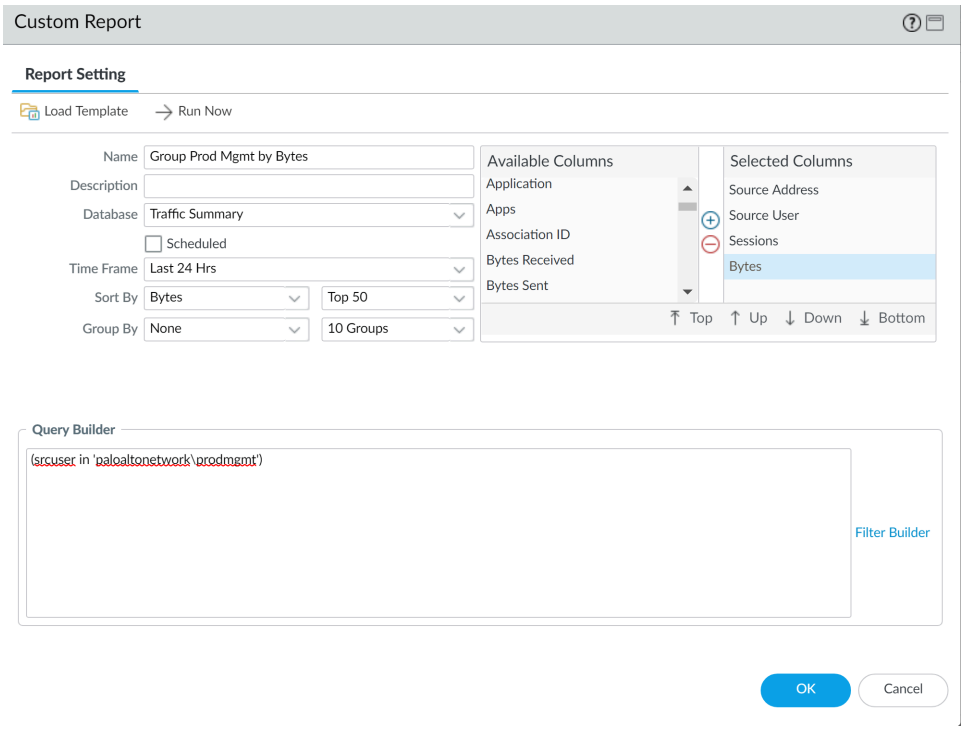
# My Traffic Summary Report

ca1demo.paloaltonetworks.com : 2016/01/25 10:34:39 - 2016/02/24 10:34:38

| Source Zone | Destination Zone | App Category | Application | Sessions | Bytes |
|---|---|---|---|---|---|
| Tap | Tap | general-internet | web-browsing | 74.54 M | 2.47 T |
| Tap | Tap | networking | dns | 52.03 M | 28.93 G |
| Tap | Tap | networking | ssl | 18.01 M | 678.13 G |
| Tap | Tap | general-internet | bittorrent | 9.80 M | 1.62 T |
| Tap | Tap | general-internet | google-base | 4.48 M | 168.99 G |
| Tap | Tap | unknown | insufficient-data | 4.45 M | 31.30 G |
| Tap | Tap | collaboration | facebook-base | 4.09 M | 99.14 G |
| Tap | Tap | networking | ntp | 4.07 M | 3.29 G |
| Tap | Tap | collaboration | blackboard | 2.84 M | 186 G |
| Tap | Tap | collaboration | smtp | 1.92 M | 172.57 G |
| Tap | Tap | networking | icmp | 1.36 M | 320.49 M |
| Tap | Tap | general-internet | gnutella | 1.17 M | 17.84 G |
| Tap | Tap | collaboration | myspace-base | 1.10 M | 35.22 G |
| Tap | Tap | general-internet | ping | 1.06 M | 86.21 M |
| Tap | Tap | general-internet | flash | 1.01 M | 168.14 G |

Supposons maintenant que vous souhaitiez utiliser le générateur de requêtes pour générer un rapport personnalisé qui représente les principaux utilisateurs des ressources réseau dans un groupe d'utilisateurs. Vous devriez configurer le rapport pour qu'il soit semblable à ci-dessous :




Le rapport indiquerait les principaux utilisateurs du groupe de gestion produit, triés par octets.

# Génération de rapports du Botnet

Le rapport du Botnet vous permet d'utiliser des mécanismes heuristiques et basés sur le comportement pour identifier d'éventuels hôtes infectés par un logiciel malveillant ou un Botnet dans votre réseau. Pour évaluer l'activité du Botnet et les hôtes infectés, le pare-feu met en corrélation les données d'activité de l'utilisateur et du réseau des journaux des menaces, de filtrage des URL et des données avec la liste d'URL de sites malveillants dans PAN-DB, les fournisseurs de domaines DNS dynamiques connus et les domaines enregistrés au cours des 30 derniers jours. Vous pouvez configurer le rapport pour identifier les hôtes ayant consulté ces sites, ainsi que les hôtes ayant communiqué avec les serveurs Internet Relay Chat (service de bavardage Internet - IRC) ou utilisé des applications inconnues. Les logiciels malveillants utilisent souvent le DNS dynamique pour éviter le blocage des IP, tandis que les serveurs IRC utilisent souvent des bots pour les fonctions automatisées.

***Le pare-feu doit disposer de licences de prévention des menaces et de filtrage des URL pour pouvoir utiliser le rapport du Botnet. L'Utilisation du moteur de corrélation automatique est possible pour surveiller les activités suspectes grâce à des indicateurs supplémentaires en plus de ceux utilisés par le rapport du Botnet. Le rapport du Botnet est toutefois le seul outil à utiliser les derniers domaines enregistrés comme indicateur.***

- Configuration d'un rapport du Botnet
- Interprétation du résultat du rapport du Botnet

## Configuration d'un rapport du Botnet

Vous pouvez planifier un rapport du Botnet ou l'exécuter sur demande. Le pare-feu génère des rapports du Botnet planifiés toutes les 24 heures car la détection basée sur le comportement requiert une corrélation du trafic sur plusieurs journaux sur cette période.

**STEP 1 |** Définissez les types de trafic révélant une éventuelle activité du Botnet.

1. Sélectionnez **Monitor (Surveillance)** > **Botnet (Botnet)** et cliquez sur le bouton **Configuration (Configuration)** à droite de la page.
2. Cliquez sur **Enable (Activer)** et définissez la valeur **Count (Nombre)** de chacun des types de trafic HTTP que le rapport doit inclure.

   Les valeurs de **Count (Nombre)** représentent le nombre minimum d'événements de chaque type de trafic qui doivent se produire pour que le rapport répertorie l'hôte associé avec une note de confiance supérieure (probabilité supérieure d'infection du Botnet). Si le nombre d'événements est inférieur au **Count (Nombre)**, le rapport indiquera une note de confiance inférieure ou (pour certains types de trafic) n'affichera pas d'entrée pour l'hôte. Par exemple, si vous définissez le **Count (Nombre)** sur trois pour **Malware URL visit (Consultation d'URL malveillantes)**, les hôtes qui consultent trois URL malveillantes connues ou plus auront des notes supérieures aux hôtes qui en consultent moins de trois. Pour plus d'informations, reportez-vous à la section Interprétation du résultat du rapport du Botnet.
3. Définissez les seuils qui déterminent si le rapport inclura les hôtes liés au trafic impliquant des applications TCP inconnues ou UDP inconnues.
4. Cochez la case **IRC (IRC)** pour inclure le trafic impliquant des serveurs IRC.
5. Cliquez sur **OK (OK)** pour enregistrer la configuration du rapport.

**STEP 2 |** Planifiez le rapport ou exécutez-le sur demande.

1. Cliquez sur **Report Setting (Paramètre du rapport)** à droite de la page.
2. Sélectionnez un intervalle pour le rapport dans la liste déroulante **Test Run Time Frame (Délai d'exécution du test)**.
3. Sélectionnez le **No. of Rows (Nombre de lignes)** à inclure dans le rapport.
4. **(**Facultatif**) Add (Ajoutez)** des requêtes au Générateur de requêtes pour filtrer les résultats du rapport par attributs tels que les adresses IP source / de destination, les utilisateurs ou les zones.

   Par exemple, si vous savez à l'avance que le trafic provenant de l'adresse IP 10.3.3.15 ne présentera aucune éventuelle activité du Botnet, ajoutez la requête **`not (addr.src in 10.0.1.35)`** pour exclure cet hôte du résultat du rapport. Pour plus d'informations, reportez-vous à la section Interprétation du résultat du rapport du Botnet.
5. Sélectionnez **Scheduled (Planifié)** pour exécuter le rapport tous les jours, ou cliquez sur **Run Now (Exécuter maintenant)** pour l'exécuter immédiatement.
6. Cliquez sur **OK**, puis sur **Commit (Valider)**.

## Interprétation du résultat du rapport du Botnet

Le rapport du Botnet affiche une ligne pour chaque hôte lié au trafic que vous avez défini comme suspect lors de la configuration du rapport. Pour chaque hôte, le rapport affiche une note de confiance de 1 à 5 afin d'indiquer la probabilité d'infection du Botnet, où 5 indique la probabilité

la plus élevée. Les notes correspondent aux niveaux de gravité des menaces suivants : 1 pour informations, 2 pour faible, 3 pour moyen, 4 pour élevé et 5 pour critique. Le pare-feu établit les notes sur les éléments suivants :

- **Type de trafic** : certains types de trafic HTTP sont plus susceptibles d'impliquer une activité du Botnet. Par exemple, le rapport attribue une confiance supérieure aux hôtes qui consultent des URL malveillantes connues qu'aux hôtes accédant à des domaines IP plutôt qu'à des URL, en supposant que vous ayez défini ces deux activités comme suspectes.
- **Nombre d'événements** : les hôtes associés à un nombre supérieur d'événements suspects se verront attribuer des notes de confiance supérieures en fonction des seuils (valeurs **Count (Nombre)**) que vous définissez lors de la Configuration d'un rapport du Botnet.
- **Téléchargements d'exécutables** : le rapport attribue une confiance supérieure aux hôtes téléchargeant des fichiers exécutables. Les fichiers exécutables représentent une partie de nombreuses infections qui, lorsqu'ils sont combinés à d'autres types de trafic suspect, vous permettent de prioriser vos recherches d'hôtes compromis.

Lors de la consultation du résultat du rapport, vous constaterez peut-être que les sources utilisées par le pare-feu pour évaluer l'activité du Botnet (par exemple, la liste des URL malveillantes dans PAN-DB) présentent des failles. Vous constaterez peut-être également que ces sources identifient du trafic que vous jugez sûr. Pour compenser ces deux cas de figure, vous pouvez ajouter des filtres de requête lors de la Configuration d'un rapport du Botnet.

## Générer le rapport sur l'utilisation d'applications SaaS

Le rapport d'utilisation de l'application SaaS au format PDF comprend deux sections. Il vous permet de facilement explorer l'activité de l'application SaaS selon le risque et l'état d'autorisation. Une application autorisée est une application pour laquelle vous autorisez officiellement l'utilisation sur votre réseau. Une application SaaS est une application qui possède la caractéristique SaaS=yes à la page des détails des applications dans **Objects (Objets)** > **Applications (Applications)**, toutes les autres applications sont considérées comme autres que SaaS. Afin d'indiquer que vous avez autorisé une application SaaS ou autre que SaaS, vous devez y apposer l'étiquette prédéfinie intitulée Sanctioned (Autorisée). Le pare-feu et Panorama considère que toute application qui n'est pas dotée d'une telle étiquette prédéfini n'est pas approuvée sur le réseau.

- La première partie du rapport présente les conclusions clés concernant les applications SaaS sur votre réseau au cours de la période de référence, notamment une comparaison des applications approuvées et des applications non approuvées, et dresse la liste des principales applications selon l'état d'approbation par rapport à l'utilisation, la conformité et les transferts de données. Pour vous aider à identifier et à explorer l'étendue de l'utilisation des applications à risque élevé, la section du rapport qui porte sur les applications comportant des caractéristiques risquées présente les applications SaaS qui possèdent les caractéristiques d'hébergement non favorables suivantes : certification obtenue, compromissions de données antérieures, support pour les restrictions basées sur IP, viabilité financières et les modalités de service. Vous pouvez également visualiser une comparaison des applications SaaS approuvées et non approuvées selon le nombre total d'applications utilisées sur votre réseau, la consommation de bande passante de ces applications, le nombre d'utilisateurs se servant de ces applications, les principaux groupes d'utilisateurs qui se servent du plus grand nombre d'applications SaaS et les principaux groupes d'utilisateurs qui transfèrent les volumes les plus importants de données via des applications SaaS approuvées et non approuvées. La première partie du rapport met également en évidence les principales sous-catégories d'applications SaaS énumérées dans l'ordre du nombre maximale

d'applications utilisées, du nombre d'utilisateurs et de la quantité de données (en octets) transférées dans chaque sous-catégorie d'applications.

- La deuxième section du rapport s'attarde aux informations de navigation détaillées sur les applications SaaS et autres que SaaS de chacune des sous-catégories d'applications figurant à la première section du rapport. Pour chaque application d'une sous-catégorie, le rapport reprend également des informations sur les utilisateurs principaux qui ont transférés des données, sur les principaux fichiers bloqués ou ayant fait l'objet d'une alerte ainsi que sur les principales menaces auxquelles chaque application doit faire face. En outre, cette section du rapport compte le nombre d'échantillons de chaque application que le pare-feu a soumis à une analyse WildFire, et le nombre d'échantillons déterminés comme étant bénins et malveillants.

Servez-vous des résultats de ce rapport pour consolider la liste des applications SaaS essentielles et autorisées et appliquer des politiques visant à contrôler les applications non autorisées et les applications risquées qui présentent des risques inutiles pour la propagation de logiciels malveillants et les fuites de données.

*Le rapport d'utilisation des applications SaaS est encore disponible sous forme de* Affichage des rapports *quotidien qui énumère les cent principales applications SaaS (c'est-à-dire les applications détenant la caractéristique des applications SaaS, SaaS=yes) qui s'exécutent sur votre réseau au cours d'une journée donnée. Ce rapport ne donne aucun aperçu des applications que vous avez désignées comme approuvées ; il donne plutôt un aperçu des applications SaaS qui sont utilisées sur votre réseau.*

**STEP 1 |** Étiquetez les applications pour lesquelles vous souhaitez approuver l'utilisation sur votre réseau en tant que Sanctioned (Autorisée).

*Si vous souhaitez générer un rapport informatif et précis, vous devez étiqueter les applications approuvées de façon uniforme sur tous les pare-feu dotés de multiples systèmes virtuels et sur des pare-feu qui appartiennent à un groupe de périphériques installés sur Panorama. Si la même application est étiquetée comme étant approuvée dans un système virtuel et comme étant non approuvée dans un autre système virtuel ou sur Panorama ou encore si une application n'est pas approuvée dans un groupe de périphériques parent mais qu'elle est approuvée dans un groupe de périphériques enfants (ou l'inverse), le rapport d'utilisation de l'application Saas indiquera que l'application est partiellement autorisée et générera des résultats non concordants.*

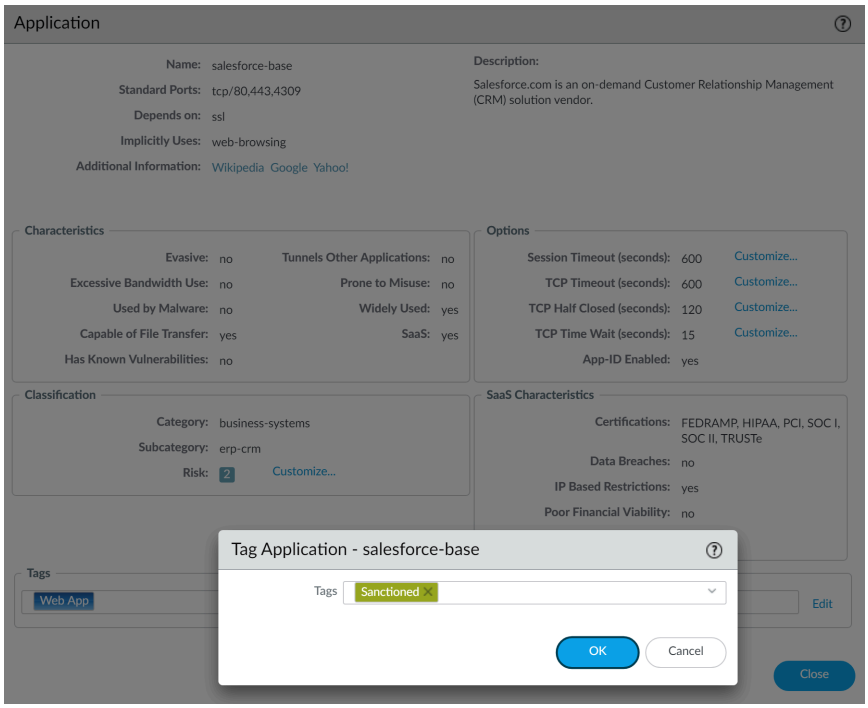
Exemple : Si Box est approuvé sur le système virtuel 1 et que Google Drive est approuvé sur le système virtuel 2, les utilisateurs de Google Drive dans le système virtuel 1 seront considérés comme des utilisateurs d'une application SaaS non approuvée et les utilisateurs de Box dans le système virtuel 2 seront considérés comme des utilisateurs d'une application SaaS non approuvée. La principale conclusion du rapport révélera la présence de deux applications SaaS uniques sur le réseau et que deux applications approuvées sont faites ainsi que deux applications non approuvées.

1. Sélectionnez **Objects (Objets)** > **Applications (Applications)**.
2. Cliquez sur le **Name (Nom)** de l'application pour modifier une application, et sélectionnez **Edit (Modifier)** dans la section Tag (Étiquette).

3. Sélectionnez **Sanctioned (Autorisé)** dans la liste déroulante **Tags (Étiquettes)**.

   Vous devez utiliser l'étiquette **Sanctioned (Autorisé)** prédéfinie (Sanctioned). Si vous utilisez une autre étiquette pour indiquer que vous avez autorisé une application, le pare-feu ne reconnaîtra pas l'étiquette et le rapport sera inexact.




4. Cliquez sur **OK (OK)** et sur **Close (Fermer)** pour quitter tous les dialogues ouverts.

**STEP 2 |** Configurez le rapport d'utilisation des applications SaaS.

1. Sélectionnez **Monitor (Surveillance)** > **PDF Reports (Rapports au format PDF)** > **SaaS Application Usage (Utilisation des applications SaaS)**.
2. Cliquez sur **Add (Ajouter)**, saisissez un **Name (Nom)**, et sélectionnez la **Time Period (Période)** du rapport (**Last 7 Days (Sept derniers jours)** par défaut).

   *Par défaut, le rapport présente des informations détaillées sur les principales sous-catégories d'applications SaaS et autres que SaaS qui peuvent alourdir le rapport en ce qui a trait au nombre de pages et à la taille du fichier. Décochez la case **Include detailed application category information in report (Inclure des renseignements détaillés sur les catégories d'application dans le rapport)** si vous voulez réduire la taille du fichier et restreindre le nombre de pages à dix.*
3. Indiquez si vous souhaitez que le rapport **Include logs from (Inclure les journaux de)** :

   *Dans PAN-OS 10.0.2 et les versions ultérieures, les rapports générés à partir des journaux du lac de données Cortex ne prennent en charge que les journaux de la **Selected Zone (Zone sélectionnée)**.*

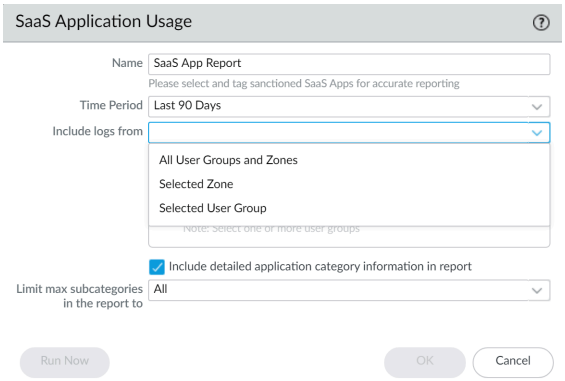
   - **All User Groups and Zones (Tous les groupes d'utilisateurs et les zones)** : le rapport contient des données sur toutes les zones de sécurité et les groupes d'utilisateurs disponibles dans les journaux.

     Si vous souhaitez inclure des groupes d'utilisateurs précis dans le rapport, sélectionnez **Include user group information in the report (Inclure des informations sur les groupes d'utilisateurs dans le rapport)** et cliquez sur le lien **manage groups (gérer les groupes)** pour sélectionner les groupes que vous souhaitez inclure. Vous devez ajouter de 1 à 25 groupes d'utilisateurs pour que le pare-feu ou Panorama puisse filtrer les journaux des groupes d'utilisateurs sélectionnés. Si vous sélectionnez les groupes à inclure, le rapport regroupera tous les groupes d'utilisateurs en un seul groupe nommé Autres.
   - **Selected Zone (Zone sélectionnée)** : le rapport filtre les données associées à la zone de sécurité indiquée et présente des données qui concernent cette zone uniquement.

     Si vous souhaitez inclure des groupes d'utilisateurs précis dans le rapport, sélectionnez **Include user group information in the report (Inclure des informations sur les groupes d'utilisateurs dans le rapport)** et cliquez sur le lien **manage groups (gérer les groupes)** pour sélectionner les groupes d'utilisateurs de cette zone que vous souhaitez inclure. Vous devez ajouter de 1 à 25 groupes d'utilisateurs pour que le pare-feu ou Panorama puisse filtrer les journaux des groupes d'utilisateurs sélectionnés au sein de la zone de sécurité. Si vous sélectionnez les groupes à inclure, le rapport regroupera tous les groupes d'utilisateurs en un seul groupe nommé Autres.
   - **Selected User Group (Groupe d'utilisateurs sélectionné)** : le rapport filtre uniquement les données concernant le groupe d'utilisateurs indiqué et présente des informations

sur l'utilisation de l'application SaaS associées au groupe d'utilisateurs sélectionné uniquement.




4. Indiquez si vous souhaitez inclure toutes les sous-catégories d'applications dans le rapport (par défaut) ou **Limit the max subcategories in the report (Limiter le nombre maximum de sous-catégories comprises dans le rapport)** aux 10, 15, 20 ou 25 catégories principales (toutes les sous-catégories par défaut).
5. Cliquez sur **Run Now (Exécuter maintenant)** pour générer le rapport sur demande pour la période correspondant aux 7 derniers jours ou aux 30 derniers jours. Vérifiez que le bloqueur de fenêtres contextuelles est désactivé dans votre navigateur, car le rapport s'ouvre dans un nouvel onglet.
6. Cliquez sur **OK** pour enregistrer vos modifications.

**STEP 3 |** Planification des rapports pour la distribution par e-mail.

Le rapport des 90 derniers jours doit être planifié aux fins de transmission par e-mail.

Sur les pare-feu PA-220R et PA-800 Series, le rapport d'utilisation d'application SaaS n'est pas transmis en tant que fichier PDF joint au e-mail. Le e-mail contient plutôt un lien que vous devez cliquer afin d'ouvrir le rapport dans un navigateur Web.

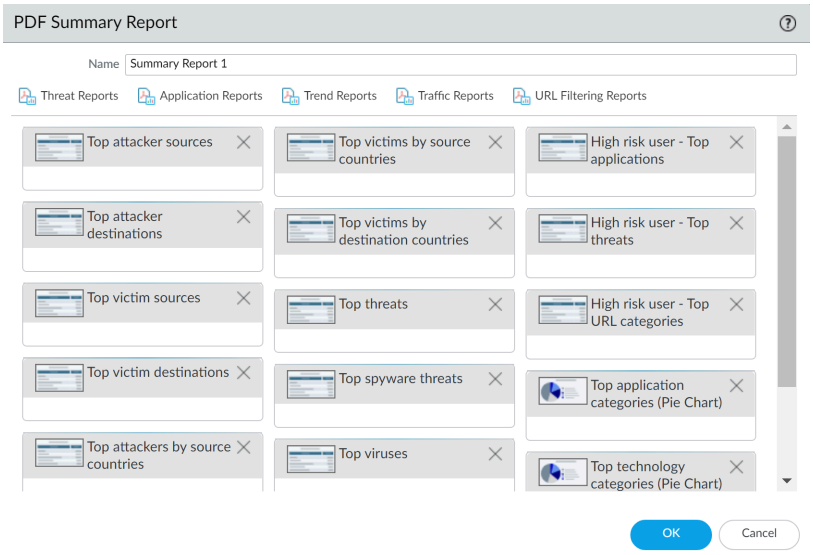
# Gestion de rapports récapitulatifs au format PDF

Les rapports récapitulatifs au format PDF contiennent des informations compilées à partir de rapports existants, en fonction des données figurant dans les 5 meilleurs de chaque catégorie (au lieu des 50 meilleurs). Ils contiennent également des diagrammes de tendance qui ne sont pas disponibles dans les autres rapports.

**STEP 1 |** Configurez un **PDF Summary Report (Rapport récapitulatif au format PDF)**.

1. Sélectionnez **Monitor (Surveillance)** > **PDF Reports (Rapports PDF)** > **Manage PDF Summary (Gérer le récapitulatif PDF)**.
2. Cliquez sur **Add (Ajouter)**, puis saisissez un **Name (Nom)** pour le rapport.
3. Utilisez la liste déroulante pour chaque groupe de rapports et sélectionnez un ou plusieurs éléments pour concevoir le rapport récapitulatif au format PDF. Vous pouvez y inclure un maximum de 18 éléments de rapport.




*La sélection des **Top Threats (menaces principales)** s'affiche en tant que `top-attacks` dans la colonne Predefined Widgets (Widgets prédéfinis) pour le rapport récapitulatif au format PDF.*

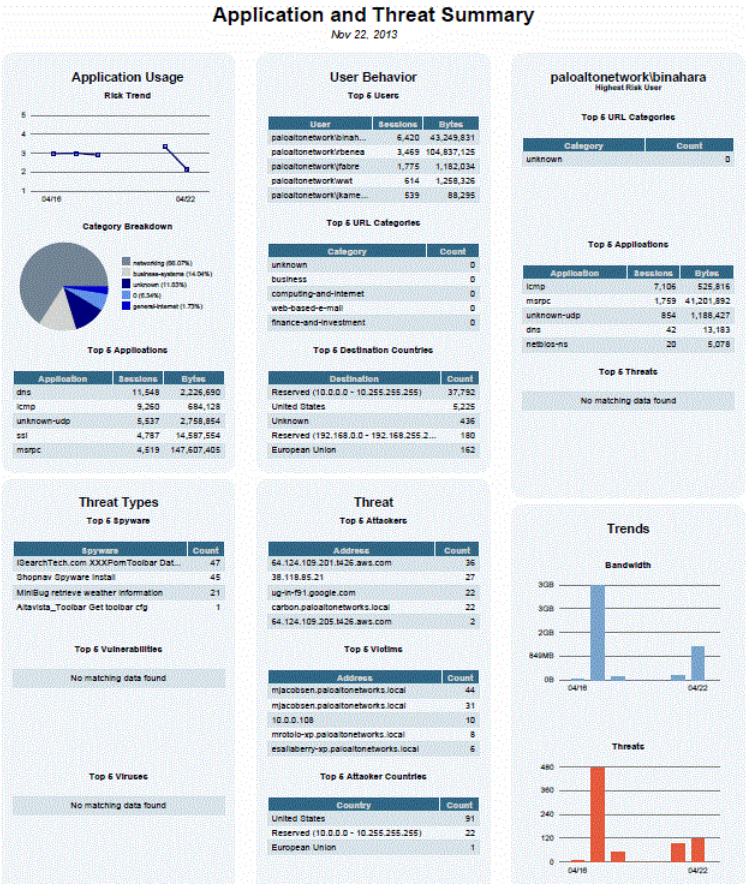
- Pour supprimer un élément du rapport, cliquez sur l'icône **x** ou effacez la sélection dans la liste déroulante du groupe de rapport approprié.
- Pour réorganiser les rapports, glissez et déposez les icônes d'éléments dans une autre zone du rapport.

4. Cliquez sur **OK** pour enregistrer le rapport.
5. **Commit (Validez)** les modifications.

**STEP 2 |** Affichez le rapport.

Pour télécharger et afficher le rapport récapitulatif au format PDF, reportez-vous à la section Affichage des rapports.




*Les sections récapitulatives suivantes se rapportent aux éléments suivants du rapport récapitulatif au format PDF :*

- ***Top 5 Attacks (Les cinq attaques principales)** : s'entend des **Top threats (Menaces principales)**.*
- ***Top 5 Threats (Les cinq menaces principales)** : s'entend de l'élément **High risk user - Top threats (Utilisateur à risque élevé - menaces principales)**.*
- *Rapport sur les menaces principales : s'entend de la liste complète des menaces sous l'élément **Top threats (Menaces principales)**.*

# Génération de rapports d'activités des utilisateurs/groupes

Les rapports d'activités des utilisateurs/groupes résument l'activité Web d'utilisateurs ou de groupes d'utilisateurs. Ces deux rapports fournissent les mêmes informations à deux exceptions près. Les informations **Browsing Summary by URL Category (Récapitulatif de navigation par catégorie**

**d'URL)** et **Browse time calculations (Calculs de durée de navigation)** sont incluses dans les rapports d'activités des utilisateurs uniquement.

Vous devez configurer le User-id sur le pare-feu pour pouvoir accéder à la liste des utilisateurs et groupes d'utilisateurs.

**STEP 1 |** Configurez les durées de navigation et le nombre de journaux pour les rapports d'activités des utilisateurs/groupes.

Requis uniquement si vous souhaitez modifier les valeurs par défaut.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)**, modifiez les Logging and Reporting Settings (Paramètres de journalisation et de génération de rapports), puis sélectionnez l'onglet **Log Export and Reporting (Exportation de journaux et génération de rapports)**.
2. Pour le **Max Rows in User Activity Report (Nombre maximum de lignes d'un rapport d'activité de l'utilisateur)**, saisissez le nombre maximum de lignes pris en charge par le rapport d'activité de l'utilisateur détaillé (plage de 1 à 1 048 576, par défaut 5 000). Cela détermine le nombre de journaux analysés par le rapport.
3. Saisissez la **Average Browse Time (Durée de navigation moyenne)** en secondes estimée de navigation d'une page Web (plage de 0 à 300, par défaut 60). Toute requête formulée une fois la durée de navigation moyenne écoulée est considérée comme une nouvelle activité de navigation. Le calcul utilise des Journalisez uniquement la page visitée par un utilisateur (consignées dans le journal de filtrage des URL) comme base et ignore les nouvelles pages Web chargées entre la première requête (heure de début) et la durée de navigation moyenne. Par exemple, si vous définissez la **Average Browse Time (Durée de navigation moyenne)** sur 2 minutes et qu'un utilisateur ouvre une page Web et la consulte pendant 5 minutes, la durée de navigation de cette page sera toujours de 2 minutes. Ceci est dû au fait que le pare-feu ne peut pas déterminer la durée de consultation d'une page donnée par un utilisateur Le calcul de la durée de navigation moyenne ignore les sites classés comme des publicités Web et des réseaux de distribution de contenu.
4. Pour le **Page Load Threshold (Seuil de chargement de page)**, saisissez la durée estimée en secondes de chargement des éléments sur la page (par défaut 20). Toute requête formulée entre le premier chargement de page et le seuil de chargement de page est considérée comme des éléments de la page. Toute requête formulée en dehors du seuil de chargement de page est censée correspondre à un clic de l'utilisateur sur un lien dans la page.
5. Cliquez sur **OK** pour enregistrer vos modifications.

**STEP 2 |** Générez les rapports d'activités de l'utilisateur/du groupe.

1. Sélectionnez **Monitor (Surveillance)** > **PDF Reports (Rapports PDF)** > **User Activity Report (Rapport d'activité de l'utilisateur)**.
2. Cliquez sur **Add (Ajouter)**, puis saisissez un **Name (Nom)** pour le rapport.
3. Créez le rapport :
   - Rapport d'activités de l'utilisateur : sélectionnez **User (Utilisateur)**, puis saisissez le **Username (Nom d'utilisateur)** ou la **IP address (Adresse IP)** (IPv4 ou IPv6) de l'utilisateur.
   - Rapport d'activités du groupe : sélectionnez **Group (Groupe)**, puis sélectionnez le **Group name (Nom du groupe)** du groupe d'utilisateurs.
4. Sélectionnez la **Time Period (Période)** du rapport.
5. (Facultatif) Cochez la case **Include Detailed Browsing (Inclure la navigation détaillée)** (décochée par défaut) pour inclure des journaux des URL détaillés dans le rapport.

   les informations relatives à la navigation détaillée peuvent inclure un grand nombre de journaux (des centaines) pour l'utilisateur ou le groupe d'utilisateurs sélectionné et peuvent rendre le rapport très volumineux.
6. Pour exécuter le rapport sur demande, cliquez sur **Run Now (Lancer l'exécution)**.
7. Pour enregistrer la configuration du rapport, cliquez sur **OK (OK)**. Vous ne pouvez pas enregistrer le résultat des rapports d'activité des utilisateurs/groupes sur le pare-feu. Pour planifier la distribution du rapport par e-mail, reportez-vous à la section Planification des rapports pour la distribution par e-mail.

## Gestion des groupes de rapports

Les groupes de rapports vous permettent de créer des ensembles de rapports que le système peut compiler et envoyer sous la forme d'un rapport unique agrégé au format PDF avec une page de titre facultative et tous les rapports constitutifs inclus.

Configurez des groupes de rapports.

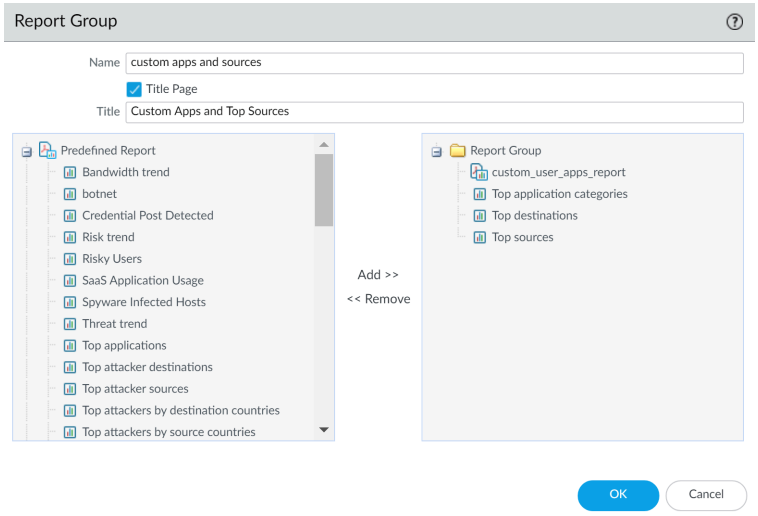
Vous devez configurer un **Report Group (groupe de rapports)** pour envoyer les rapports par courrier électronique.

1. Créez un profil de serveur de messagerie.

2. Définissez le **Groupe de rapports**. Un groupe de rapport peut compiler des rapports prédéfinis, des rapports récapitulatifs au format PDF, des rapports personnalisés et un rapport Aperçu du journal dans un même PDF.

   1. Sélectionnez **Monitor (Surveillance)** > **Reports (Rapports)**.
   2. Cliquez sur **Add (Ajouter)**, puis saisissez un **Name (Nom)** à donner au groupe de rapports.
   3. (Facultatif) Sélectionnez **Title Page (Titre de la page)** et ajoutez un **Title (Titre)** pour la sortie PDF.
   4. Sélectionnez les rapports dans la colonne de gauche et cliquez sur **Add (Ajouter)** pour déplacer chaque rapport vers le groupe de rapports situés sur la droite.




   Le rapport **Aperçu du journal** est un type de rapport qui est automatiquement généré lors de la création d'un rapport personnalisé et qui utilise le même nom que ce rapport personnalisé. Ce rapport affichera les journaux qui ont été utilisés pour générer le contenu du rapport personnalisé.

   Pour inclure des données d'aperçu du log, lors de la création d'un groupe de rapports, ajoutez votre rapport personnalisé sous la liste **Rapports personnalisés**, puis ajoutez le rapport d'aperçu du log en sélectionnant le nom du rapport correspondant dans la liste **Aperçu du log**. Le rapport inclura les données du rapport personnalisé et les données du journal qui ont été utilisées pour créer le rapport personnalisé.

   5. Cliquez sur **OK** pour enregistrer les paramètres.
   6. Pour utiliser le groupe de rapports, reportez-vous à la section Planifier des rapports pour la livraison par courrier électronique.

## Planification des rapports pour la distribution par e-mail

Les rapports peuvent être planifiés pour être distribués chaque jour ou chaque semaine le jour indiqué. L'exécution des rapports planifiés commence à 2h00 et la distribution par e-mail s'effectue une fois tous les rapports planifiés générés.

**STEP 1 |** Sélectionnez **Monitor** > **PDF Reports (Rapports PDF)** > **Email Scheduler (Planificateur d'e-mail)**, puis cliquez sur **Add (Ajoutez)**.

**STEP 2 |** Saisissez un **Name (Nom)** pour identifier le calendrier.

**STEP 3 |** Sélectionnez le **Groupe de rapports** à distribuer par courrier électronique. Pour configurer le groupe de rapports, reportez-vous à la section Gestion des Groupes de Rapport.

**STEP 4 |** Pour le **Email Profile (Profil de messagerie)**, sélectionnez un profil de serveur de messagerie à utiliser pour la distribution des rapports, ou cliquez sur le lien **Email Profile (Profil de messagerie)** pour Créer un profil de serveur de messagerie.

**STEP 5 |** Sélectionnez la fréquence à laquelle le rapport doit être généré et envoyé dans **Récurrence**.

**STEP 6 |** Le champ **Override Email Addresses (Adresses électroniques de contrôle prioritaire)** vous permet d'envoyer ce rapport exclusivement vers les destinataires spécifiés. Lorsque vous ajoutez des destinataires dans le champ, le pare-feu n'envoie pas le rapport aux destinataires configurés dans le profil de serveur de messagerie. Utilisez cette option lorsque le rapport est destiné à des utilisateurs autres que l'administration ou les destinataires définis dans le profil de serveur de messagerie.

**STEP 7 |** Cliquez sur **OK**, puis sur **Commit (Valider)**.

## Gestion de la capacité de stockage des rapports

Par défaut, les pare-feu contiennent 200 Mo d'espace de stockage dédié aux rapports qu'ils génèrent. Dans certains cas, particulièrement pour les pare-feu PA-7000 Series et PA-5200 Series, vous pouvez également accroître la capacité de stockage de rapports disponible afin de générer avec succès de nouveaux rapports.

**STEP 1 |** Accédez à la CLI du pare-feu.

**STEP 2 |** Confirmez la capacité de stockage de rapports dont dispose actuellement le pare-feu :

La sortie de la commande affiche la taille de stockage de rapports en octets. Pour cette procédure, le pare-feu dispose de la capacité de stockage de rapports par défaut, soit 200 Mo.

```
admin@ISP-CONDOR-B(active)> request report-storage-size show

209715200
```

**STEP 3 |** Vérifiez que vous disposez d'un espace de stockage suffisant sur le pare-feu pour vous permettre d'accroître la capacité de stockage des rapports :

```
admin> show system disk-space
```

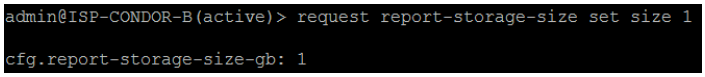
```
admin@ISP-CONDOR-B(active)> show system disk-space

Filesystem      Size  Used Avail Use% Mounted on
/dev/root        12G  8.9G  2.0G  83% /
none            7.9G   52K  7.9G   1% /dev
/dev/sda5        16G  8.5G  5.9G  59% /opt/pancfg
/dev/sda6        12G  5.8G  5.0G  54% /opt/panrepo
tmpfs           7.9G  247M  7.6G   4% /dev/shm
/dev/sda8        22G  8.7G   12G  43% /opt/panlogs
tmpfs            12M     0   12M   0% /opt/pancfg/mgmt/lcaas/ssl/private
```

**STEP 4 |** Augmentez la capacité de stockage des rapports, au besoin :

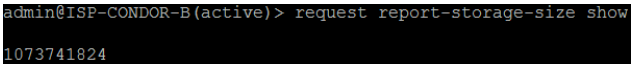
Par exemple, nous augmentons la capacité de stockage des rapports à 1 Go.

```
admin> request report-storage-size set size <0-4>
```




**STEP 5 |** Vérifiez que la capacité de stockage des rapports passe à la limite définie à l'étape précédente :

```
admin> request report-storage-size show
```



# Affichage de l'utilisation de la règle de politique

Affichez le nombre de fois où une règle de sécurité, NAT, de qualité de service (QoS), de transfert basé sur une politique, de décryptage, d'inspection des tunnels, de contrôle prioritaire sur l'application, authentification ou de protection DoS est mise en correspondance avec le trafic afin de garder les politiques de vos pare-feu à jour au fur et à mesure que votre environnement et vos besoins en matière de sécurité évoluent. Pour empêcher les pirates d'exploiter un accès sur-provisionné, par exemple lorsqu'un serveur est mis hors service ou lorsque vous n'avez plus besoin d'un accès temporaire à un service, utilisez les données relatives au nombre de fois où la règle de politique est utilisée pour déceler les règles non utilisées et les supprimer.

Les données sur l'utilisation d'une règle de politique vous donnent la possibilité de valider les ajouts de règles et les changements apportés aux règles de même que de surveiller la période au cours de laquelle une règle a été utilisée. Par exemple, lorsque vous migrez des règles basées sur les ports vers des règles basées sur les applications, vous créez une règle basée sur les applications qui a préséance sur la règle basée sur les ports et cherchez le trafic qui correspond à la règle basée sur les ports. À l'issue de la migration, les données relatives au nombre d'utilisations vous aident à déterminer s'il est sécuritaire de supprimer la règle basée sur les ports en confirmant que le trafic correspond à la règle basée sur les applications plutôt qu'à la règle basée sur les ports. Le nombre de correspondances à la règle de politique vous donne les informations qui vous permettent de déterminer si une règle est efficace pour faire respecter les droits d'accès.

Vous pouvez réinitialiser les données relatives au nombre de fois où la règle est utilisée pour valider une règle existante ou pour évaluer l'utilisation de la règle au cours d'une période de temps donnée. Les données relatives au nombre de correspondances à la règle de politique ne sont pas stockées sur le pare-feu ni sur Panorama. De ce fait, lorsque vous les supprimez en utilisant l'option de réinitialisation, ces données ne sont plus disponibles.

Après avoir filtré votre base de règles de politique, les administrateurs peuvent prendre une mesure pour supprimer, désactiver, activer et étiqueter les règles de politique directement depuis l'optimiseur de politiques. Par exemple, vous pouvez filtrer les règles non utilisées puis les étiqueter afin de les examiner et déterminer si elles peuvent être supprimées ou conservée en toute sécurité dans la base de règles. En permettant aux administrateurs de prendre une mesure directement depuis l'optimiseur de politiques, vous pouvez réduire les frais de gestion nécessaires pour aider à simplifier la gestion du cycle de vie de vos règles et vous assurer que vos pare-feux ne sont suralimentés.

***Les données relatives au nombre de correspondances à la règle de politique ne sont pas synchronisées sur l'ensemble des pare-feu dans un déploiement HA, vous devez donc vous connecter à chaque pare-feu pour consulter les données relatives au nombre de correspondance à la règle de politique applicables à chaque pare-feu ou utilisez Panorama pour afficher les informations sur les homologues HA.***

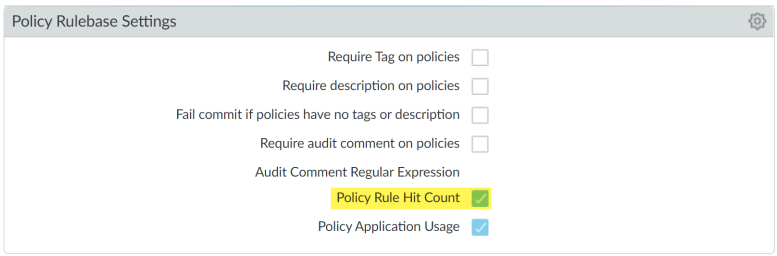
***Les données sur l'utilisation des règles de politique peuvent également s'avérer utiles lors de l'utilisation de l'optimiseur de politique afin d'établir la priorité des règles à migrer ou nettoyer en premier.***

**STEP 1 |** Lancement de l'interface Web.

**STEP 2 |** Vérifiez que le **Policy Rule Hit Count (Nombre de correspondance à la règle de politique)** est activé.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et accédez aux paramètres de la base de règles de politique.
2. Vérifiez que le **Policy Rule Hit Count (Nombre de correspondance à la règle de politique)** est activé.

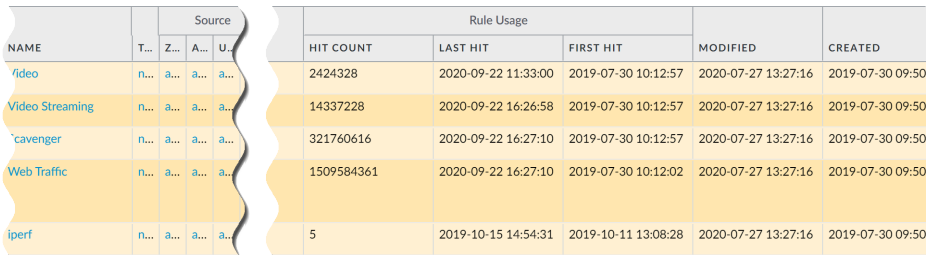



**STEP 3 |** Sélectionnez **Policies ( Politiques)**.

**STEP 4 |** Affichez l'utilisation d'une règle de politique pour chaque règle de politique :

- **Hit Count (Nombre de correspondances)** : le nombre de fois où le trafic a correspondu aux critères que vous avez définis dans la règle de politique. Ces données demeurent après le redémarrage, le redémarrage du plan de données et les mises à jours, sauf si vous réinitialisez ou renommez manuellement la règle.
- **Last Hit (Dernière correspondance)** : le plus récent horodatage correspondant à la correspondance du trafic à la règle.
- **First Hit (Première correspondance)** : la première instance où le trafic a été mis en correspondance avec cette règle.
- **Modified (Modification)** : Date et heure de la dernière modification de la règle de politique.
- **Created (Création)** : Date et heure de création de la règle de politique.

*Si la règle a été créée lorsque Panorama exécutait PAN-OS 8.1 et que le paramètre du Nombre de correspondances à la règle de politique, la date et l'heure de la première correspondance sont utilisées en tant que date et heure de création lors de la mise à niveau vers PAN-OS 9.0. Si la règle a été créée dans PAN-OS 8.1 lorsque le paramètre du Nombre de correspondances à la règle de politique est désactivé, ou si la règle a été créée lorsque Panorama exécutait PAN-OS 8.0 ou toute version antérieure, la date et l'heure de la mise à niveau de Panorama à PAN-OS 9.0 sert de date de création.*




**STEP 5 |** Dans la boîte de dialogue de l'optimiseur de politique, cliquez sur le filtre **Rule Usage (Utilisation des règles)**.

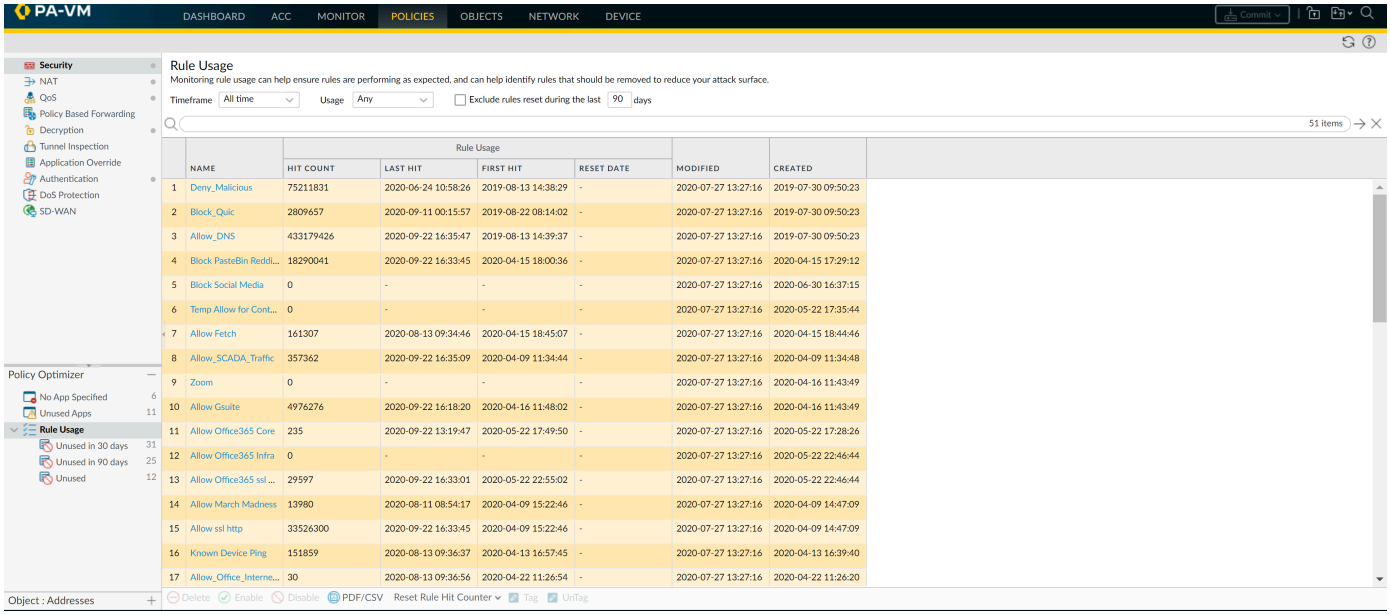
**STEP 6 |** Filtrez les règles de la base de règles sélectionnée.

*Utilisez le filtre d'utilisation des règles pour évaluer l'utilisation des règles sur une période de temps donnée. Par exemple, filtrez la base de règles sélectionnée pour connaître les règles non utilisées au cours des 30 derniers jours. Vous pouvez également évaluer l'utilisation des règles en utilisant d'autres attributs, comme les dates de création et de modification, ce qui vous permet de filtrer le bon ensemble de règles à passer en revue. Vous pouvez utiliser ces données pour vous aider à gérer le cycle de vie de vos règle et déterminer si une règle doit être supprimée afin de réduire la surface d'attaque de votre réseau.*

1. Sélectionnez la **Timeframe (Période)** à laquelle vous souhaitez appliquer le filtre, ou spécifiez une période **Custom (Personnalisée)**.
2. Sélectionnez la règle **Usage** pour laquelle vous souhaitez appliquer le filtre.
3. (Facultatif) Si vous avez réinitialisé les données d'utilisation d'une règle, cochez la case **Exclure les règles réinitialisées au cours des derniers *<nombre de jours>* jours** et déterminez quand exclure une règle en fonction du nombre de jours que vous avez indiqué

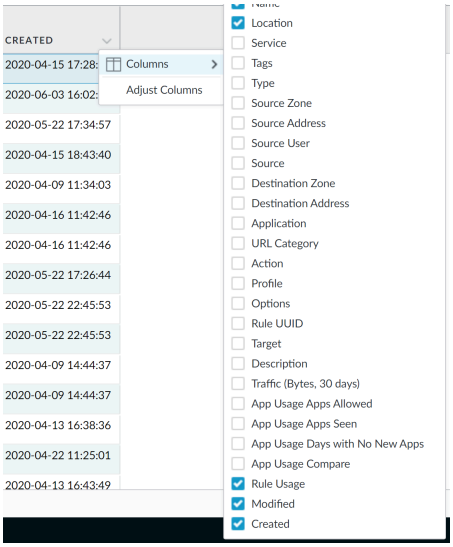
 

depuis la réinitialisation de la règle. Les règles qui ont été réinitialisées avant le nombre de jours indiqués sont incluses dans les résultats du filtrage.




4. (Optionnel) Spécifiez les filtres de recherche basé sur les données de la règle

   1. Mettez votre curseur sur l'en-tête de la colonne et **Colonnes**.
   2. Ajoutez des colonnes supplémentaires à utiliser pour l'affichage ou le filtrage.

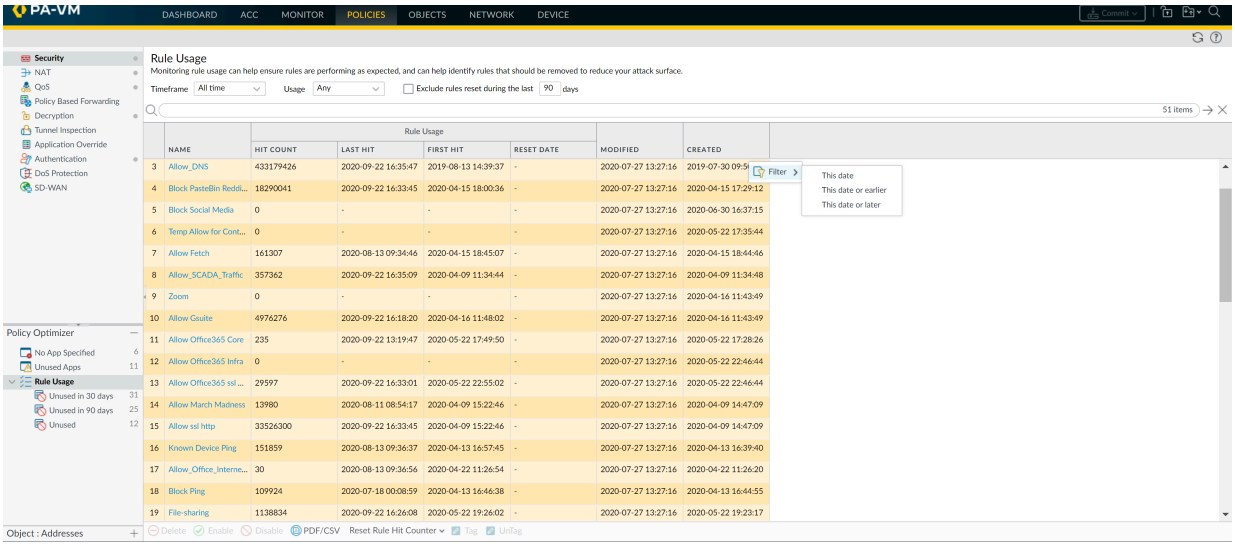



   3. Mettez votre curseur sur les données de la colonne que vous souhaitez filtrer dans **Filter**. Pour les données comprenant des dates, sélectionnez l'option de filtrage

souhaitée : **This date (Cette date)**, **This date or earlier (Cette date ou avant cette date)** ou **This date or later (Cette date ou après cette date)**.

4. **Apply Filter (Appliquez le filtre)** (→).




**STEP 7 |** Prenez une mesure pour une ou plusieurs politiques non utilisées.

1. Sélectionnez une ou plusieurs règles de politique non utilisées.
2. Effectuez l'une des actions suivantes :
   - **Delete (Supprimer)** : supprimez une ou plusieurs règles de politique sélectionnées.
   - **Enable (Activer)** : activez une ou plusieurs règles de politique sélectionnées.
   - **Disable (Désactiver)** : désactivez une ou plusieurs règles de politique sélectionnées.
   - **Tag (Etiqueter)** : appliquez une ou plusieurs étiquettes de groupe à une ou plusieurs règles de politique. L'étiquette de groupe doit déjà exister afin d'étiqueter la règle de politique.
   - **Untag (Supprimer l'étiquette)** : retirez une ou plusieurs étiquettes de groupe d'une ou plusieurs règles de politique.
3. **Commit (Validez)** vos modifications.

# Utilisation de services externes pour la surveillance

L'utilisation d'un service externe pour surveiller le pare-feu vous permet de recevoir des alertes d'événements importants, d'archiver des informations surveillées sur des systèmes disposant d'un stockage à long terme dédié, et d'intégrer des outils de surveillance de sécurité tiers. Les scénarios suivants sont les plus courants lors de l'utilisation de services externes :

- Pour obtenir immédiatement une notification sur les événements ou menaces système importants, une Surveillance des statistiques à l'aide de SNMP, un Transfert des pièges de pare-feu à un gestionnaire SNMP ou la Configuration des alertes par e-mail sont possibles.
- Pour envoyer une requête d'API basée sur HTTP directement à un service tiers qui expose une API pour automatiser un flux de travail ou une action. Vous pouvez, par exemple, transférer les journaux qui correspondent à un critère défini pour créer un ticket d'incidence sur ServiceNow au lieu de compter sur un système externe pour convertir les messages syslog ou traps SNMP en requête HTTP. Vous pouvez modifier l'URL, l'en-tête HTTP, les paramètres et la charge utile dans la requête HTTP pour déclencher une action basée sur les attributs dans un journal de pare-feu. Reportez-vous à Transférer les journaux vers une destination HTTP(s).
- Pour le stockage du journal à long terme et la surveillance centralisée des pare-feu, la Configuration de la surveillance Syslog est possible pour l'envoi des données des journaux à un serveur Syslog. Cela permet l'intégration d'outils de surveillance de sécurité tiers, tels que Splunk ou ArcSight.
- Pour obtenir des statistiques de surveillance sur le trafic IP traversant les interfaces du pare-feu, vous pouvez procéder à la Configuration des exportations NetFlow pour afficher les statistiques dans un collecteur NetFlow.

Vous pouvez procéder à la Configuration du transfert des journaux directement entre les pare-feu et les services externes ou entre les pare-feu et Panorama. Ensuite, vous configurez Panorama pour transférer les journaux aux serveurs. Reportez-vous aux Options de transfert des journaux pour les facteurs à prendre en compte lors du choix de la destination du transfert des journaux.

***Vous ne pouvez pas agréger des enregistrements NetFlow sur Panorama ; vous devez les envoyer directement des pare-feu à un collecteur NetFlow.***

# Configuration du transfert des journaux

Dans un environnement où vous utilisez plusieurs pare-feu pour contrôler et analyser le trafic sur le réseau, les pare-feu ne peuvent afficher que les journaux et les rapports du trafic qu'ils surveillent. Puisque surveillance peut devenir fastidieuse lorsque vous vous connectez à plusieurs pare-feu, vous obtiendrez une meilleure visibilité globale de l'activité sur votre réseau en transmettant les journaux des pare-feu à Panorama ou aux services externes. Si vous optez pour l'Utilisation de services externes pour la surveillance, le pare-feu convertit automatiquement les journaux au format nécessaire : messages Syslog, pièges SNMP, notifications par e-mail ou en tant que charge utile HTTP pour transmettre les détails des journaux au serveur HTTP(S). Dans les situations où certaines équipes de votre entreprise peuvent être plus efficaces en surveillant uniquement les journaux qui concernent leurs activités, vous pouvez créer des filtres de transfert en fonction d'un attribut de journal (comme le type de menace ou l'utilisateur source). Par exemple, un analyste des activités liées à la sécurité qui examine les attaques menées par des logiciels malveillants pourrait être uniquement intéressé aux journaux des menaces dont l'attribut Type serait défini sur wildfire-virus.

***Vous pouvez transférer des journaux directement entre les pare-feu et les services externes ou entre les pare-feu et Panorama. Ensuite, vous** configurez Panorama pour transférer les journaux aux serveurs**. Reportez-vous aux** Options de transfert des journaux **pour les facteurs à prendre en compte lors du choix de la destination du transfert des journaux.***

***Vous pouvez** utiliser des commandes Secure Copy (SCP) de la CLI **pour exporter l'ensemble de la base de données de journaux vers un serveur SCP et l'importer sur un autre pare-feu. La base de données de journaux étant trop volumineuse pour que l'exportation ou l'importation soit pratique sur le pare-feu PA-7000 Series, ce dernier ne prend pas en charge ces options. Vous pouvez également utiliser l'interface Web sur toutes les plates-formes pour** Afficher et gérer les rapports**, mais uniquement par type de journal et non sur l'ensemble de la base de données de journaux.***

**STEP 1 |** Configurez un profil de serveur pour chaque service externe qui recevra des informations des journaux.

***Vous pouvez utiliser des profils distincts pour envoyer à un autre serveur des ensembles de journaux différents, filtrés selon les attributs du journal. Pour augmenter la disponibilité, définissez plusieurs serveurs dans un même profil.***

Configurez un ou plusieurs des profils de serveur suivants :

- (Requis pour SMTP sur TLS) Si vous ne l'avez pas encore fait, créez un certificate profile (profil de certificat) pour le serveur de messagerie.
- 2 Pour activer le gestionnaire SNMP (serveur d'interruptions) afin d'interpréter les interruptions de pare-feu, vous devez charger des MIB prises en charge Palo Alto Networks dans le gestionnaire SNMP et, le cas échéant, les compiler. Pour plus d'informations, reportez-vous à la documentation de votre logiciel de gestion SNMP.
- Si le serveur syslog requiert l'authentification du client, vous devez aussi 5.
- Configurez un profil de serveur HTTP (consultez Transfert des journaux vers une destination HTTP/S).

**STEP 2 |** Création d'un profil de transfert des journaux.

Le profil définit les destinations des journaux du trafic, des menaces, des envois WildFire, de filtrage des URL, de filtrage des données, de tunnel et d'authentification.

1. Sélectionnez **Objects (Objets)** > **Log Forwarding (Transfert des journaux)** et **Add (Ajoutez)** un profil.
2. Saisissez un **Name (Nom)** pour identifier le profil.

   Si vous souhaitez que le pare-feu associe automatiquement le profil aux nouvelles règles et zones de sécurité, saisissez **`default`**. Si vous ne souhaitez pas disposer d'un profil par défaut, ou si vous souhaitez remplacer un profil par défaut existant, saisissez un **Name (Nom)** qui vous permettra d'identifier le profil lors de son association à des règles et zones de sécurité.

   *S'il n'existe aucun profil de transfert des journaux nommé **`default`**, la sélection du profil est définie par défaut sur **None (Aucun)** dans les nouvelles règles de sécurité (champ **Log Forwarding (Transfert des journaux)**) et les nouvelles zones de sécurité (champ **Log Setting (Paramètre de journal)**), bien que vous puissiez modifier la sélection.*
3. **Add (Ajoutez)** au moins un *profil de la liste de correspondance*.

   Les profils indiquent les filtres de requête de journal, les destinations de transfert et les actions automatiques, comme l'étiquetage. Pour chaque profil de la liste de correspondance :

   1. Saisissez un **Name (Nom)** pour identifier le profil.
   2. Sélectionnez le **Log Type (Type de journal)**.
   3. Dans la liste déroulante **Filter (Filtre)**, sélectionnez **Filter Builder (Générateur de filtre)**. Indiquez les éléments suivants, puis **Add (Ajoutez)** chaque requête :
      - **Connector (Connecteur)** logique (et/ou)
      - **Attribute (Attribut)** du journal
      - L'**Operator (Opérateur)** pour définir la logique d'inclusion ou d'exclusion
      - La **Value (Valeur)** d'attribut à laquelle doit correspondre la requête
   4. Sélectionnez **Panorama** si vous souhaitez transmettre des journaux aux collecteurs de journaux ou au serveur de gestion Panorama.
   5. **Add (Ajoutez)** au moins un profil de serveur pour chaque type de service externe que vous utilisez pour la surveillance (SNMP, e-mail, Syslog et HTTP).
4. (Facultatif, GlobalProtect uniquement) Si vous utilisez un profil de transfert des journaux avec une politique de sécurité pour mettre automatiquement en quarantaine un périphérique à l'aide de GlobalProtect, sélectionnez **Quarantine (Quarantaine)** dans la zone **Built-in Actions (Actions intégrées)**.
5. Cliquez sur **OK** pour enregistrer le profil de transfert des journaux.

**STEP 3 |** Affectation du profil de transfert des journaux aux règles de politique et aux zones réseau.

Les règles de sécurité, d'authentification et de protection DoS prennent en charge le transfert des journaux. Dans cet exemple, vous associez le profil à une règle de sécurité.

Effectuez les étapes suivantes pour chaque règle qui déclenchera le transfert des journaux :

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis modifiez la règle.
2. Sélectionnez **Actions** et sélectionnez le profil de **Log Forward (Transfert de journaux)** que vous avez créé.
3. Définissez le **Profile Type (Type de profil)** sur **Profiles (Profils)** ou sur **Group (Groupe)**, puis sélectionnez les profils de sécurité ou le **Group Profile (Profil de groupe)** requis pour déclencher la génération et le transfert des journaux suivants :
   - Journaux des menaces : le trafic doit correspondre à un profil de sécurité associé à une règle de sécurité.
   - Journaux d'envois WildFire : le trafic doit correspondre à un profil d'analyse WildFire associé à la règle.
4. Pour les journaux de trafic, sélectionnez **Log At Session Start (Connexion en début de session)** et/ou **Log At Session End (Connexion en fin de session)**.
5. Cliquez sur **OK** pour enregistrer la règle.

**STEP 4 |** Configurez les destinations pour System (Système), Configuration, Correlation (Corrélation), GlobalProtect, HIP Match (Correspondance HIP), et User-ID logs (Journaux d'ID d'utilisateur).

*Panorama génère des journaux de corrélation en fonction des journaux du pare-feu qu'il reçoit, plutôt que d'agréger les journaux de corrélation des pare-feu.*

1. Sélectionnez **Device (Périphérique)** > **Log Settings (Paramètres des journaux)**.
2. Reportez-vous à l'étape Ajout d'un ou de plusieurs profils de la liste de correspondance pour chaque type de fichier que le pare-feu transférera.

**STEP 5 |** (Pare-feu PA-7000 Series uniquement) Configurez une interface de carte de journal pour le transfert des journaux.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)**, puis cliquez sur **Add Interface (Ajouter une interface)**.
2. Sélectionnez le **Slot (Logement)** et le **Interface Name (Nom de l'interface)**.
3. Définissez le **Interface Type (Type d'interface)** sur **Log Card (Carte de journal)**.
4. Saisissez la **IP Address (Adresse IP)**, la **Default Gateway (Passerelle par défaut)** et, (pour IPv4 uniquement), le **Netmask (Masque réseau)**.
5. Sélectionnez **Advanced (Avancé)** et spécifiez la **Link Speed (Vitesse de liaison)**, le **Link Duplex (Duplex de la liaison)** et le **Link State (État de la liaison)**.

   *La valeur par défaut de ces champs est **auto**, qui indique que le pare-feu détermine automatiquement les valeurs selon la connexion. Toutefois, la **Link Speed (Vitesse de liaison)** minimale recommandée pour toutes les connexions est **1000 (1 000)** (Mbits/s).*
6. Cliquez sur **OK** pour enregistrer vos modifications.

**STEP 6 |** Validez et vérifiez vos modifications.

1. **Commit (Validez)** vos modifications.
2. Vérifiez que les destinations des journaux que vous avez configurées reçoivent les journaux du pare-feu :
   - Panorama : si le pare-feu transfère les journaux à un appareil Panorama virtuel en mode Panorama ou à un appareil M-Series, vous devez configurer un groupe de collecteurs pour que Panorama puisse recevoir les journaux. Vous pouvez ensuite vérifier le transfert des journaux.
   - Serveur de messagerie : vérifiez que les destinataires spécifiés reçoivent les journaux sous forme de notifications par e-mail.
   - Serveur Syslog : reportez-vous à la documentation de votre serveur Syslog pour vérifier qu'il reçoit les journaux sous forme de messages Syslog.
   - Gestionnaire SNMP :Utilisation d'un gestionnaire SNMP pour parcourir les MIB et les objets pour vérifier qu'il reçoit les journaux comme interruptions SNMP.
   - Serveur HTTP : Transfert des journaux vers une destination HTTP/S.

# Configuration des alertes par e-mail

Vous pouvez configurer des alertes par e-mail pour les journaux système, de configuration, de correspondance HIP, de corrélation, de menaces, d'envois WildFire et du trafic. Vous pouvez utiliser différents profils pour envoyer des notifications par e-mail pour chaque type de journal à un serveur distinct. Pour augmenter la disponibilité, définissez plusieurs serveurs (jusqu'à quatre) dans un même profil.

*Comme meilleure pratique, configurez la Transport Layer Security (TLS) pour exiger que le pare-feu s'authentifie auprès du serveur de messagerie avant que le pare-feu ne relaie l'e-mail vers le serveur. Cela permet de prévenir les activités malveillantes, telles que le relais Simple Mail Transfer Protocol (protocole simple de transfert de courrier - SMTP), qui peut être utilisé pour envoyer du spam ou des logiciels malveillants, et l'usurpation d'e-mail, qui peut être utilisée pour des attaques de phishing.*

**STEP 1 |** (Requis pour SMTP sur TLS) Si vous ne l'avez pas encore fait, créez un certificate profile (profil de certificat) pour le serveur de messagerie.

**STEP 2 |** Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveur)** > **Email (Messagerie)**.

**STEP 3 |** **Add (Ajoutez)** un profil du serveur de messagerie et saisissez un **Name (Nom)**.

**STEP 4 |** Dans la fenêtre en lecture seule qui apparaît, **Add (Ajoutez)** le serveur de messagerie et saisissez un **Name (Nom).**

**STEP 5 |** Si le pare-feu comporte plusieurs systèmes virtuels (vsys), sélectionnez le **Location(Emplacement)** (vsys ou **Shared (Partagé)**) où ce profil est disponible.

**STEP 6 |** (Facultatif) Saisissez un **Email Display Name (Nom complet de messagerie)** pour spécifier le nom à afficher dans le champ « De » de l'e-mail.

**STEP 7 |** Saisissez l'adresse e-mail **From (De)** avec laquelle le pare-feu envoie les e-mails.

**STEP 8 |** Saisissez l'adresse e-mail **To (À)** à laquelle le pare-feu envoie les e-mails.

**STEP 9 |** (Facultatif) Si vous souhaitez envoyer les e-mails à un deuxième compte, saisissez l'adresse du **Additional Recipient (Destinataire supplémentaire)**. Vous ne pouvez ajouter qu'un seul destinataire supplémentaire. Pour ajouter plusieurs destinataires, saisissez l'adresse e-mail d'une liste de distribution.

**STEP 10 |** Saisissez l'adresse IP ou le nom d'hôte de la **Email Gateway (Passerelle de messagerie)** à utiliser pour l'envoi des e-mails.

**STEP 11 |** Sélectionnez le **Type** de protocole à utiliser pour le serveur de messagerie :

- **Unauthenticated SMTP (SMTP sans authentification)** : utilisez SMTP pour vous connecter au serveur de messagerie sans authentification. Le **Port** par défaut est 25, mais vous pouvez spécifiez un port différent en option. Ce protocole n'offre pas la même sécurité que SMTP sur TLS, mais si vous sélectionnez ce protocole, sautez l'étape suivante.

- **SMTP sur TLS** : (Recommandé) Utilisez TLS pour exiger une authentification afin de vous connecter au serveur de messagerie. Passez à l'étape suivante pour configurer l'authentification TLS.

**STEP 12 |** (SMTP sur TLS uniquement) : Configurez le pare-feu pour utiliser l'authentification TLS afin de vous connecter au serveur de messagerie.

1. (Facultatif) Spécifiez le **Port** à utiliser pour la connexion au serveur de messagerie (par défaut : 587).
2. **Version TLS** : spécifiez la version TLS (**1.1** ou **1.2**).

   *Palo Alto Networks recommande vivement d'utiliser la dernière version de TLS.*
3. Sélectionnez la **Authentication Method (Méthode d'authentification)** pour le pare-feu et le serveur de messagerie :
   - **Auto** : autorisez le pare-feu et le serveur de messagerie à déterminer la méthode d'authentification.
   - **Login (Connexion)** : Utilisez l'encodage Base64 pour le nom d'utilisateur et le mot de passe et transmettez-les séparément.
   - **Plain (Clair)** : Utilisez l'encodage Base64 pour le nom d'utilisateur et le mot de passe et transmettez-les ensemble.
4. Sélectionnez un **Certificate Profile (Profil de certificat)** pour l'authentification avec le serveur de messagerie.
5. Saisissez le **Username (Nom d'utilisateur)** et le **Password (Mot de passe)** du compte qui envoie les e-mails, puis **Confirm Password (Confirmez le mot de passe)**.
6. (Facultatif) Pour confirmer que le pare-feu peut s'authentifier avec succès auprès du serveur de messagerie, vous pouvez **Test Connection (Tester la connexion)**.

**STEP 13 |** Cliquez sur **OK (OK)** pour enregistrer le profil de serveur de messagerie.

**STEP 14 |** (Facultatif) Sélectionnez l'onglet **Custom Log Format (Format de journal personnalisé)** et personnalisez le format des e-mails. Pour plus d'informations sur la création de formats personnalisés pour les divers types de journaux, reportez-vous au Guide de configuration des formats d'événements courants.

**STEP 15 |** Configurez des alertes par e-mail pour les journaux du trafic, des menaces et d'envois WildFire.

1. Consultez Création d'un profil de transfert des journaux.
   1. Sélectionnez **Objects (Objets)** > **Log Forwarding (Transfert des journaux)**, cliquez sur **Add (Ajouter)**, et saisissez un **Name (Nom)** pour identifier le profil.
   2. Pour chaque type de journal et chaque niveau de gravité ou verdict WildFire, sélectionnez le profil de serveur de messagerie, puis cliquez sur **OK (OK)**.
2. Consultez Affectation du profil de transfert des journaux aux règles de politique et aux zones réseau.

**STEP 16 |** Configurez des alertes par e-mail pour les journaux système, de configuration, de correspondance HIP et de corrélation.

1. Sélectionnez **Device (Périphérique)** > **Log Settings (Paramètres des journaux)**.
2. Pour les journaux système et de corrélation, cliquez sur chaque niveau de gravité, sélectionnez le profil de serveur **Email (Messagerie)**, puis cliquez sur **OK (OK)**.
3. Pour les journaux de configuration et de correspondance HIP, modifiez la section, sélectionnez le profil de serveur **Email (Messagerie)**, puis cliquez sur **OK (OK)**.
4. Cliquez sur **Commit (Valider)**.

# Utilisation de Syslog pour la surveillance

Syslog est un mécanisme de transfert de journaux standard qui permet l'agrégation des données des journaux à partir de différents périphériques réseau, tels que routeurs, pare-feu, imprimantes, de différents fournisseurs, dans un référentiel central, pour l'archivage, l'analyse et la création de rapports. Les pare-feu Palo Alto Networks peuvent transférer tous les types de journaux qu'ils génèrent à un serveur Syslog externe. Vous pouvez utiliser TCP ou TLS (TLSv1.2 uniquement) pour un transfert fiable et sécurisé des journaux, ou UDP pour un transfert non sécurisé.

- Configuration de la surveillance Syslog
- Descriptions des champs Syslog

## Configuration de la surveillance Syslog

Pour l'utilisation de Syslog pour la surveillance d'un pare-feu Palo Alto Networks, créez un profil de serveur Syslog et associez-le aux paramètres des journaux de périphériques pour chaque type de journal. (Facultatif) Vous pouvez configurer le format d'en-tête utilisé dans les messages Syslog et activer l'authentification client pour Syslog sur TLSv1.2.

***Pour la** CEF-formated syslog events collection (collecte d'événements syslog au format CEF), **vous devez modifier la configuration syslog par défaut. La configuration de surveillance syslog par défaut n'est pas prise en charge pour la collecte d'événements syslog CEF.***

**STEP 1 |** Configurez un profil de serveur Syslog.

*Vous pouvez utiliser différents profils pour envoyer des messages Syslog pour chaque type de journal à un serveur distinct. Pour augmenter la disponibilité, définissez plusieurs serveurs (jusqu'à quatre) dans un même profil.*

1. Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveur)** > **Syslog (Syslog)**.
2. Cliquez sur **Add (Ajouter)** et entrez un **Name (Nom)** pour le profil.
3. Si le pare-feu comporte plusieurs systèmes virtuels (vsys), sélectionnez le **Location(Emplacement)** (vsys ou **Shared (Partagé)**) où ce profil est disponible.
4. Pour chaque serveur Syslog, cliquez sur **Add (Ajouter)** et saisissez les informations nécessaires au pare-feu pour s'y connecter :
   - **Name (Nom)** : nom unique du profil de serveur.
   - **Syslog Server (Serveur Syslog)** : adresse IP ou Fully Qualified Domaine Name (om de domaine complet ; FQDN) du serveur syslog.

     *Si vous configurez un FQDN et utilisez le transport **UDP** et que le pare-feu ne peut résoudre le FQDN, le pare-feu utilise la résolution d'adresse IP existante pour le FQDN en tant qu'adresses du **Syslog Server (Serveur Syslog)**.*
   - **Transport (Transport)** : sélectionnez **TCP**, **UDP** ou **SSL** (TLS) comme protocole de communication avec le serveur Syslog. Pour **SSL**, le pare-feu ne prend en charge que TLSv1.2.
   - **Port (Port)** : numéro de port sur lequel envoyer des messages Syslog (UDP sur le port 514 par défaut) ; vous devez utiliser le même numéro de port sur le pare-feu et le serveur Syslog.
   - **Format (Format)** : sélectionnez le format de message Syslog à utiliser : **BSD (BSD)** (par défaut) ou **IETF (IETF)**. Généralement, le format **BSD (BSD)** est sur UDP et le format **IETF (IETF)** est sur TCP ou SSL/TLS.
   - **Facility (Site)** : sélectionnez une valeur standard Syslog (par défaut **LOG_USER (LOG_USER)**) pour calculer le champ PRI (priorité) dans l'implémentation de votre serveur Syslog. Sélectionnez la valeur correspondant à l'utilisation du champ PRI pour gérer vos messages Syslog.
5. (**Facultatif**) Pour personnaliser le format des messages Syslog envoyés par le pare-feu, sélectionnez l'onglet **Custom Log Format (Format de journal personnalisé)**. Pour plus d'informations sur la création de formats personnalisés pour les divers types de journaux, reportez-vous au Guide de configuration des formats d'événements courants.
6. Cliquez sur **OK** pour enregistrer le profil de serveur.

**STEP 2 |** Configurez le transfert Syslog pour les journaux du trafic, des menaces et d'envois WildFire.

1. Configurez le pare-feu pour qu'il transmette les journaux. Pour obtenir de plus amples renseignements, reportez-vous à l'étape Création d'un profil de transfert des journaux.

   1. Sélectionnez **Objects (Objets)** > **Log Forwarding (Transfert des journaux)**, cliquez sur **Add (Ajouter)**, et saisissez un **Name (Nom)** pour identifier le profil.
   2. Pour chaque type de journal et chaque niveau de gravité ou verdict WildFire, sélectionnez le profil de serveur **Syslog (Syslog)**, puis cliquez sur **OK (OK)**.

2. Affectez le profil de transfert des journaux à une politique de sécurité pour déclencher la génération et le transfert des journaux. Pour obtenir de plus amples renseignements, reportez-vous à l'étape Affectation du profil de transfert des journaux aux règles de politique et aux zones réseau.

   1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis choisissez une règle de politique.
   2. Sélectionnez l'onglet **Actions** et sélectionnez le profil de **Log Forward (Transfert de journaux)** que vous avez créé.
   3. Dans le menu déroulant **Profile Type (Type de profil)**, sélectionnez **Profiles (Profils)** ou **Group (Groupe)**, puis sélectionnez les profils de sécurité ou les **Group Profiles (Profils de groupe)** requis pour déclencher la génération et le transfert des journaux.
   4. Pour les journaux de trafic, cochez au moins l'une des cases **Log at Session Start (Journaliser au début de la session)** et **Log At Session End (Journaliser à la fin de la session)**, puis cliquez sur **OK**.

   Pour obtenir des renseignements détaillés sur la configuration d'un profil de transfert des journaux et l'affectation du profil à une règle de politique, reportez-vous à la section Configuration du transfert des journaux.

**STEP 3 |** Configurez le transfert Syslog pour les journaux système, de configuration, de correspondance HIP et de corrélation.

1. Sélectionnez **Device (Périphérique)** > **Log Settings (Paramètres des journaux)**.
2. Pour les journaux système et de corrélation, cliquez sur chaque niveau de gravité, sélectionnez le profil de serveur **Syslog (Syslog)**, puis cliquez sur **OK (OK)**.
3. Pour les journaux de configuration, de correspondance HIP et de corrélation, modifiez la section, sélectionnez le profil de serveur **Syslog (Syslog)**, puis cliquez sur **OK (OK)**.

**STEP 4 |** (Facultatif) Configurez le format d'en-tête des messages Syslog.

Les données des journaux incluent l'identifiant unique du pare-feu qui a généré le journal. Le choix du format d'en-tête offre plus de flexibilité en matière de filtrage et de génération de

rapports sur les données de journal pour certains serveurs Security Information and Event Management (gestion des informations et des événements de sécurité - SIEM).

Il s'agit d'un paramètre général qui s'applique à tous les profils de serveur Syslog configurés sur le pare-feu.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Logging and Reporting Settings (paramètres de journalisation et de génération de rapports).
2. Sélectionnez l'onglet **Log Export and Reporting (Exportation de journaux et génération de rapports)** et sélectionnez le format de nom d'hôte dans les messages Syslog :
   - **FQDN (FQDN)** (par défaut) : concatène le nom d'hôte et le nom de domaine définis sur le pare-feu expéditeur.
   - **Hostname (Nom d'hôte)** : utilise le nom d'hôte défini sur le pare-feu expéditeur.
   - **ipv4-address (Adresse IPv4)** : utilise l'adresse IPv4 de l'interface du pare-feu utilisée pour envoyer les journaux. Par défaut, il s'agit de l'interface MGT.
   - **ipv6-address (Adresse IPv6)** : utilise l'adresse IPv6 de l'interface du pare-feu utilisée pour envoyer les journaux. Par défaut, il s'agit de l'interface MGT.
   - **None (Aucun)** : le champ du nom d'hôte n'est pas renseigné sur le pare-feu. Aucun identifiant n'est défini pour le pare-feu qui a envoyé les journaux.
3. Cliquez sur **OK** pour enregistrer vos modifications.

**STEP 5 |** Créez un certificat pour sécuriser la communication Syslog sur TLSv1.2.

Requis uniquement si le serveur Syslog utilise l'authentification du client. Le serveur Syslog utilise ce certificat pour vérifier que le pare-feu est autorisé à communiquer avec le serveur Syslog.

Vérifiez que les conditions suivantes sont remplies :

- La clé privée doit être disponible sur le pare-feu expéditeur ; les clés ne peuvent pas se trouver sur un Hardware Security Module (module de sécurité matériel ; HSM).
- L'objet et l'émetteur du certificat ne doivent pas être identiques.
- Le serveur Syslog et le pare-feu expéditeur doivent disposer de certificats signés par la même Certificate Authority (autorité de certification ; CA) de confiance. Vous pouvez également générer un certificat auto-signé sur le pare-feu, l'exporter à partir du pare-feu et l'importer sur le serveur Syslog.
- La connexion à un serveur Syslog sur TLS est validée au moyen du protocole Online Certificate Status Protocol (protocole de vérification en ligne de certificat ; OCSP) ou au moyen des Certificate Revocation Lists (listes de révocation de certificats - CRL) tant que chaque certificat de la chaîne de confiance indique l'une de ces extensions, ou les deux. Cependant, vous ne pouvez pas contourner les échecs OCSP ou CRL. Vous devez donc vous

assurer que la chaîne de certificat est valide et que vous pouvez vérifier chaque certificat à l'aide d'OCSP ou de CRL.

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, puis cliquez sur **Generate (Générer)**.
2. Donnez un **Name (Nom)** au certificat.
3. Dans le champ **Common Name (Nom commun)**, saisissez l'adresse IP du pare-feu qui envoie les journaux au serveur Syslog.
4. Dans **Signed by (Signé par)**, sélectionnez la CA de confiance ou la CA auto-signée approuvée par le serveur Syslog et le pare-feu expéditeur.

   Le certificat ne peut pas être une **Certificate Authority (Autorité de certification)** ni une **External Authority (Autorité externe)** (Certificate Signing Request (demande de signature de certificat ; CSR]).
5. Cliquez sur **Generate (Générer)**. Le pare-feu génère la paire certificat/clé.
6. Cliquez sur le nom du certificat pour le modifier, cochez la case **Certificate for Secure Syslog (Certificat pour Syslog sécurisé)**, puis cliquez sur **OK (OK)**.

**STEP 6 |** Validez vos modifications et passez en revue les journaux sur le serveur Syslog.

1. Cliquez sur **Commit (Valider)**.
2. Pour passer en revue les journaux, reportez-vous à la documentation de votre logiciel de gestion Syslog. Vous pouvez également passer en revue les descriptions des champs Syslog.

**STEP 7 |** (Optional (Facultatif)) Configurez le pare-feu pour mettre fin à la connexion au serveur syslog lors de l'actualisation du nom de domaine complet.

Lorsque vous configurez un profil de serveur syslog à l'aide d'un nom de domaine complet, le pare-feu maintient sa connexion au serveur syslog par défaut en cas de changement de nom de nom de domaine complet.

Par exemple, vous avez remplacé un serveur syslog existant par un nouveau serveur syslog qui utilise un nom de domaine complet différent. Si vous souhaitez que le pare-feu se connecte au nouveau serveur syslog à l'aide d'un nouveau nom de domaine complet, vous pouvez configurer le pare-feu pour qu'il mette automatiquement fin à sa connexion à l'ancien serveur syslog et établisse une connexion au nouveau serveur syslog à l'aide du nouveau nom de domaine complet.

1. Connectez-vous à l'ILC du pare-feu.
2. Configurez le pare-feu pour mettre fin à la connexion au serveur syslog lors de l'actualisation du nom de domaine complet.

```
admin> set syslogng fqdn-refresh yes
```

## Descriptions des champs Syslog

Les rubriques suivantes répertorient les champs standard de chaque type de journal que les pare-feu Palo Alto Networks peuvent transférer à un serveur externe, ainsi que les niveaux de gravité, les formats personnalisés et les séquences d'échappement. Pour simplifier l'analyse, le délimiteur est une

virgule ; chaque champ est une chaîne Comma-Separated Valeur (Valeur séparée par une virgule ; CSV). L'étiquette FUTURE_USE s'applique aux champs que les pare-feu ne mettent actuellement pas en œuvre.

*Les journaux d'envois WildFire sont un sous-type de journal des menaces et ils utilisent le même format Syslog.*



## Champs du journal de trafic

**Format :** FUTURE_USE, Heure de réception, Numéro de série, Type, Type de contenu/menace, FUTURE_USE, Heure de génération, Adresse source, Adresse de destination, Adresse IP source NAT, Adresse IP de destination NAT, Nom de la règle, Utilisateur source, Utilisateur de destination, Application, Système virtuel, Zone source, Zone de destination, Interface d'entrée, Interface de sortie, Action des journaux, FUTURE_USE, ID de session, Nombre de répétitions, Port source, Port de destination, Port source NAT, Port de destination NAT, Indicateurs, Protocole, Action, Octets, Octets envoyés, Octets reçus, Paquets, Heure de début, Temps écoulé, Catégorie, FUTURE_USE, Numéro de séquence, Indications d'action, Pays source, Pays de destination, FUTURE_USE, Paquets envoyés, Paquets reçus, Motif de fin de session, Hiérarchie de groupes de périphériques niveau 1, Hiérarchie de groupes de périphériques niveau 2, Hiérarchie de groupes de périphériques niveau 3, Hiérarchie de groupes de périphériques niveau 4, Nom du système virtuel, Nom du périphérique, Source d'action, UUID VM source, UUID VM destination, ID/IMSI tunnel, Tag/IMEI surveillance, ID session parent, Heure de début du parent, Type de tunnel, ID d'association SCTP, Blocs SCTP, Blocs SCTP envoyés, Blocs SCTP reçus, UUID de la règle, Connexion HTTP/2, Nombre de basculement d'application, ID de politique, Commutateurs de liens, Cluster SD-WAN, Type de périphérique SD-WAN, Type de cluster SD-WAN, Site SD-WAN, Nom du groupe d'utilisateurs dynamique, Adresse XFF, Catégorie de périphérique source, Profil de périphérique source, Modèle de périphérique source, Fournisseur du périphérique source, Famille de système d'exploitation du périphérique source, Version de système d'exploitation du périphérique source, Nom d'hôte source, Adresse Mac

source, Catégorie de périphérique de destination, Profil de périphérique de destination, Modèle de périphérique de destination, Fournisseur du périphérique de destination, Famille de système d'exploitation du périphérique de destination, Version de système d'exploitation du périphérique de destination, Nom d'hôte de destination, Adresse MAC de destination, ID de conteneur, Espace de noms POD, Nom POD, Liste dynamique externe source, Liste dynamique externe de destination, ID d'hôte, Numéro de série, Groupe d'adresses dynamiques source, Groupe d'adresses dynamiques de destination, Propriétaire de session, Horodatage haute résolution, Motif, Justification, Type de service de tranche A, Différenciateur de tranche, Sous-catégorie d'application, Catégorie d'application, Technologie de l'application, Risque lié à l'application, Caractéristique de l'application, Conteneur de l'application, Saas de l'application, Etat sanctionné de l'application

| Nom du champ | Description |
|---|---|
| Heure de réception (receive_time ou cef-formatted-receive_time) | Heure de réception du journal dans le panneau de gestion. |
| Numéro de série (serial) | Numéro de série du pare-feu ayant généré le journal. |
| Type (type) | Spécifie le type de journal ; la valeur est TRAFFIC. |
| Menace / Type de contenu (sous-type) | Sous-type du journal du trafic ; les valeurs possibles sont start, end, drop et deny<br>• Start — session ouverte<br>• End — session fermée<br>• Drop — session arrêtée avant l'identification de l'application et absence de règle autorisant la session.<br>• Deny — session arrêtée après l'identification de l'application et présence d'une règle de blocage ou absence de règle autorisant la session. |
| Heure de génération (time_generated ou cef-formatted-time_generated) | Heure de génération du journal dans le plan de données. |
| Adresse source (src) | Adresse IP source de la session d'origine. |
| Adresse de destination (dst) | Adresse IP de destination de la session d'origine. |
| Adresse IP source NAT (natsrc) | En cas de NAT source, il s'agit de l'adresse IP source post-NAT. |
| IP de destination NAT (natdst) | En cas de NAT de destination, il s'agit de l'adresse IP de destination post-NAT. |
| Nom de la règle (rule) | Nom de la règle à laquelle la session correspond. |

| Nom du champ | Description |
|---|---|
| Utilisateur source (srcuser) | Nom de l'utilisateur ayant ouvert la session. |
| Utilisateur de destination (dstuser) | Nom de l'utilisateur auquel la session est destinée. |
| Application (app) | Application associée à la session. |
| Système virtuel (vsys) | Système virtuel associé à la session. |
| Zone source (from) | Zone d'origine de la session. |
| Zone de destination (to) | Zone à laquelle la session est destinée. |
| Interface entrante (inbound_if) | Interface d'origine de la session. |
| Interface sortante (outbound_if) | Interface à laquelle la session est destinée. |
| Action du journal (logset) | Profil de transfert des journaux appliqué à la session. |
| ID de session (sessionid) | Identificateur numérique interne appliqué à chaque session. |
| Nombre de répétitions (repeatcnt) | Nombre de sessions avec les mêmes adresses IP source et de destination, application et sous-type constatées sur une période de 5 secondes. |
| Port source (sport) | Port source utilisé par la session. |
| Port de destination (dport) | Port de destination utilisé par la session. |
| Port source NAT (natsport) | Port source post-NAT. |
| Port de destination NAT (natdport) | Port de destination post-NAT. |
| Indicateurs (flags) | Champ 32 bits qui fournit des détails sur la session ; ce champ peut être décodé en ajoutant (opérateur AND) les valeurs à la valeur consignée :<br>• 0x80000000 : la session inclut la capture de paquets (PCAP)<br>• 0x40000000 : la session permet d'autoriser un client à utiliser plusieurs chemins pour se connecter à un hôte de destination<br>• 0x20000000 : le fichier est transmis à WildFire pour l'obtention d'un verdict |

| Nom du champ | Description |
|---|---|
| | • 0x10000000 : la soumission des informations d'identification d'entreprise par l'utilisateur final a été détectée<br>• 0x08000000 : la source du flux se trouve dans la liste d'autorisation et n'est pas assujettie à la protection de reconnaissance<br>• 0x02000000 : session IPv6<br>• 0x01000000 : la session SSL est déchiffrée (proxy SSL)<br>• 0x00800000 : la session est refusée via le filtrage des URL<br>• 0x00400000 : la session a exécuté une traduction NAT<br>• 0x00200000 : les informations sur l'utilisateur de la session ont été capturées via le portail d'authentification<br>• 0x00100000 : le trafic de l'application se trouve sur un port de destination non standard<br>• 0x00080000 : la valeur X-Forwarded-For d'un proxy est contenue dans le champ de l'utilisateur source<br>• 0x00040000 : le journal correspond à une transaction d'une session de proxy http (Proxy Transaction)<br>• 0X00020000 : le flux du client vers serveur est assujetti au transfert basé sur une politique<br>• 0X00010000 : le flux du serveur vers le client est assujetti au transfert basé sur une politique<br>• 0x00008000 : la session permet d'accéder à une page de conteneur (Container Page)<br>• 0x00002000 :la session inclut une correspondance temporaire d'une règle pour le traitement implicite des dépendances d'application. Disponible dans PAN-OS 5.0.0 et versions ultérieures.<br>• 0x00000800 : un retour symétrique est utilisé pour transférer le trafic de cette session<br>• 0x00000400 : le trafic déchiffré est transmis en texte clair via un port miroir<br>• 0x00000100 : le charge du tunnel extérieur fait l'objet d'une inspection |
| Protocole IP (proto) | Protocole IP associé à la session. |
| Action (action) | Action prise pour la session. Les valeurs possibles sont :<br>• allow — la session a été autorisée par la politique<br>• deny — la session a été refusée par la politique<br>• drop — la session a été abandonnée à l'arrière-plan |

| Nom du champ | Description |
|---|---|
| | • drop ICMP — la session a été abandonnée à l'arrière-plan avec un message ICMP inaccessible vers l'hôte ou l'application<br>• reset both — la session a été terminée et une réinitialisation TCP est envoyée aux deux côtés de la connexion<br>• reset client — la session a été terminée et une réinitialisation TCP est envoyée au client<br>• reset server — la session a été terminée et une réinitialisation TCP est envoyée aux serveurs |
| Octets (bytes) | Nombre total d'objets (émission et réception) de la session. |
| Octets envoyés (bytes_sent) | Nombre d'octets dans le sens client/serveur de la session. |
| Octets reçus (bytes_received) | Nombre d'octets dans le sens serveur/client de la session. |
| Paquets (packets) | Nombre total de paquets (émission et réception) de la session. |
| Heure de début (start) | Heure de début de la session. |
| Temps écoulé (elapsed) | Durée écoulée de la session. |
| Catégorie (category) | Catégorie d'URL associée à la session (le cas échéant). |
| Numéro de séquence (seqno) | Identifiant d'entrée de journal 64 bits incrémenté de manière séquentielle ; chaque type de journal contient un espace de numéro unique. |
| Indicateurs d'action (actionflags) | Champ de bits indiquant si le journal a été transféré à Panorama. |
| Pays source (srcloc) | Pays ou région source pour les adresses privées ; 32 octets maximum. |
| Pays de destination (dstloc) | Pays ou région de destination pour les adresses privées. 32 octets maximum. |
| Paquets envoyés (pkts_sent) | Nombre de paquets client/serveur de la session. |
| Paquets reçus (pkts_received) | Nombre de paquets serveur/client de la session. |
| Motif de fin de session (session_end_reason) | Le motif pour lequel une session s'est terminée. S'il existe plusieurs motifs, ce champ affiche uniquement le motif principal (celui dont la priorité est la plus élevée). Les valeurs de motif de |

| Nom du champ | Description |
| --- | --- |
| | fin de session possibles sont les suivantes, par ordre de priorité (où la première est la plus élevée) :<br>• threat : le pare-feu a détecté une menace associée à une action de réinitialisation, d'abandon ou de blocage (d'adresse IP).<br>• policy-deny : la session a été mise en correspondance avec une règle de sécurité dont l'action est le refus ou l'abandon.<br>• Decrypt-cert-validation : la session s'est terminée parce que vous avez configuré le pare-feu pour qu'il bloque le décryptage du proxy de transfert SSL ou l'inspection SSL entrante lorsque la session utilise l'authentification du client ou qu'elle utilise un certificat du serveur ayant l'une ou l'autre des conditions suivantes : expiré, émetteur non approuvé, état inconnu ou expiration de la vérification de l'état. Le motif de fin de session s'affiche également lorsque le certificat du serveur produit une alerte d'erreur fatale de type bad_certificate (mauvais certificat), unsupported_certificate (certificat non pris en charge), certificate_revoked (certificat révoqué), access_denied (accès refusé), ou no_certificate_RESERVED (aucun certificat réservé) (uniquement SSLv3).<br>• decrypt-unsupport-param : la session s'est terminée parce que vous avez configuré le pare-feu pour qu'il bloque le décryptage du proxy de transfert SSL ou l'inspection SSL entrante lorsque la session utilise une version de protocole, un cryptage ou un algorithme non pris en charge. Le motif de fin de session s'affiche lorsque la session produit une alerte d'erreur fatale du type unsupported_extension (extension non prise en charge), unexpected_message (message inattendu), ou handshake_failure (échec de la liaison de segmentation).<br>• decrypt-unsupport-param : la session s'est terminée, car vous avez configuré le pare-feu pour qu'il bloque le décryptage du proxy de transfert SSL ou l'inspection SSL entrante lorsque des ressources sur le pare-feu ou le hardware security module (module de sécurité matériel ; HSM) étaient indisponibles. Le motif de fin de session s'affiche lorsque vous configurez le pare-feu pour qu'il bloque le trafic SSL ayant des erreurs SSH ou qui a produit une alerte d'erreur fatale autre que celles énumérées sous les motifs de fin de session decrypt-cert-validation et decrypt-unsupport-param.<br>• tcp-rst-from-client : le client a envoyé une demande de réinitialisation TCP au serveur.<br>• tcp-rst-from-server : le serveur a envoyé une demande de réinitialisation TCP au client. |

| Nom du champ | Description |
| --- | --- |
| | • resources-unavailable : la session a été abandonnée en raison d'une limitation des ressources système. Par exemple, il se peut que la session ait dépassé le nombre de paquets dans le désordre autorisés par flux ou la file d'attente générale des paquets dans le désordre.<br>• tcp-fin : les deux hôtes de la connexion a/ont envoyé un message TCP FIN pour fermer la session. |
| | • tcp-reuse : une session a été réutilisée et le pare-feu a fermé la session précédente.<br>• decoder : le décodeur a détecté une nouvelle connexion via le protocole (proxy HTTP, par exemple) et a fermé la connexion précédente.<br>• aged-out : la session a expiré.<br>• unknown : cette valeur s'applique aux situations suivantes :<br>  • Les fins de sessions non couvertes par les motifs précédents (par exemple, une commande **`clear session all`**).<br>  • Pour les journaux générés dans une version PAN-OS qui ne prend pas en charge le champ Motif de fin de session (versions ultérieures à PAN-OS 6.1), la valeur est **`unknown`** après une mise à niveau vers la version PAN-OS actuelle ou le chargement des journaux sur le pare-feu.<br>  • Dans Panorama, les journaux reçus des pare-feu pour lesquels la version PAN-OS ne prend pas en charge les motifs de fin de session ont la valeur **`unknown`**.<br>• n/a : cette valeur s'applique lorsque le type de journal du trafic n'est pas **`end`**. |
| Hiérarchie de groupes de périphériques (dg_hier_level_1 à dg_hier_level_4) | Une séquence de numéros d'identification qui indique l'emplacement du groupe de périphériques dans une hiérarchie de groupes de périphériques. Le pare-feu (ou système virtuel) générant le journal inclut le numéro d'identification de chaque ancêtre dans sa hiérarchie de groupes de périphériques. Le groupe de périphériques partagé (niveau 0) n'est pas inclus dans cette structure.<br>Si les valeurs du journal sont 12, 34, 45, 0, cela signifie que le journal a été généré par un pare-feu (ou système virtuel) appartenant au groupe de périphériques 45, et que ses ancêtres sont 34 et 12. Pour afficher les noms des groupes de périphériques correspondant à la valeur 12, 34 ou 45, utilisez l'une des méthodes suivantes : |

| Nom du champ | Description |
|---|---|
| | Requête d'API :<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| Nom du système virtuel (vsys_name) | Le nom du système virtuel associé à la session ; valide uniquement sur les pare-feu pouvant comporter plusieurs systèmes virtuels. |
| Nom du périphérique (device_name) | Le nom d'hôte du pare-feu sur lequel la session a été consignée. |
| Source d'action (action_source) | Indique si l'action prise pour autoriser ou bloquer une application a été définie dans l'application ou dans une politique. Les actions peuvent être allow, deny, drop, reset- server, reset-client ou reset-both pour la session. |
| UUID VM source (src_uuid) | Identifie l'identificateur unique universel source pour une machine virtuelle invitée dans l'environnement VMware NSX. |
| UUID VM de destination (dst_uuid) | Identifie l'identificateur unique universel de destination pour une machine virtuelle invitée dans l'environnement VMware NSX. |
| ID/IMSI du tunnel (tunnelid/imsi) | La International Mobile Subscriber Identity (identité internationale d'abonné mobile ; IMSI) est un numéro unique alloué à chaque abonné mobile dans le système GSM/UTTS/EPS. Ce numéro se compose de chiffres décimaux (de 0 à 9) uniquement, et un maximum de 15 chiffres est permis. |
| Balise de surveillance/IMEI (monitortag/imei) | La International Mobile Equipment Identity (identité internationale d'équipement mobile ; IMEI) est un nombre unique composée de 15 à 16 chiffres qui est alloué à chaque équipement de station mobile. |
| ID de session parent (parent_session_id) | L'ID de la session mise en tunnel. Il s'applique au tunnel interne (s'il y a deux niveaux de tunnellisation) ou au contenu interne (s'il n'y a qu'un seul niveau de tunnellisation) uniquement. |
| Heure de début parent (parent_start_time) | Années/mois/jours heures:minutes:secondes depuis le début de la session de tunnel parent. |
| Type de tunnel (tunnel) | Type de tunnel, par exemple GRE ou IPsec. |
| ID d'association SCTP (assoc_id) | Nombre qui identifie toutes les connexions d'une association entre deux points de terminaison SCTP. |
| Blocs SCTP (chunks) | Somme des blocs SCTP envoyés et reçus pour une association. |

| Nom du champ | Description |
|---|---|
| Blocs SCTP envoyés (chunks_sent) | Nombre de blocs SCTP envoyés pour une association. |
| Blocs SCTP reçus (chunks_received) | Nombre de blocs SCTP reçus pour une association. |
| UUID de la règle (rule_uuid) | L'UUID qui identifie la règle de manière permanente. |
| Connexion HTTP/2 (http2_connection) | Identifie si le trafic a utilisé une connexion HTTP/2 en affichant l'une des valeurs suivantes :<br>• ID de session parent : connexion HTTP/2<br>• 0 : session SSL |
| Nombre de rabats d'application (link_change_count) | Nombre de battements de liaisons qui se sont produits au cours de la session. |
| ID de la politique (policy_id) | Nom de la politique SD-WAN. |
| Commutateurs de liaisons (link_switches) | Contient un maximum de quatre entrées de battements de liaisons, chaque entrée contenant le nom de la liaison, l'étiquette de la liaison, le type de liaison, l'interface physique, l'horodatage, le nombre d'octets lus, le nombre d'octets écrits, l'état de la liaison et la cause du battement de la liaison. |
| Cluster SD-WAN (sdwan_cluster) | Nom du cluster SD-WAN. |
| Type de périphérique SD-WAN (sdwan_device_type) | Type de périphérique (**`hub (pôle)`** ou **`branch (branche)`**). |
| Type de cluster SD-WAN (sdwan_cluster_type) | Type de cluster (**`mesh [maillage]`** ou **`hub-spoke`**). |
| Site SD-WAN (sdwan_site) | Nom du site SD-WAN. |
| Nom de groupe des utilisateurs dynamiques (dynusergroup_name) | Nom du groupe d'utilisateurs dynamiques qui contient l'utilisateur qui a initié la session. |
| Adresse XFF (xff_ip) | L'adresse IP de l'utilisateur qui a demandé la page web ou l'adresse IP de l'avant-dernier périphérique que la requête a traversé. Si la requête passe par un ou plusieurs proxies, équilibreurs de charge ou autres périphériques en amont, le pare-feu affiche l'adresse IP du périphérique le plus récent. |

| Nom du champ | Description |
|---|---|
| Catégorie de périphérique source (src_category) | La catégorie du périphérique que Device-ID identifie comme étant la source du trafic. |
| Profil de périphérique source (src_profile) | Le profil du périphérique que Device-ID identifie comme étant la source du trafic. |
| Modèle de périphérique source (src_model) | Le modèle du périphérique que Device-ID identifie comme étant la source du trafic. |
| Fournisseur du périphérique source (src_vendor) | Le fournisseur du périphérique que Device-ID identifie comme étant la source du trafic. |
| Famille d'OS du périphérique source (src_osfamily) | Le type de système d'exploitation pour le périphérique que Device-ID identifie comme étant la source du trafic. |
| Version d'OS du périphérique source (src_osversion) | La version du système d'exploitation pour le périphérique que Device-ID identifie comme étant la source du trafic. |
| Nom d'hôte source (src_host) | Le nom d'hôte du périphérique que Device-ID identifie comme étant la source du trafic. |
| Adresse MAC source (src_mac) | L'adresse MAC du périphérique que Device-ID identifie comme étant la source du trafic. |
| Catégorie de périphérique de destination (dst_category) | La catégorie du périphérique que Device-ID identifie comme la destination du trafic. |
| Profil de périphérique de destination (dst_profile) | Le profil de périphérique pour le périphérique que Device-ID identifie comme la destination du trafic. |
| Modèle de périphérique de destination (dst_model) | Le modèle du périphérique que Device-ID identifie comme la destination du trafic. |
| Fournisseur du périphérique de destination (dst_vendor) | Le fournisseur du périphérique que Device-ID identifie comme la destination du trafic. |
| Famille de système d'exploitation du périphérique de destination (dst_osfamily) | Le type de système d'exploitation pour le périphérique que Device-ID identifie comme étant la destination du trafic. |
| Version de système d'exploitation du périphérique de destination (dst_osversion) | La version du système d'exploitation pour le périphérique que Device-ID identifie comme étant la destination du trafic. |
| Nom d'hôte de destination (dst_host) | Le nom d'hôte du périphérique que Device-ID identifie comme la destination du trafic. |

| Nom du champ | Description |
|---|---|
| Adresse MAC de destination (dst_mac) | L'adresse MAC du périphérique que Device-ID identifie comme la destination du trafic. |
| ID de conteneur (container_id) | L'ID de conteneur du pod PAN-NGFW sur le nœud Kubernetes où l'application POD est déployée. |
| Espace de noms de POD (pod_namespace) | L'espace de noms de l'application POD étant sécurisé. |
| Nom de POD (pod_name) | L'application POD étant sécurisée. |
| Liste dynamique externe source (src_edl) | Le nom de la liste dynamique externe qui contient l'adresse IP source du trafic. |
| Liste dynamique externe de destination (dst_edl) | Le nom de la liste dynamique externe qui contient l'adresse IP de destination du trafic. |
| ID d'hôte (hostid) | ID unique que GlobalProtect affecte afin d'identifier l'hôte. |
| Numéro de série du périphérique de l'utilisateur (serialnumber) | Numéro de série de la machine ou du périphérique de l'utilisateur. |
| Groupe d'adresses dynamique source (src_dag) | Groupe d'adresse dynamique source de la session d'origine. |
| Groupe d'adresses dynamiques de destination (dst_dag) | Groupe d'adresse dynamique source de la destination d'origine. |
| Propriétaire de session (session_owner) | Le propriétaire original de la session d'homologue haute disponibilité (HA) dans un cluster HA à partir duquel les données de la table de session ont été synchronisées lors du basculement HA. |
| Horodatage haute résolution (high_res_timestamp) | L'heure en milliseconde de réception du journal dans le plan de gestion.<br>Le format pour ce nouveau champ est YYYY-MM-DDThh:ss:sssTZD:<br>• **YYYY**—Année sur quatre chiffres<br>• **MM**—Mois sur deux chiffres<br>• **DD**—Jours du mois sur deux chiffres (01 à 31)<br>• **T**—Indicateur pour le début de l'horodatage |

| Nom du champ | Description |
|---|---|
| | • **hh**—Heures sur deux chiffres utilisant le format 24 heures (00 à 23)<br>• **mm**—Minutes sur deux chiffres (00 à 59)<br>• **ss**—Sondes sur deux chiffres (00 à 60)<br>• **sss**—Un ou plusieurs chiffres pour les millisecondes<br>• **TZD**—Indicateur de fuseau horaire (+hh:mm ou -hh:mm)<br><br>*L'horodatage haute résolution est pris en charge pour les journaux reçus des pare-feux gérés fonctionnant sous PAN-OS 10.1 et les versions ultérieures. Les journaux reçus de pare-feux gérés exécutant PAN-OS 9.1 et les versions antérieures affichent un horodatage `1969-12-31T16:00:00:000-8:00` quelle que soit la date à laquelle le journal a été reçu.* |
| Type de service de tranche A (nsdsai_sst) | Le type de service de tranche A de l'ID de tranche de réseau. |
| Différenciateur de tranche A (nsdsai_sd) | Le différenciateur de tranche A de l'ID de tranche de réseau. |
| Sous-catégorie d'application (subcategory_of_app) | La sous-catégorie d'application spécifiée dans les propriétés de configuration de l'application. |
| Catégorie d'application (category_of_app) | Catégorie d'application spécifiée dans les propriétés de configuration de l'application. Les valeurs sont :<br>• systèmes professionnels<br>• collaboration<br>• Internet grand public<br>• multimédia<br>• Mise en réseau<br>• saas |
| Technologie d'application (technology_of_app) | La technologie d'application spécifiée dans les propriétés de configuration de l'application. Les valeurs sont :<br>• basé sur navigateur<br>• client/serveur<br>• protocole réseau<br>• poste à poste |

| Nom du champ | Description |
|---|---|
| Risque d'application (risk_of_app) | Niveau de risque associé à l'application (1=le plus faible à 5=le plus élevé). |
| Caractéristique de l'application (characteristic_of_app) | Liste séparée par des virgules des caractéristiques applicables de l'application |
| Conteneur d'applications (container_of_app) | L'application parent d'une application. |
| Application SaaS (is_saas_of_app) | Affiche `1` s'il s'agit d'une application SaaS ou `0` s'il ne s'agit pas d'une application SaaS. |
| État sanctionné de l'application (sanctioned_state_of_app) | Affiche `1` si la candidature est sanctionnée ou `0` si la candidature n'est pas sanctionnée. |
| Sous-catégorie d'application (subcategory_of_app) | La sous-catégorie d'application spécifiée dans les propriétés de configuration de l'application. |

## Champs du journal des menaces

**Format** : FUTURE_USE, Heure de réception, Numéro de série, Type, Type de contenu/menace, FUTURE_USE, Heure de génération, Adresse source, Adresse de destination, Adresse IP source NAT, Adresse IP de destination NAT, Nom de la règle, Utilisateur source, Utilisateur de destination, Application, Système virtuel, Zone source, Zone de destination, Interface d'entrée, Interface de sortie, Action des journaux, FUTURE_USE, ID de session, Nombre de répétitions, Port source, Port de destination, Port source NAT, Port de destination NAT, Indicateurs, Protocole, Action, URL/Nom de fichier, ID de menace, Catégorie, Gravité, Sens, Numéro de séquence, Indicateurs d'action, Emplacement source, Emplacement de destination, FUTURE_USE, Type de contenu, PCAP_ID, File Digest, Cloud, Index d'URL, Agent utilisateur, Type de fichier, X-Forwarded-For, Référant, Expéditeur, Sujet, Destinataire, ID de rapport, Hiérarchie de groupes de périphériques niveau 1, Hiérarchie de groupes de périphériques niveau 2, Hiérarchie de groupes de périphériques niveau 3, Hiérarchie de groupes de périphériques niveau 4, Nom du système virtuel, Nom du périphérique, FUTURE_USE, UUID VM source, UUID VM destination, Méthode HTTP, ID/IMSI tunnel, Tag/IMEI surveillance, ID session parent, Heure de début du parent, Type de tunnel, Catégorie de menace, Version du contenu, FUTURE_USE, ID d'association SCTP, ID de protocole de charge utile, En-têtes HTTP, Liste de catégories d'URL, UUID de la règle, Connexion HTTP/2, Nom de groupe des utilisateurs dynamiques, Adresse XFF, Catégorie de périphérique source, Profil de périphérique source, Modèle de périphérique source, Fournisseur du périphérique source, Famille de système d'exploitation du périphérique source, Version de système d'exploitation du périphérique source, Nom d'hôte source, Adresse MAC source, Catégorie de périphérique de destination, Profil de périphérique de destination, Modèle de périphérique de destination, Fournisseur du périphérique de destination, Famille de système d'exploitation du périphérique de destination, Version de système d'exploitation du périphérique de destination, Nom d'hôte de destination, Adresse MAC de destination, ID de conteneur, Espace de noms POD, Nom POD, Liste dynamique externe source, Liste dynamique externe de destination, ID d'hôte, Numéro de série, EDL de domaine, Groupe d'adresses dynamiques

source, Groupe d'adresses dynamiques de destination, Propriétaire de session, Hachage partiel, Horodatage haute résolution, Motif, Justification, Type de service de tranche A, Sous-catégorie d'application, Catégorie d'application, Technologie de l'application, Risque lié à l'application, Caractéristique de l'application, Conteneur de l'application, Saas d'application, Etat sanctionné de l'application

| Nom du champ | Description |
|---|---|
| Heure de réception (receive_time ou cef-formatted-receive_time) | Heure de réception du journal dans le panneau de gestion. |
| Numéro de série (serial #) | Numéro de série du pare-feu ayant généré le journal. |
| Type (type) | Spécifie le type de journal ; la valeur est THREAT. |
| Menace / Type de contenu (sous-type) | Sous-type de journal des menaces. Les valeurs incluent ce qui suit :<br>• data (données) : modèle de données correspondant à un profil de filtrage des données<br>• file : type de fichiers correspondant à un profil de blocage de fichiers.<br>• flood : saturation détectée via un profil de protection de zone.<br>• packet : protection contre les attaques basées sur le paquet qui est déclenchée par un profil de protection de zone.<br>• scan : analyse détectée via un profil de protection de zone.<br>• spyware : spyware détecté via un profil Antispyware.<br>• url : journal de filtrage des URL<br>• ml-virus : virus détecté par WildFire Inline ML via un profil antivirus.<br>• Virus : virus détecté via un profil Antivirus.<br>• vulnerability : exploitation des vulnérabilités détectée via un profil de protection de vulnérabilité.<br>• wildfire : un verdict WildFire généré lorsque le pare-feu envoie un fichier à WildFire via un profil d'analyse WildFire et un verdict (logiciel malveillant, hameçonnage, indésirable ou bénin, selon les informations que vous consignez) est consigné au journal des envois WildFire.<br>• wildfire-virus : virus détecté via un profil Antivirus. |
| Heure de génération (time_generated ou cef-formatted-time_generated) | Heure de génération du journal dans le plan de données. |

| Nom du champ | Description |
|---|---|
| Adresse source (src) | Adresse IP source de la session d'origine. |
| Adresse de destination (dst) | Adresse IP de destination de la session d'origine. |
| Adresse IP source NAT (natsrc) | En cas de NAT source, il s'agit de l'adresse IP source post-NAT. |
| IP de destination NAT (natdst) | En cas de NAT de destination, il s'agit de l'adresse IP de destination post-NAT. |
| Nom de la règle (rule) | Nom de la règle à laquelle la session correspond. |
| Utilisateur source (srcuser) | Nom de l'utilisateur ayant ouvert la session. |
| Utilisateur de destination (dstuser) | Nom de l'utilisateur auquel la session est destinée. |
| Application (app) | Application associée à la session. |
| Système virtuel (vsys) | Système virtuel associé à la session. |
| Zone source (from) | Zone d'origine de la session. |
| Zone de destination (to) | Zone à laquelle la session est destinée. |
| Interface entrante (inbound_if) | Interface d'origine de la session. |
| Interface sortante (outbound_if) | Interface à laquelle la session est destinée. |
| Action du journal (logset) | Profil de transfert des journaux appliqué à la session. |
| ID de session (sessionid) | Identificateur numérique interne appliqué à chaque session. |
| Nombre de répétitions (repeatcnt) | Nombre de sessions avec les mêmes adresses IP source et de destination, application et Type de contenu/de menace sur une période de 5 secondes. |
| Port source (sport) | Port source utilisé par la session. |
| Port de destination (dport) | Port de destination utilisé par la session. |

| Nom du champ | Description |
|---|---|
| Port source NAT (natsport) | Port source post-NAT. |
| Port de destination NAT (natdport) | Port de destination post-NAT. |
| Indicateurs (flags) | Champ 32 bits qui fournit des détails sur la session ; ce champ peut être décodé en ajoutant (opérateur AND) les valeurs à la valeur consignée :<br>• 0x80000000 : la session inclut la capture de paquets (PCAP)<br>• 0x40000000 : la session permet d'autoriser un client à utiliser plusieurs chemins pour se connecter à un hôte de destination<br>• 0x20000000 : le fichier est transmis à WildFire pour l'obtention d'un verdict<br>• 0x10000000 : la soumission des informations d'identification d'entreprise par l'utilisateur final a été détectée<br>• 0x08000000 : la source du flux se trouve dans une liste d'autorisation et n'est pas assujettie à la protection de reconnaissance<br>• 0x02000000 : session IPv6<br>• 0x01000000 : la session SSL est déchiffrée (proxy SSL)<br>• 0x00800000 : la session est refusée via le filtrage des URL<br>• 0x00400000 : la session a exécuté une traduction NAT<br>• 0x00200000 : les informations sur l'utilisateur de la session ont été capturées via le portail d'authentification<br>• 0x00100000 : le trafic de l'application se trouve sur un port de destination non standard<br>• 0x00080000 : la valeur X-Forwarded-For d'un proxy est contenue dans le champ de l'utilisateur source<br>• 0x00040000 : le journal correspond à une transaction d'une session de proxy http (Proxy Transaction)<br>• 0X00020000 : le flux du client vers serveur est assujetti au transfert basé sur une politique<br>• 0X00010000 : le flux du serveur vers le client est assujetti au transfert basé sur une politique<br>• 0x00008000 : la session permet d'accéder à une page de conteneur (Container Page)<br>• 0x00002000 : la session inclut une correspondance temporaire d'une règle pour le traitement implicite des dépendances d'application. Disponible dans PAN-OS 5.0.0 et versions ultérieures. |

| Nom du champ | Description |
|---|---|
| | • 0x00000800 : un retour symétrique est utilisé pour transférer le trafic de cette session<br>• 0x00000400 : le trafic déchiffré est transmis en texte clair via un port miroir<br>• 0x00000010 : le charge du tunnel extérieur fait l'objet d'une inspection |
| Protocole IP (proto) | Protocole IP associé à la session. |
| Action (action) | Action prise pour la session ; les valeurs possibles sont alert, allow, deny, drop, drop-all-packets, reset-client, reset-server, reset-both, block-url.<br>• alert : menace ou URL détectée mais non bloquée<br>• allow : alerte de détection de saturation<br>• deny : mécanisme de détection de saturation activé et rejet du trafic en fonction de la configuration<br>• drop : menace détectée et session associée arrêtée<br>• reset-client : menace détectée et RST TCP envoyée au client<br>• reset-server : menace détectée et RST TCP envoyée au serveur<br>• reset-both : menace détectée et RST TCP envoyée au client et au serveur<br>• block-url : requête d'URL bloquée car elle correspond à une catégorie d'URL définie pour être bloquée<br>• block-ip : menace détectée et adresse IP du client bloquée<br>• random-drop : saturation détectée et le paquet a fait l'objet d'un abandon aléatoire<br>• sinkhole : mise en entonnoir DNS activée<br>• syncookie-sent : alerte syncookie<br>• block-continue (sous-type d'URL uniquement) : une requête HTTP est bloquée et redirigée vers une page Continue sur laquelle se trouve un bouton de confirmation pour poursuivre<br>• continue (sous-type d'URL uniquement) : réponse à une page block-continue URL continue indiquant qu'une requête block-continue a reçu l'autorisation de poursuivre<br>• block-override (sous-type d'URL uniquement) : une requête HTTP est bloquée et redirigée vers une page de contrôle prioritaire par l'administrateur sur laquelle il faut saisir le mot de passe de l'administrateur du pare-feu pour poursuivre<br>• override-lockout (sous-type d'URL uniquement) : un trop grand nombre de tentatives de saisir le mot de passe de contrôle prioritaire de l'administrateur ont échoué à partir de l'adresse |

| Nom du champ | Description |
|---|---|
| | IP source. L'adresse IP est désormais bloquée sur la page de redirection block-override.<br>• override (sous-type d'URL uniquement) : réponse à une page block-override, où le bon mot de passe a été saisi et la requête a été autorisée<br>• block (Wildfire uniquement) : le fichier a été bloqué par le pare-feu et téléchargé sur Wildfire |
| URL/Nom de fichier (misc) | Champ de longueur variable. Un nom de fichier compte un maximum de 63 caractères. Un URL compte un maximum de 1 023 caractères.<br>URl réelle lorsque le sous-type est URL<br>Nom ou type du fichier lorsque le sous-type est file<br>Nom du fichier lorsque le sous-type est virus<br>Nom du fichier lorsque le sous-type est wildwire-virus<br>Nom du fichier lorsque le sous-type est wildfire<br>URL ou nom du fichier lorsque le sous-type est vulnerability, le cas échéant<br>URL lorsque la Threat Category (Catégorie de menace) est `domain-edl` |
| Nom de la menace/ contenu (threatid) | Identifiant Palo Alto Networks pour les menaces connues et personnalisées. Il s'agit d'une chaîne de description suivie d'un identifiant numérique 64 bits entre parenthèses pour certains sous-types.<br>• 8000 – 8099 : détection d'analyse<br>• 8500 – 8599 : détection de saturation<br>• 9999 : journal de filtrage des URL<br>• 10000 – 19999 : détection du logiciel espion Phone Home<br>• 20000 – 29999 : détection de téléchargement de logiciel espion<br>• 30000 – 44999 : détection d'exploitation des vulnérabilités<br>• 52000 – 52999 : détection du type de fichier<br>• 60000 – 69999 : détection de filtrage des données<br>Si le champ Domain EDL (EDL de domaine) est rempli, ce champ est rempli avec la même valeur. |

| Nom du champ | Description |
|---|---|
| | *Les plages d'ID de menace pour la détection des virus, le flux de signature WildFire et les signatures DNS C2 utilisées dans les versions précédentes ont été remplacées par des ID uniques à l'échelle globale permanents. Reportez-vous aux noms de champ Type de contenu/menace (sous-type) et Catégorie de menace (thr_category) pour créer des rapports à jour, filtrer les journaux des menaces, et l'activité ACC.* |
| Catégorie (category) | Pour le sous-type URL, il s'agit de la catégorie d'URL. Pour le sous-type WildFire, il s'agit du verdict sur le fichier et sa valeur est «logiciel malveillant», «hameçonnage», «grayware» ou «bégnin». Pour les autres sous-types, la valeur est «n'importe laquelle». |
| Gravité (severity) | Gravité associée à la menace ; les valeurs possibles sont informational, low, medium, high, critical. |
| Sens (direction) | Indique le sens de l'attaque, client-to-server ou server-to-client :<br>• 0 — le sens de la menace est du client vers le serveur<br>• 1 — le sens de la menace est du serveur vers le client |
| Numéro de séquence (seqno) | Identifiant d'entrée de journal 64 bits incrémenté de manière séquentielle. Chaque type de journal dispose d'un espace de numéros unique. |
| Indicateurs d'action (actionflags) | Champ de bits indiquant si le journal a été transféré à Panorama. |
| Pays source (srcloc) | Pays ou région source pour les adresses privées. 32 octets maximum. |
| Pays de destination (dstloc) | Pays ou région de destination pour les adresses privées. 32 octets maximum. |
| Type de contenu (contenttype) | S'applique uniquement lorsque le sous-type est URL.<br>Type de contenu des données de la réponse HTTP. 32 octets maximum. |
| ID pcap (pcap_id) | L'ID de capture de paquets (pcap) est un entier 64 bits non signé représentant un ID pour corréler des fichiers pcap de menace avec des fichiers pcap étendus faisant partie de ce flux. Tous les journaux des menaces contiennent un pcap_id 0 (aucun pcap associé) ou un ID faisant référence au fichier pcap étendu. |
| File Digest (filedigest) | Uniquement pour le sous-type WildFire ; aucun autre type n'utilise ce champ. |

| Nom du champ | Description |
|---|---|
| | La chaîne filedigest indique le hachage binaire du fichier envoyé pour être analysé par le service WildFire. |
| Cloud (cloud) | Uniquement pour le sous-type WildFire ; aucun autre type n'utilise ce champ.<br>La chaîne cloud indique le FQDN de l'appareil WildFire (privé) ou du cloud WildFire (public) duquel le fichier a été chargé pour analyse. |
| Index d'URL (url_idx) | Utilisé dans les sous-types Filtrage des URL et WildFire.<br>Lorsqu'une application utilise des keepalives TCP pour maintenir une connexion ouverte sur une période de temps, toutes les entrées de journal de cette session portent un même ID de session. Dans ce cas, lorsque vous ne disposez que d'un seul journal des menaces (et ID de session) qui inclut plusieurs entrées d'URL, l'url_idx est un compteur qui vous permet de corréler l'ordre de chaque entrée de journal au cours d'une même session.<br>Par exemple, pour connaître l'URL d'un fichier transféré par le pare-feu à WildFire pour analyse, recherchez l'ID de session et l'url_idx dans le journal d'envois WildFire et recherchez les mêmes ID de session et url_idx dans vos journaux de filtrage des URL. L'entrée de journal correspondant à l'ID de session et l'url_idx contiendra l'URL du fichier transféré à WildFire. |
| Agent utilisateur (user_agent) | Uniquement pour le sous-type Filtrage des URL ; aucun autre type n'utilise ce champ.<br>Le champ Agent utilisateur spécifie le navigateur Web utilisé par l'utilisateur pour accéder à l'URL, Internet Explorer par exemple. Ces informations sont incluses dans la demande HTTP envoyée au serveur. |
| Type de fichier (filetype) | Uniquement pour le sous-type WildFire ; aucun autre type n'utilise ce champ.<br>Spécifie le type de fichier que le pare-feu transfère pour analyse WildFire. |
| X-Forwarded-For (xff) | Uniquement pour le sous-type Filtrage des URL ; aucun autre type n'utilise ce champ.<br>Le champ X-Forwarded-For de l'en-tête HTTP contient l'adresse IP de l'utilisateur qui a demandé la page Web. Il vous permet d'identifier l'adresse IP de l'utilisateur, ce qui est particulièrement utile si vous disposez d'un serveur proxy sur votre réseau qui remplace l'adresse IP de l'utilisateur par sa propre adresse dans le champ d'adresse IP source de l'en-tête du paquet. |

| Nom du champ | Description |
|---|---|
| Référant (referer) | Uniquement pour le sous-type Filtrage des URL ; aucun autre type n'utilise ce champ.<br>Le champ Référant de l'en-tête HTTP contient l'URL de la page Web associée qui relie l'utilisateur à une autre page Web ; il s'agit de la source qui a redirigé (référé) l'utilisateur vers (à) la page Web demandée. |
| Expéditeur (sender) | Spécifie le nom de l'expéditeur d'un e-mail. |
| Sujet (subject) | Spécifie l'objet d'un e-mail. |
| Destinataire (recipient) | Spécifie le nom du destinataire d'un e-mail. |
| ID de rapport (reportid) | Uniquement pour le sous-type WildFire ; aucun autre type n'utilise ce champ.<br>Identifie la demande d'analyse sur le cloud ou l'appareil WildFire. |
| Hiérarchie de groupes de périphériques (dg_hier_level_1 à dg_hier_level_4) | Une séquence de numéros d'identification qui indique l'emplacement du groupe de périphériques dans une hiérarchie de groupes de périphériques. Le pare-feu (ou système virtuel) générant le journal inclut le numéro d'identification de chaque ancêtre dans sa hiérarchie de groupes de périphériques. Le groupe de périphériques partagé (niveau 0) n'est pas inclus dans cette structure.<br>Si les valeurs du journal sont 12, 34, 45, 0, cela signifie que le journal a été généré par un pare-feu (ou système virtuel) appartenant au groupe de périphériques 45, et que ses ancêtres sont 34 et 12. Pour afficher les noms des groupes de périphériques correspondant à la valeur 12, 34 ou 45, utilisez l'une des méthodes suivantes :<br>Requête d'API :<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| Nom du système virtuel (vsys_name) | Le nom du système virtuel associé à la session ; valide uniquement sur les pare-feu pouvant comporter plusieurs systèmes virtuels. |
| Nom du périphérique (device_name) | Le nom d'hôte du pare-feu sur lequel la session a été consignée. |
| UUID VM source (src_uuid) | Identifie l'identificateur unique universel source pour une machine virtuelle invitée dans l'environnement VMware NSX. |
| UUID VM de destination (dst_uuid) | Identifie l'identificateur unique universel de destination pour une machine virtuelle invitée dans l'environnement VMware NSX. |

| Nom du champ | Description |
|---|---|
| Méthode HTTP (http_method) | Uniquement dans les journaux de filtrage des URL. Décrit la méthode HTTP utilisée dans la requête Web. Seules les méthodes suivantes sont journalisées : Connect, Delete, Get, Head, Options, Post, Put. |
| ID/IMSI du tunnel (tunnel_id/imsi) | La International Mobile Subscriber Identity (identité internationale d'abonné mobile ; IMSI) est un numéro unique alloué à chaque abonné mobile dans le système GSM/UTTS/EPS. Ce numéro se compose de chiffres décimaux (de 0 à 9) uniquement, et un maximum de 15 chiffres est permis. |
| Balise de surveillance/ IMEI (monitortag/imei) | La International Mobile Equipment Identity (identité internationale d'équipement mobile ; IMEI) est un nombre unique composée de 15 à 16 chiffres qui est alloué à chaque équipement de station mobile. |
| ID de session parent (parent_session_id) | L'ID de la session mise en tunnel. Il s'applique au tunnel interne (s'il y a deux niveaux de tunnellisation) ou au contenu interne (s'il n'y a qu'un seul niveau de tunnellisation) uniquement. |
| Heure de début de la session parent (parent_start_time) | Années/mois/jours heures:minutes:secondes depuis le début de la session de tunnel parent. |
| Type de tunnel (tunnel) | Type de tunnel, par exemple GRE ou IPsec. |
| Catégorie de menace (thr_category) | Décrit les catégories de menace utilisées pour classer les différents types de signatures de menace.<br>Si une liste dynamique externe de domaine a généré le journal, `domain-edl` rempli ce champ. |
| Version du contenu (contentver) | La version des applications et des menaces sur votre pare-feu lorsque le journal a été généré. |
| ID d'association SCTP (assoc_id) | Nombre qui identifie toutes les connexions d'une association entre deux points de terminaison SCTP. |
| ID de protocole de charge utile (ppid) | ID du protocole de charge utile dans la portion données du<br>bloc de données. |
| En-têtes HTTP (http_headers) | Indique l'en-tête HTTP qui a été inséré dans les entrées du journal des URL sur le pare-feu. |
| Liste de catégorie d'URL (url_category_list) | Présente la liste des catégories de filtrage des URL que le pare-feu a utilisées pour appliquer la politique. |

| Nom du champ | Description |
|---|---|
| UUID de la règle (rule_uuid) | L'UUID qui identifie la règle de manière permanente. |
| Connexion HTTP/2 (http2_connection) | Identifie si le trafic a utilisé une connexion HTTP/2 en affichant l'une des valeurs suivantes :<br>• ID de session de connexion TCP : la session est HTTP/2<br>• 0 : la session n'est pas HTTP/2 |
| Nom de groupe des utilisateurs dynamiques (dynusergroup_name) | Le nom du groupe d'utilisateurs dynamiques qui contient l'utilisateur qui a initié la session. |
| Adresse XFF (xff_ip) | L'adresse IP de l'utilisateur qui a demandé la page web ou l'adresse IP de l'avant-dernier périphérique que la requête a traversé. Si la requête passe par un ou plusieurs proxies, équilibreurs de charge ou autres périphériques en amont, le pare-feu affiche l'adresse IP du périphérique le plus récent. |
| Catégorie de périphérique source (src_category) | La catégorie du périphérique que Device-ID identifie comme étant la source du trafic. |
| Profil de périphérique source (src_profile) | Le profil du périphérique que Device-ID identifie comme étant la source du trafic. |
| Modèle de périphérique source (src_model) | Le modèle du périphérique que Device-ID identifie comme étant la source du trafic. |
| Fournisseur du périphérique source (src_vendor) | Le fournisseur du périphérique que Device-ID identifie comme étant la source du trafic. |
| Famille d'OS du périphérique source (src_osfamily) | Le type de système d'exploitation pour le périphérique que Device-ID identifie comme étant la source du trafic. |
| Version d'OS du périphérique source (src_osversion) | La version du système d'exploitation pour le périphérique que Device-ID identifie comme étant la source du trafic. |
| Nom d'hôte source (src_host) | Le nom d'hôte du périphérique que Device-ID identifie comme étant la source du trafic. |
| Adresse MAC source (src_mac) | L'adresse MAC du périphérique que Device-ID identifie comme étant la source du trafic. |

| Nom du champ | Description |
|---|---|
| Catégorie de périphérique de destination (dst_category) | La catégorie du périphérique que Device-ID identifie comme la destination du trafic. |
| Profil de périphérique de destination (dst_profile) | Le profil de périphérique pour le périphérique que Device-ID identifie comme la destination du trafic. |
| Modèle de périphérique de destination (dst_model) | Le modèle du périphérique que Device-ID identifie comme la destination du trafic. |
| Fournisseur du périphérique de destination (dst_vendor) | Le fournisseur du périphérique que Device-ID identifie comme la destination du trafic. |
| Famille de système d'exploitation du périphérique de destination (dst_osfamily) | Le type de système d'exploitation pour le périphérique que Device-ID identifie comme étant la destination du trafic. |
| Version de système d'exploitation du périphérique de destination (dst_osversion) | La version du système d'exploitation pour le périphérique que Device-ID identifie comme étant la destination du trafic. |
| Nom d'hôte de destination (dst_host) | Le nom d'hôte du périphérique que Device-ID identifie comme la destination du trafic. |
| Adresse MAC de destination (dst_mac) | L'adresse MAC du périphérique que Device-ID identifie comme la destination du trafic. |
| ID de conteneur (container_id) | L'ID de conteneur du pod PAN-NGFW sur le nœud Kubernetes où l'application POD est déployée. |
| Espace de noms de POD (pod_namespace) | L'espace de noms de l'application POD étant sécurisé. |
| Nom de POD (pod_name) | L'application POD étant sécurisée. |
| Liste dynamique externe source (src_edl) | Le nom de la liste dynamique externe qui contient l'adresse IP source du trafic. |

| Nom du champ | Description |
|---|---|
| Liste dynamique externe de destination (dst_edl) | Le nom de la liste dynamique externe qui contient l'adresse IP de destination du trafic. |
| ID d'hôte (hostid) | ID unique que GlobalProtect affecte afin d'identifier l'hôte. |
| Numéro de série du périphérique de l'utilisateur (serialnumber) | Numéro de série de la machine ou du périphérique de l'utilisateur. |
| EDL de domaine (domain_edl) | Le nom de la liste dynamique externe qui contient le nom de domaine du trafic. |
| Groupe d'adresses dynamique source (src_dag) | Groupe d'adresse dynamique source de la session d'origine. |
| Groupe d'adresses dynamiques de destination (dst_dag) | Groupe d'adresse dynamique source de la destination d'origine. |
| Hachage partiel (partial_hash) | Hachage partiel de l'apprentissage machine. |
| Horodatage haute résolution (high_res_timestamp) | L'heure en milliseconde de réception du journal dans le plan de gestion.<br>Le format pour ce nouveau champ est YYYY-MM-DDThh:ss:sssTZD:<br>• **YYYY**—Année sur quatre chiffres<br>• **MM**—Mois sur deux chiffres<br>• **DD**—Jours du mois sur deux chiffres (01 à 31)<br>• **T**—Indicateur pour le début de l'horodatage<br>• **hh**—Heures sur deux chiffres utilisant le format 24 heures (00 à 23)<br>• **mm**—Minutes sur deux chiffres (00 à 59)<br>• **ss**—Sondes sur deux chiffres (00 à 60)<br>• **sss**—Un ou plusieurs chiffres pour les millisecondes<br>• **TZD**—Indicateur de fuseau horaire (+hh:mm ou -hh:mm) |

| Nom du champ | Description |
|---|---|
| | *L'horodatage haute résolution est pris en charge pour les journaux reçus des pare-feux gérés fonctionnant sous PAN-OS 10.1 et les versions ultérieures. Les journaux reçus de pare-feux gérés exécutant PAN-OS 9.1 et les versions antérieures affichent un horodatage `1969-12-31T16:00:00.000-8:00` quelle que soit la date à laquelle le journal a été reçu.* |
| Motif (reason) | Motif de l'action de filtrage des données. |
| Justification (justification) | Justification pour l'action de filtrage des données. |
| Type de service de tranche A (nssai_sst) | Le type de service de tranche A de l'ID de tranche de réseau. |
| Sous-catégorie d'application (subcategory_of_app) | La sous-catégorie d'application spécifiée dans les propriétés de configuration de l'application. |
| Catégorie d'application (category_of_app) | Catégorie d'application spécifiée dans les propriétés de configuration de l'application. Les valeurs sont :<br>• systèmes professionnels<br>• collaboration<br>• Internet grand public<br>• multimédia<br>• Mise en réseau<br>• saas |
| Technologie d'application (technology_of_app) | La technologie d'application spécifiée dans les propriétés de configuration de l'application. Les valeurs sont :<br>• basé sur navigateur<br>• client/serveur<br>• protocole réseau<br>• poste à poste |
| Risque d'application (risk_of_app) | Niveau de risque associé à l'application (1=le plus faible à 5=le plus élevé). |
| Caractéristique de l'application (characteristic_of_app) | Liste séparée par des virgules des caractéristiques applicables de l'application |

| Nom du champ | Description |
|---|---|
| Conteneur d'applications (container_of_app) | L'application parent d'une application. |
| Application SaaS (is_saas_of_app) | Affiche `1` s'il s'agit d'une application SaaS ou `0` s'il ne s'agit pas d'une application SaaS. |
| État sanctionné de l'application (sanctioned_state_of_app) | Affiche `1` si la candidature est sanctionnée ou `0` si la candidature n'est pas sanctionnée. |
| Sous-catégorie d'application (subcategory_of_app) | La sous-catégorie d'application spécifiée dans les propriétés de configuration de l'application. |

## Champs du journal de correspondance HIP

**Format :** FUTURE_USE, Heure de réception, Numéro de série, Type, Type de menace/contenu, FUTURE_USE, Heure de génération, Utilisateur source, Système virtuel, Nom de la machine, Système d'exploitation, Adresse source, HIP, Nombre de répétitions, Type HIP, FUTURE_USE, FUTURE_USE, Numéro de séquence, Indicateurs d'action, Hiérarchie de groupes de périphériques niveau 1, Hiérarchie de groupes de périphériques niveau 2, Hiérarchie de groupes de périphériques niveau 3, Hiérarchie de groupes de périphériques niveau 4, Nom du système virtuel, Nom du périphérique, ID pour le système virtuel, Adresse source IPv6, ID d'hôte, Numéro de série du périphérique de l'utilisateur, Adresse MAC du périphérique, Horodatage haute résolution

| Nom du champ | Description |
|---|---|
| Heure de réception (receive_time ou cef-formatted-receive_time) | Heure de réception du journal dans le panneau de gestion. |
| Numéro de série (serial) | Numéro de série du pare-feu ayant généré le journal. |
| Type (type) | Spécifie le type de journal ; la valeur est HIP-MATCH. |
| Menace / Type de contenu (sous-type) | Sous-type du journal de correspondance HIP ; non utilisé. |
| Heure de génération (time_generated ou cef-formatted-time_generated) | Heure de génération du journal dans le plan de données. |

| Nom du champ | Description |
|---|---|
| Utilisateur source (srcuser) | Nom de l'utilisateur ayant ouvert la session. |
| Système virtuel (vsys) | Système virtuel associé au journal de correspondance HIP. |
| Nom de la machine (machinename) | Nom de la machine de l'utilisateur. |
| Système d'exploitation (os) | Système d'exploitation installé sur la machine ou le périphérique de l'utilisateur (ou sur le système client). |
| Adresse source (src) | Adresse IP de l'utilisateur source. |
| HIP (matchname) | Nom de l'objet ou du profil HIP. |
| Nombre de répétitions (repeatcnt) | Nombre de fois où le profil HIP a correspondu. |
| Type HIP (matchtype) | Si le champ HIP représente un objet HIP ou un profil HIP. |
| Numéro de séquence (seqno) | Identifiant d'entrée de journal 64 bits incrémenté de manière séquentielle ; chaque type de journal contient un espace de numéro unique. |
| Indicateurs d'action (actionflags) | Champ de bits indiquant si le journal a été transféré à Panorama. |
| Hiérarchie de groupes de périphériques (dg_hier_level_1 à dg_hier_level_4) | Une séquence de numéros d'identification qui indique l'emplacement du groupe de périphériques dans une hiérarchie de groupes de périphériques. Le pare-feu (ou système virtuel) générant le journal inclut le numéro d'identification de chaque ancêtre dans sa hiérarchie de groupes de périphériques. Le groupe de périphériques partagé (niveau 0) n'est pas inclus dans cette structure.<br><br>Si les valeurs du journal sont 12, 34, 45, 0, cela signifie que le journal a été généré par un pare-feu (ou système virtuel) appartenant au groupe de périphériques 45, et que ses ancêtres sont 34 et 12. Pour afficher les noms des groupes de périphériques correspondant à la valeur 12, 34 ou 45, utilisez l'une des méthodes suivantes :<br><br>Requête d'API :<br><br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |

| Nom du champ | Description |
|---|---|
| Nom du système virtuel (vsys_name) | Le nom du système virtuel associé à la session ; valide uniquement sur les pare-feu pouvant comporter plusieurs systèmes virtuels. |
| Nom du périphérique (device_name) | Le nom d'hôte du pare-feu sur lequel la session a été consignée. |
| ID du système virtuel (vsys_id) | Un identificateur unique pour un système virtuel sur un pare-feu Palo Alto Networks. |
| Adresse IPv6 du système (srcipv6) | Adresse IPv6 de la machine ou du périphérique de l'utilisateur. |
| ID d'hôte (hostid) | ID unique que GlobalProtect affecte afin d'identifier l'hôte. |
| Numéro de série du périphérique de l'utilisateur (serialnumber) | Numéro de série de la machine ou du périphérique de l'utilisateur. |
| Adresse MAC du périphérique (mac) | Adresse MAC de la machine ou du périphérique de l'utilisateur. |
| Horodatage haute résolution (high_res_timestamp) | L'heure en milliseconde de réception du journal dans le plan de gestion.<br>Le format pour ce nouveau champ est YYYY-MM-DDThh:ss:sssTZD:<br>• **YYYY**—Année sur quatre chiffres<br>• **MM**—Mois sur deux chiffres<br>• **DD**—Jours du mois sur deux chiffres (01 à 31)<br>• **T**—Indicateur pour le début de l'horodatage<br>• **hh**—Heures sur deux chiffres utilisant le format 24 heures (00 à 23)<br>• **mm**—Minutes sur deux chiffres (00 à 59)<br>• **ss**—Sondes sur deux chiffres (00 à 60)<br>• **sss**—Un ou plusieurs chiffres pour les millisecondes<br>• **TZD**—Indicateur de fuseau horaire (+hh:mm ou -hh:mm)<br>*L'horodatage haute résolution est pris en charge pour les journaux reçus des pare-feux gérés fonctionnant sous PAN-OS 10.1 et les versions ultérieures. Les journaux reçus de pare-feux gérés exécutant PAN-OS 9.1 et les versions antérieures affichent un horodatage `1969-12-31T16:00:00:000-8:00` quelle que soit la date à laquelle le journal a été reçu.* |

## Champs du journal GlobalProtect

Format : FUTURE_USE, heure de réception, numéro de série, type, type de menace/contenu, FUTURE_USE, heure générée, système virtuel, ID d'événement, étape, méthode d'authentification, type de tunnel, utilisateur source, région source, nom de la machine, IP publique, IPv6 public, privé IP, IPv6 privé, ID d'hôte, numéro de série, version client, système d'exploitation client, version du système d'exploitation client, nombre de répétitions, raison, erreur, description, état, emplacement, durée de connexion, méthode de connexion, code d'erreur, portail, numéro de séquence, indicateurs d'action , Horodatage haute résolution, Type de sélection, Temps de réponse, Priorité, Tentatives de passerelles, Passerelle, Niveau de hiérarchie de groupes de périphériques 1, Niveau de hiérarchie de groupes de périphériques 2, Niveau de hiérarchie de groupes de périphériques 3, Niveau de hiérarchie de groupes de périphériques 4, Nom de système virtuel, Nom de périphérique, Virtuel Identifiant système

| Nom du champ | Description |
|---|---|
| Heure de réception (receive_time) | L'heure de réception du journal dans le panneau de gestion. |
| Numéro de série (serial) | Le numéro de série du pare-feu ayant généré le journal. |
| Type (type) | Spécifie le type de journal ; la valeur est GLOBALPROTECT. |
| Menace / Type de contenu (sous-type) | Sous-type de journal des menaces. Les valeurs incluent ce qui suit :<br>• data (données) : modèle de données correspondant à un profil de filtrage des données<br>• file : type de fichiers correspondant à un profil de blocage de fichiers.<br>• flood : saturation détectée via un profil de protection de zone.<br>• packet : protection contre les attaques basées sur le paquet qui est déclenchée par un profil de protection de zone.<br>• scan : analyse détectée via un profil de protection de zone.<br>• spyware : spyware détecté via un profil Antispyware.<br>• url : journal de filtrage des URL<br>• Virus : virus détecté via un profil Antivirus.<br>• vulnerability : exploitation des vulnérabilités détectée via un profil de protection de vulnérabilité.<br>• wildfire : un verdict WildFire généré lorsque le pare-feu envoie un fichier à WildFire via un profil d'analyse WildFire et un verdict (malveillant, hameçonnage, indésirable ou bénin, selon les informations que vous consignez) est consigné au journal des envois WildFire.<br>• wildfire-virus : virus détecté via un profil Antivirus. |

| Nom du champ | Description |
|---|---|
| Heure de génération (time_generated) | L'heure de génération du journal dans le plan de données. |
| Système virtuel (vsys) | Le système virtuel associé à la session. |
| ID d'événement (eventid) | Une chaîne indiquant le nom de l'événement. |
| Étape (stage) | Une chaîne montrant l'étape de la connexion (par exemple, **before-login**, **login** ou **tunnel**). |
| Méthode d'authentification (auth_method) | Une chaîne montrant le type d'authentification, comme **LDAP**, **RADIUS** ou **SAML**. |
| Type de tunnel (tunnel_type) | Le type de tunnel (SSLVPN ou IPSec). |
| Utilisateur source (srcuser) | Le nom de l'utilisateur ayant ouvert la session. |
| Région source (srcregion) | La région de l'utilisateur ayant ouvert la session. |
| Nom de la machine (machinename) | Le nom de la machine de l'utilisateur. |
| Adresse IP publique (public_ip) | L'adresse IP publique de l'utilisateur ayant ouvert la session. |
| Adresse IPv6 publique (public_ipv6) | L'adresse IPv6 publique de l'utilisateur ayant ouvert la session. |
| Adresse IP privée (private_ip) | L'adresse IP privée de l'utilisateur ayant ouvert la session. |
| Adresse IPv6 privée (private_ipv6) | L'adresse IPv6 privée de l'utilisateur ayant ouvert la session. |
| ID d'hôte (hostid) | L'ID unique que GlobalProtect affecte afin d'identifier l'hôte. |
| Numéro de série (serialnumber) | Le numéro de série de la machine ou du périphérique de l'utilisateur. |
| Version du client (client_ver) | La version de l'application GlobalProtect du client. |

| Nom du champ | Description |
|---|---|
| Système d'exploitation du client (client_os) | Le type de système d'exploitation du périphérique du client (par exemple, Windows ou Linux). |
| Version du système d'exploitation du client (client_os_ver) | La version du système d'exploitation du périphérique du client. |
| Nombre de répétitions (repeatcnt) | Le nombre de sessions ayant la même adresse IP source, la même adresse IP de destination, la même application et le même sous-type que GlobalProtect a détecté au cours des cinq dernières secondes. |
| Motif (reason) | Une chaîne qui montre le motif de la quarantaine. |
| Erreur (error) | Une chaîne montrant l'erreur qui s'est produite dans un événement. |
| Description (opaque) | Tout renseignement supplémentaire sur un événement qui s'est produit. |
| État (status) | L'état (réussite ou échec) de l'événement. |
| Emplacement (location) | Une chaîne montrant l'emplacement défini par l'administrateur du portail ou de la passerelle GlobalProtect. |
| Durée de la connexion (login_duration) | La durée, en secondes, pendant laquelle l'utilisateur est connecté à la passerelle GlobalProtect, de la connexion à la déconnexion. |
| Méthode de connexion (connect_method) | Une chaîne montrant la manière dont l'application GlobalProtect se connecte à la passerelle, (par exemple, `on-demand` ou `user-logon`. |
| Code d'erreur (error_code) | Un nombre entier associé aux erreurs qui se sont produites. |
| Portail (portal) | Le nom du portail ou de la passerelle GlobalProtect. |
| Numéro de séquence (seqno) | Identifiant d'entrée de journal 64 bits incrémenté de manière séquentielle ; chaque type de journal contient un espace de numéro unique. |
| Indicateurs d'action (actionflags) | Champ de bits indiquant si le journal a été transféré à Panorama. |
| Méthode de sélection de passerelle (selection_type) | La méthode de connexion qui est choisie pour se connecter à la passerelle.<br>• manual (manuelle) : la passerelle à laquelle vous souhaitez que l'application GlobalProtect se connecte manuellement. |

| Nom du champ | Description |
|---|---|
| | • preferred (préférée) : la passerelle préférée à laquelle vous souhaitez que l'application GlobalProtect se connecte.<br>• auto : se connecter automatiquement à la **meilleure passerelle disponible** en fonction de la priorité attribuée à la passerelle et du temps de réponse. |
| Temps de réponse SSL (response_time) | Le temps de réponse SSL de la passerelle sélectionnée qui est mesuré en millisecondes sur le terminal pendant la configuration du tunnel. |
| Priorité de passerelle (priority) | L'ordre de priorité de la passerelle qui est basée sur la plus haute (1), haute (2), moyenne (3), basse (4), ou la plus basse (5) à laquelle l'application GlobalProtect peut se connecter. |
| Passerelles tentées (attempted_gateways) | Les champs qui sont collectés pour chaque tentative de connexion de passerelle avec le nom de la passerelle, le temps de réponse SSL et la priorité (consultez Priorité de la passerelle dans une configuration à passerelles multiples). Chaque entrée de champ est séparée par des virgules telles que `g82-gateway,12,3`. Chaque entrée de passerelle est séparée par des points-virgules tels que `g83-gateway,10,2;g84-gateway,-1,1`. |
| Nom de la passerelle d'application (gateway) | Le nom de la passerelle qui est spécifié sur la configuration du portail. |
| Hiérarchie de groupes de périphériques (dg_hier_level_1 à dg_hier_level_4) | Une séquence de numéros d'identification qui indique l'emplacement du groupe de périphériques dans une hiérarchie de groupes de périphériques. Le pare-feu (ou système virtuel) générant le journal inclut le numéro d'identification de chaque ancêtre dans sa hiérarchie de groupes de périphériques. Le groupe de périphériques partagé (niveau 0) n'est pas inclus dans cette structure.<br>Si les valeurs du journal sont 12, 34, 45, 0, cela signifie que le journal a été généré par un pare-feu (ou système virtuel) appartenant au groupe de périphériques 45, et que ses ancêtres sont 34 et 12. Pour afficher les noms des groupes de périphériques correspondant à la valeur 12, 34 ou 45, utilisez l'une des méthodes suivantes :<br>Requête d'API :<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| Nom du système virtuel (vsys_name) | Le nom du système virtuel associé à la session ; valide uniquement sur les pare-feu pouvant comporter plusieurs systèmes virtuels. |

| Nom du champ | Description |
|---|---|
| Nom du périphérique (device_name) | Le nom d'hôte du pare-feu sur lequel la session a été consignée. |
| ID du système virtuel (vsys_id) | Un identificateur unique pour un système virtuel sur un pare-feu Palo Alto Networks. |

## Champs des journaux des indicateurs d'adresse IP

Format : FUTURE_USE, Heure de réception, Série, Type, Menace/Type de contenu, FUTURE_USE, Heure de génération, Système virtuel, IP Source, Nom de l'étiquette , ID d'événement, Nombre de répétitions, Seuil d'expiration, Nom source des données, Type de source de données, Sous-type de source de données, Numéro de séquence, Indicateurs d'action, Hiérarchie de groupes de périphériques niveau 1, Hiérarchie de groupes de périphériques niveau 2, Hiérarchie de groupes de périphériques niveau 3, Hiérarchie de groupes de périphériques niveau 4, Nom du système virtuel, Nom du périphérique, ID du système virtuel, Horodatage haute résolution

| Nom du champ | Description |
|---|---|
| Heure de réception (receive_time ou cef-formatted-receive_time) | L'heure de réception du journal dans le panneau de gestion. |
| Numéro de série (serial) | Le numéro de série du pare-feu ayant généré le journal. |
| Type (type) | Spécifie le type de journal ; la valeur est IPTAG. |
| Menace / Type de contenu (sous-type) | Le sous-type du journal de correspondance HIP ; non utilisé. |
| Heure de génération (time_generated ou cef-formatted-time_generated) | L'heure de génération du journal dans le plan de données. |
| Système virtuel (vsys) | Le système virtuel associé au journal de correspondance HIP. |
| IP source (src) | L'adresse IP de l'utilisateur source. |
| Nom de l'étiquette (tag_name) | L'étiquette mise en correspondance avec l'adresse IP source. |
| ID d'événement (event_id) | Une chaîne indiquant le nom de l'événement. |

| Nom du champ | Description |
|---|---|
| Nombre de répétitions (repeatcnt) | Le nombre de sessions avec les mêmes adresses IP source et de destination, application et sous-type constatées sur une période de 5 secondes. |
| Seuil d'expiration (timeout) | La durée de temps avant l'expiration du mappage adresse IP/étiquette pour l'adresse IP source. |
| Nom de source de données (datasourcename) | Le nom de la source à partir de laquelle les informations de mappage sont collectées. |
| Type de source de données (datasource_type) | La source à partir de laquelle les informations de mappage sont collectées. |
| Sous-type de source de données (datasource_subtype) | Le mécanisme utilisé pour identifier les mappages IP/Utilisateur dans une source de données. |
| Numéro de séquence (seqno) | Identifiant d'entrée de journal 64 bits incrémenté de manière séquentielle. Chaque type de journal dispose d'un espace de numéros unique. |
| Indicateurs d'action (actionflags) | Le champ de bits indiquant si le journal a été transféré à Panorama. |
| Hiérarchie de groupes de périphériques (dg_hier_level_1 à dg_hier_level_4) | Une séquence de numéros d'identification qui indique l'emplacement du groupe de périphériques dans une hiérarchie de groupes de périphériques. Le pare-feu (ou système virtuel) générant le journal inclut le numéro d'identification de chaque ancêtre dans sa hiérarchie de groupes de périphériques, sauf le groupe de périphériques partagés (niveau 0), qui n'est pas inclus dans cette structure.<br>Si les valeurs du journal sont 12, 34, 45 et 0, c'est que le journal a été généré par un pare-feu (ou système virtuel) appartenant au groupe de périphériques 45, et que ses ancêtres sont 34 et 12. Pour afficher les noms des groupes de périphériques correspondant à la valeur 12, 34 ou 45, utilisez l'une des méthodes suivantes :<br>Requête d'API :<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| Nom du système virtuel (vsys_name) | Le nom du système virtuel associé à la session ; valide uniquement sur les pare-feu pouvant comporter plusieurs systèmes virtuels. |

| Nom du champ | Description |
|---|---|
| Nom du périphérique (device_name) | Le nom d'hôte du pare-feu sur lequel la session a été consignée. |
| ID du système virtuel (vsys_id) | Un identificateur unique pour un système virtuel sur un pare-feu Palo Alto Networks. |
| Horodatage haute résolution (high_res_timestamp) | L'heure en milliseconde de réception du journal dans le plan de gestion.<br>Le format pour ce nouveau champ est YYYY-MM-DDThh:ss:sssTZD:<br>• **YYYY**—Année sur quatre chiffres<br>• **MM**—Mois sur deux chiffres<br>• **DD**—Jours du mois sur deux chiffres (01 à 31)<br>• **T**—Indicateur pour le début de l'horodatage<br>• **hh**—Heures sur deux chiffres utilisant le format 24 heures (00 à 23)<br>• **mm**—Minutes sur deux chiffres (00 à 59)<br>• **ss**—Sondes sur deux chiffres (00 à 60)<br>• **sss**—Un ou plusieurs chiffres pour les millisecondes<br>• **TZD**—Indicateur de fuseau horaire (+hh:mm ou -hh:mm)<br>*L'horodatage haute résolution est pris en charge pour les journaux reçus des pare-feux gérés fonctionnant sous PAN-OS 10.1 et les versions ultérieures. Les journaux reçus de pare-feux gérés exécutant PAN-OS 9.1 et les versions antérieures affichent un horodatage `1969-12-31T16:00:00:000-8:00` quelle que soit la date à laquelle le journal a été reçu.* |

## Champs des journaux User-ID

**Format** : FUTURE_USER, Heure de réception, Numéro de série, Type, Menace / Type de contenu, FUTURE_USE, Heure de génération, Système virtuel, IP Source, Utilisateur, Nom de source de données, ID d'événement, Nombre de répétitions, Seuil d'expiration, Port source, Port de destination, Type de source de données, Numéro de séquence, Indicateurs d'action, Hiérarchie de groupes de périphériques niveau 1, Hiérarchie de groupes de périphériques niveau 2, Hiérarchie de groupes de périphériques niveau 3, Hiérarchie de groupes de périphériques niveau 4, Nom du système virtuel, Nom du périphérique, ID du système virtuel, Type de facteur, Délai d'exécution du facteur, Nombre de facteurs, FUTURE_USE, FUTURE_USE, Indicateurs de groupes d'utilisateurs, Utilisateur selon la source, Horodatage haute résolution

| Nom du champ | Description |
|---|---|
| Heure de réception (receive_time ou cef-formatted-receive_time) | Heure de réception du journal dans le panneau de gestion. |
| Numéro de série (serial) | Numéro de série du pare-feu ayant généré le journal. |
| Type (type) | Spécifie le type de journal ; la valeur est USERID. |
| Menace / Type de contenu (sous-type) | Sous-type de journal User-ID ; les valeurs sont les suivantes : login (connexion), logout (déconnexion), register-tag (enregistrement d'étiquette) et unregister-tag (désenregistrement d'étiquette).<br>• login (connexion) : l'utilisateur s'est connecté.<br>• logout (déconnexion) : l'utilisateur s'est déconnecté.<br>• register-tag (enregistrement d'étiquette) : indique qu'une ou plusieurs étiquettes ont été enregistrées pour l'utilisateur.<br>• unregister-tag (désenregistrement d'étiquette) : indique qu'une ou plusieurs étiquettes ont été désenregistrées pour l'utilisateur. |
| Heure de génération (time_generated ou cef-formatted-time_generated) | L'heure de génération du journal dans le plan de données. |
| Système virtuel (vsys) | Système virtuel associé au journal de configuration. |
| IP source (ip) | Adresse IP source de la session d'origine. |
| Utilisateur (user) | Identifie l'utilisateur final. |
| Nom de source de données (datasourcename) | La source d'User-ID qui envoie le mappage IP (Port)-Utilisateur. |
| ID d'événement (eventid) | Chaîne indiquant le nom de l'événement. |
| Nombre de répétitions (repeatcnt) | Nombre de sessions avec les mêmes adresses IP source et de destination, application et sous-type constatées sur une période de 5 secondes. |
| Seuil d'expiration (timeout) | Temps d'expiration après lequel les mappages IP/Utilisateur sont effacés. |
| Port source (beingport) | Port source utilisé par la session. |

| Nom du champ | Description |
|---|---|
| Port de destination (endport) | Port de destination utilisé par la session. |
| Source de données (datasource) | La source à partir de laquelle les informations de mappage sont collectées. |
| Type de source de données (datasourcetype) | Mécanisme utilisé pour identifier les mappages IP/Utilisateur dans une source de données. |
| Numéro de séquence (seqno) | Numéro de série du pare-feu ayant généré le journal. |
| Indicateurs d'action (actionflags) | Champ de bits indiquant si le journal a été transféré à Panorama. |
| Hiérarchie de groupes de périphériques (dg_hier_level_1 à dg_hier_level_4) | Une séquence de numéros d'identification qui indique l'emplacement du groupe de périphériques dans une hiérarchie de groupes de périphériques. Le pare-feu (ou système virtuel) générant le journal inclut le numéro d'identification de chaque ancêtre dans sa hiérarchie de groupes de périphériques. Le groupe de périphériques partagé (niveau 0) n'est pas inclus dans cette structure.<br>Si les valeurs du journal sont 12, 34, 45, 0, cela signifie que le journal a été généré par un pare-feu (ou système virtuel) appartenant au groupe de périphériques 45, et que ses ancêtres sont 34 et 12. Pour afficher les noms des groupes de périphériques correspondant à la valeur 12, 34 ou 45, utilisez l'une des méthodes suivantes :<br>API query: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| Nom du système virtuel (vsys_name) | Le nom du système virtuel associé à la session ; valide uniquement sur les pare-feu pouvant comporter plusieurs systèmes virtuels. |
| Nom du périphérique (device_name) | Le nom d'hôte du pare-feu sur lequel la session a été consignée. |
| ID du système virtuel (vsys_id) | Un identificateur unique pour un système virtuel sur un pare-feu Palo Alto Networks. |
| Type de facteur (factortype) | Fournisseur utilisé pour authentifier un utilisateur lorsque l'authentification multifacteur est présente. |
| Délai d'exécution du facteur (factorcompletiontime) | Heure à laquelle l'authentification a été terminée. |

| Nom du champ | Description |
|---|---|
| Nombre de facteurs (factorno) | Indique l'utilisation de l'authentification principale (1) ou de facteurs supplémentaires (2, 3). |
| Indicateurs de groupes d'utilisateurs (ugflags) | Affiche si le groupe d'utilisateurs qui a été trouvé au cours du mappage de groupe. Les valeurs prises en charge sont les suivantes :<br>• Groupe d'utilisateurs trouvé : indique si l'utilisateur a pu être associé à un groupe.<br>• Utilisateur dupliqué : indique si des utilisateurs en double ont été trouvés dans un groupe d'utilisateurs. `N/A` s'affiche si aucun groupe d'utilisateurs n'a été trouvé. |
| Utilisateur selon la source (userbysource) | Indique le nom d'utilisateur reçu de la source par l'intermédiaire du mappage de l'adresse IP au nom d'utilisateur. |
| Horodatage haute résolution (high_res_timestamp) | L'heure en milliseconde de réception du journal dans le plan de gestion.<br>Le format pour ce nouveau champ est YYYY-MM-DDThh:ss:sssTZD:<br>• **YYYY**—Année sur quatre chiffres<br>• **MM**—Mois sur deux chiffres<br>• **DD**—Jours du mois sur deux chiffres (01 à 31)<br>• **T**—Indicateur pour le début de l'horodatage<br>• **hh**—Heures sur deux chiffres utilisant le format 24 heures (00 à 23)<br>• **mm**—Minutes sur deux chiffres (00 à 59)<br>• **ss**—Sondes sur deux chiffres (00 à 60)<br>• **sss**—Un ou plusieurs chiffres pour les millisecondes<br>• **TZD**—Indicateur de fuseau horaire (+hh:mm ou -hh:mm)<br>*L'horodatage haute résolution est pris en charge pour les journaux reçus des pare-feux gérés fonctionnant sous PAN-OS 10.1 et les versions ultérieures. Les journaux reçus de pare-feux gérés exécutant PAN-OS 9.1 et les versions antérieures affichent un horodatage `1969-12-31T16:00:00:000-8:00` quelle que soit la date à laquelle le journal a été reçu.* |

## Champs du journal de décryptage

**Format :** FUTURE_USE, Heure de réception, Numéro de série, Type, Type de menace/contenu, Version de configuration, Heure de génération, Adresse source, Adresse de destination, IP source NAT, IP de destination NAT, Règle, Utilisateur source, Utilisateur de destination, Application,

Système virtuel, Zone source, Zone de destination, Interface entrante, Interface sortante, Action de journalisation, Heure enregistrée, ID de session, Nombre de répétitions, Port source, Port de destination, Port source NAT, Port de destination NAT, Indicateurs, Protocole IP, Action, Tunnel, FUTURE_USE, FUTURE_USE, UUID de VM source, UUID de VM de destination, UUID de règle, Étape pour le client vers le pare-feu, Étape pour le pare-feu vers le serveur, Version TLS, Algorithme d'échange de clés, Algorithme de chiffrement, Algorithme de hachage, Nom de politique, Courbe elliptique, Index d'erreur, État de la racine, État de la chaîne, Type de proxy, Numéro de série du certificat, Empreinte digitale, Date de début du certificat, Date de fin du certificat, Version du certificat, Taille du certificat, Longueur du nom commun, Longueur du nom commun de l'émetteur, Longueur du nom commun de la racine, Longueur du SNI, Indicateurs du certificat, Nom commun du sujet, Nom commun du sujet de l'émetteur, Nom commun du sujet de la racine, Indication du nom du serveur, Erreur, ID du conteneur, Espace de noms POD, Nom de POD, Liste dynamique externe de la source, Liste dynamique externe de la destination, Groupe d'adresses dynamiques de la source, Groupe d'adresses dynamiques de la destination, Horodatage haute résolution, Catégorie de dispositif source, Profil de dispositif source, Modèle de dispositif source, Fournisseur de dispositif source, Famille de système d'exploitation du dispositif source, Version de système d'exploitation du dispositif source, Nom d'hôte de la source, Adresse Mac de la source, Catégorie de périphérique de destination, Profil de périphérique de destination, Modèle de périphérique de destination, Fournisseur du périphérique de destination, Famille de système d'exploitation du périphérique de destination, Version de système d'exploitation du périphérique de destination, Nom d'hôte de destination, Adresse Mac de destination, Numéro de séquence, Indicateurs d'action, Niveau de la Hiérarchie du Groupe de périphériques, Niveau 2 de la Hiérarchie du Groupe de périphériques, Niveau 3 de la Hiérarchie du Groupe de périphériques, Niveau 4 de la Hiérarchie du Groupe de périphériques, Nom du système virtuel, Nom du périphérique, ID du système virtuel, Sous-catégorie de l'application, Catégorie de l'application, Technologie de l'application, Risque lié à l'application, Caractéristique de l'application, Conteneur de l'application, Saas de l'application, Etat sanctionné de l'application

| Nom du champ | Description |
|---|---|
| Heure de réception (receive_time ou cef-formatted-receive_time) | Heure de réception du journal dans le panneau de gestion. |
| Numéro de série (serial) | Numéro de série du pare-feu ayant généré le journal. |
| Type (type) | Spécifie le type de journal ; la valeur est DECRYPTION. |
| Type de contenu/ menace (subtype) | Pas utilisé dans le journal de décryptage. |
| Version de configuration (config_ver) | La version du logiciel. |

| Nom du champ | Description |
|---|---|
| Heure de génération (time_generated) | Heure de génération du journal dans le plan de données. |
| Adresse source (src) | Adresse IP source de la session d'origine. |
| Adresse de destination (dst) | Adresse IP de destination de la session d'origine. |
| Adresse IP source NAT (natsrc) | En cas de NAT source, il s'agit de l'adresse IP source post-NAT. |
| IP de destination NAT (natdst) | En cas de NAT de destination, il s'agit de l'adresse IP de destination post-NAT. |
| Règle (rule) | Règle de politique de sécurité qui contrôle le trafic de la session. |
| Utilisateur source (srcuser) | Nom de l'utilisateur ayant ouvert la session. |
| Utilisateur de destination (dstuser) | Nom de l'utilisateur auquel la session est destinée. |
| Application (app) | Application associée à la session. |
| Système virtuel (vsys) | Système virtuel associé à la session. |
| Zone source (from) | Zone d'origine de la session. |
| Zone de destination (to) | Zone à laquelle la session est destinée. |
| Interface entrante (inbound_if) | Interface d'origine de la session. |
| Interface sortante (outbound_if) | Interface à laquelle la session est destinée. |
| Action du journal (logset) | Profil de transfert du journal appliqué à la session. |
| Heure enregistrée (time_received) | L'heure à laquelle le journal a été reçu. |
| ID de session (sessionid) | Identificateur numérique interne appliqué à chaque session. |

| Nom du champ | Description |
|---|---|
| Nombre de répétitions (repeatcnt) | Nombre de sessions avec les mêmes adresses IP source et de destination, application et Type de contenu/menace sur une période de 5 secondes. |
| Port source (sport) | Port source utilisé par la session. |
| Port de destination (dport) | Port de destination utilisé par la session. |
| Port source NAT (natsport) | Port source post-NAT. |
| Port de destination NAT (natdport) | Port de destination post-NAT. |
| Indicateurs (flags) | Champ 32 bits qui fournit des détails sur la session ; ce champ peut être décodé en ajoutant (opérateur AND) les valeurs à la valeur consignée :<br>• 0x80000000 : la session inclut la capture de paquets (PCAP)<br>• 0x40000000 : la session permet d'autoriser un client à utiliser plusieurs chemins pour se connecter à un hôte de destination<br>• 0x20000000 : le fichier est transmis à WildFire pour l'obtention d'un verdict<br>• 0x10000000 : la soumission des informations d'identification d'entreprise par l'utilisateur final a été détectée<br>• 0x08000000 : la source du flux se trouve dans la liste d'autorisation et n'est pas assujettie à la protection de reconnaissance<br>• 0x02000000 : session IPv6<br>• 0x01000000 : la session SSL est déchiffrée (proxy SSL)<br>• 0x00800000 : la session est refusée via le filtrage des URL<br>• 0x00400000 : la session a exécuté une traduction NAT<br>• 0x00200000 : les informations sur l'utilisateur de la session ont été capturées via le portail d'authentification<br>• 0x00100000 : le trafic de l'application se trouve sur un port de destination non standard<br>• 0x00080000 : la valeur X-Forwarded-For d'un proxy est contenue dans le champ de l'utilisateur source<br>• 0x00040000 : le journal correspond à une transaction d'une session de proxy http (Proxy Transaction)<br>• 0X00020000 : le flux du client vers serveur est assujetti au transfert basé sur une politique |

| Nom du champ | Description |
|---|---|
| | • 0X00010000 : le flux du serveur vers le client est assujetti au transfert basé sur une politique<br>• 0x00008000 : la session permet d'accéder à une page de conteneur (Container Page)<br>• 0x00002000 :la session inclut une correspondance temporaire d'une règle pour le traitement implicite des dépendances d'application. Disponible dans PAN-OS 5.0.0 et versions ultérieures.<br>• 0x00000800 : un retour symétrique est utilisé pour transférer le trafic de cette session<br>• 0x00000400 : le trafic déchiffré est transmis en texte clair via un port miroir<br>• 0x00000100 : le charge du tunnel extérieur fait l'objet d'une inspection |
| Protocole IP (proto) | Protocole IP associé à la session. |
| Action (action) | Action prise pour la session. Les valeurs possibles sont :<br>• allow — la session a été autorisée par la politique<br>• deny — la session a été refusée par la politique<br>• drop — la session a été abandonnée à l'arrière-plan<br>• drop ICMP — la session a été abandonnée à l'arrière-plan avec un message ICMP inaccessible vers l'hôte ou l'application<br>• reset both — la session a été terminée et une réinitialisation TCP est envoyée aux deux côtés de la connexion<br>• reset client — la session a été terminée et une réinitialisation TCP est envoyée au client<br>• reset server — la session a été terminée et une réinitialisation TCP est envoyée aux serveurs |
| Tunnel (tunnel) | Type de tunnel. |
| UUID VM source (src_uuid) | L'identificateur unique universel source pour une machine virtuelle invitée dans l'environnement VMware NSX. |
| UUID VM de destination (dst_uuid) | L'identificateur unique universel de destination pour une machine virtuelle invitée dans l'environnement VMware NSX. |
| UUID pour la règle (rule_uuid) | L'UUID qui identifie la règle de manière permanente. |

| Nom du champ | Description |
|---|---|
| Étape pour le client vers le pare-feu (hs_stage_c2f) | L'étape de la communication TLS entre le client et le pare-feu, par exemple, Bonjour client, Bonjour serveur, Certificat, Échange de clés client/serveur, etc. |
| Étape pour le pare-feu vers le serveur (hs_stage_f2s) | L'étape de la communication TLS entre le pare-feu et le serveur. |
| Version TLS (tls_version) | La version du protocole TLS utilisée pour la session. |
| Algorithme d'échange de clés (tls_keyxchg) | L'algorithme d'échange de clés utilisé pour la session. |
| Algorithme de chiffrement (tls_enc) | L'algorithme utilisé pour crypter les données de la session, comme AES-128-CBC, AES-256-GCM, etc. |
| Algorithme de hachage (tls_auth) | L'algorithme d'authentification utilisé pour la session, par exemple, SHA, SHA256, SHA384, etc. |
| Nom de politique (policy_name) | Le nom de la politique de décryptage associée à la session. |
| Courbe elliptique (ec_curve) | La courbe de cryptographie elliptique que le client et le serveur négocient et utilisent pour les connexions qui utilisent les suites de chiffrement ECDHE. |
| Index d'erreur (err_index) | Le type d'erreur qui s'est produite : Chiffrement, Ressource, Reprise, Version, Protocole, Certificat, Fonctionnalité ou HSM. |
| État de la racine (root_status) | L'état du certificat racine, par exemple, fiable, non approuvé ou non inspecté. |
| État de la chaîne (chain_status) | Si la chaîne est fiable. Les valeurs sont :<br>• Non inspectée<br>• Non approuvée<br>• Fiable<br>• Incomplet |
| Type de proxy (proxy_type) | Le type de proxy de décryptage, tel que Forward pour Proxy de transfert, Inbound pour Inspection entrante, No Decrypt pour trafic non décrypté, GlobalProtect, etc. |
| Numéro de série du certificat (cert_serial) | L'identifiant unique du certificat (généré par l'émetteur du certificat). |

| Nom du champ | Description |
|---|---|
| Empreinte du certificat (fingerprint) | Un hachage du certificat au format binaire x509. |
| Date de début du certificat (notbefore) | Le moment où le certificat est devenu valide (certificat non valide avant ce moment). |
| Date de fin du certificat (notafter) | Le moment où le certificat expire (le certificat devient invalide après ce moment). |
| Version du certificat (cert_ver) | La version du certificat (V1, V2 ou V3). |
| Taille du certificat (cert_size) | La taille de la clé du certificat. |
| Longueur de nom commun (cn_len) | La longueur du nom commun du sujet. |
| Longueur du nom commun de l'émetteur (issuer_len) | La longueur du nom commun de l'émetteur. |
| Longueur du nom commun de la racine (rootcn_len) | La longueur du nom commun de la racine. |
| Longueur SNI (sni_len) | La longueur de l'indication du nom du serveur (nom d'hôte). |
| Indicateurs de certificat (cert_flags) | Les indicateurs de certificat peuvent renvoyer sept valeurs :<br>• Session reprise (b_resume_session)<br>• Le nom commun de certificat (sujet) est tronqué (b_cert_cn_truncated)<br>• Le nom commun de l'émetteur est tronqué (b_issuer_cn_truncated)<br>• Le nom commun de la racine est tronqué (b_root_cn_truncated)<br>• L'identification du nom de serveur (SNI) est tronquée (b_sni_truncated)<br>• Type de certificat, RSA ou ECDSA (b_cert_type)<br>• Inutilisé (padding3) |
| Nom commun du sujet (cn) | Le nom de domaine (le nom du serveur que le certificat protège). |
| Nom commun de l'émetteur (issuer_cn) | Le nom de l'organisation qui a vérifié le contenu du certificat. |

| Nom du champ | Description |
|---|---|
| Nom commun de la racine (root_cn) | Le nom de l'autorité de certification racine. |
| Indication du nom de serveur (sni) | Le nom d'hôte du serveur que le client essaie de contacter. L'utilisation de SNI permet à un serveur d'héberger plusieurs sites web et de présenter plusieurs certificats sur la même adresse IP et le même port TCP car chaque site web possède un SNI unique. |
| Erreur (error) | Une chaîne indiquant l'erreur qui s'est produite dans l'événement. |
| ID de conteneur (container_id) | Une chaîne alphanumérique unique qui identifie le conteneur si le pare-feu fonctionne dans un conteneur en cloud. |
| Espace de noms de POD (pod_namespace) | Le nom de l'espace de noms de pod Kubernetes. |
| Nom de POD (pod_name) | Le nom de pod kubernetes. |
| Liste dynamique externe source (src_edl) | Le nom de la liste dynamique externe qui contient l'adresse IP source du trafic. |
| Liste dynamique externe de destination (dst_edl) | Le nom de la liste dynamique externe qui contient l'adresse IP de destination du trafic. |
| Groupe d'adresses dynamique source (src_dag) | Le groupe d'adresses dynamiques que le Device-ID identifie comme étant la source du trafic. |
| Groupe d'adresses dynamiques de destination (dst_dag) | Le groupe d'adresses dynamiques que le Device-ID identifie comme étant la destination du trafic. |
| Horodatage haute résolution (high_res_timestamp) | L'heure en milliseconde de réception du journal dans le plan de gestion.<br>Le format pour ce champ est YYYY-MM-DDThh:ss:sssTZD:<br>• **YYYY**—Année sur quatre chiffres<br>• **MM**—Mois sur deux chiffres<br>• **DD**—Jours du mois sur deux chiffres (01 à 31)<br>• **T**—Indicateur pour le début de l'horodatage<br>• **hh**—Heures sur deux chiffres utilisant le format 24 heures (00 à 23)<br>• **mm**—Minutes sur deux chiffres (00 à 59) |

| Nom du champ | Description |
|---|---|
| | • **ss**—Sondes sur deux chiffres (00 à 60)<br>• **sss**—Un ou plusieurs chiffres pour les millisecondes<br>• **TZD**—Indicateur de fuseau horaire (+hh:mm ou -hh:mm)<br><br>*L'horodatage haute résolution est pris en charge pour les journaux reçus des pare-feux gérés fonctionnant sous PAN-OS 10.1 et les versions ultérieures. Les journaux reçus de pare-feux gérés exécutant PAN-OS 9.1 et les versions antérieures affichent un horodatage `1969-12-31T16:00:00:000-8:00` quelle que soit la date à laquelle le journal a été reçu.* |
| Catégorie de périphérique source (src_category) | La catégorie du périphérique que Device-ID identifie comme étant la source du trafic. |
| Profil de périphérique source (src_profile) | Le profil du périphérique que Device-ID identifie comme étant la source du trafic. |
| Modèle de périphérique source (src_model) | Le modèle du périphérique que Device-ID identifie comme étant la source du trafic. |
| Fournisseur du périphérique source (src_vendor) | Le fournisseur du périphérique que Device-ID identifie comme étant la source du trafic. |
| Famille d'OS du périphérique source (src_osfamily) | Le type de système d'exploitation pour le périphérique que Device-ID identifie comme étant la source du trafic. |
| Version d'OS du périphérique source (src_osversion) | La version du système d'exploitation pour le périphérique que Device-ID identifie comme étant la source du trafic. |
| Nom d'hôte source (src_host) | Le nom d'hôte du périphérique que Device-ID identifie comme étant la source du trafic. |
| Adresse MAC source (src_mac) | L'adresse MAC du périphérique que Device-ID identifie comme étant la source du trafic. |
| Catégorie de périphérique de destination (dst_category) | La catégorie du périphérique que Device-ID identifie comme la destination du trafic. |

| Nom du champ | Description |
|---|---|
| Profil de périphérique de destination (dst_profile) | Le profil de périphérique pour le périphérique que Device-ID identifie comme la destination du trafic. |
| Modèle de périphérique de destination (dst_model) | Le modèle du périphérique que Device-ID identifie comme la destination du trafic. |
| Fournisseur du périphérique de destination (dst_vendor) | Le fournisseur du périphérique que Device-ID identifie comme la destination du trafic. |
| Famille de système d'exploitation du périphérique de destination (dst_osfamily) | Le type de système d'exploitation pour le périphérique que Device-ID identifie comme étant la destination du trafic. |
| Version de système d'exploitation du périphérique de destination (dst_osversion) | La version du système d'exploitation pour le périphérique que Device-ID identifie comme étant la destination du trafic. |
| Nom d'hôte de destination (dst_host) | Le nom d'hôte du périphérique que Device-ID identifie comme la destination du trafic. |
| Adresse MAC de destination (dst_mac) | L'adresse MAC du périphérique que Device-ID identifie comme la destination du trafic. |
| Numéro de séquence (seqno) | Identifiant d'entrée de journal 64 bits incrémenté de manière séquentielle ; chaque type de journal contient un espace de numéro unique. |
| Indicateurs d'action (actionflags) | Champ de bits indiquant si le journal a été transféré à Panorama. |
| Hiérarchie de groupes de périphériques (dg_hier_level_1 à dg_hier_level_4) | Une séquence de numéros d'identification qui indique l'emplacement du groupe de périphériques dans une hiérarchie de groupes de périphériques. Le pare-feu (ou système virtuel) générant le journal inclut le numéro d'identification de chaque ancêtre dans sa hiérarchie de groupes de périphériques. Le groupe de périphériques partagé (niveau 0) n'est pas inclus dans cette structure. |

| Nom du champ | Description |
|---|---|
| | Si les valeurs du journal sont 12, 34, 45, 0, cela signifie que le journal a été généré par un pare-feu (ou système virtuel) appartenant au groupe de périphériques 45, et que ses ancêtres sont 34 et 12. Pour afficher les noms des groupes de périphériques correspondant à la valeur 12, 34 ou 45, utilisez l'une des méthodes suivantes :<br>Requête d'API :<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| Nom du système virtuel (vsys_name) | Le nom du système virtuel associé à la session ; valide uniquement sur les pare-feu pouvant comporter plusieurs systèmes virtuels. |
| Nom du périphérique (device_name) | Le nom d'hôte du pare-feu sur lequel la session a été consignée. |
| ID du système virtuel (vsys_id) | Un identificateur unique pour un système virtuel sur un pare-feu Palo Alto Networks. |
| Sous-catégorie d'application (subcategory_of_app) | La sous-catégorie d'application spécifiée dans les propriétés de configuration de l'application. |
| Catégorie d'application (category_of_app) | Catégorie d'application spécifiée dans les propriétés de configuration de l'application. Les valeurs sont :<br>• systèmes professionnels<br>• collaboration<br>• Internet grand public<br>• multimédia<br>• Mise en réseau<br>• saas |
| Technologie d'application (technology_of_app) | La technologie d'application spécifiée dans les propriétés de configuration de l'application. Les valeurs sont :<br>• basé sur navigateur<br>• client/serveur<br>• protocole réseau<br>• poste à poste |
| Risque d'application (risk_of_app) | Niveau de risque associé à l'application (1=le plus faible à 5=le plus élevé). |

| Nom du champ | Description |
|---|---|
| Caractéristique de l'application (characteristic_of_app) | Liste séparée par des virgules des caractéristiques applicables de l'application |
| Conteneur d'applications (container_of_app) | L'application parent d'une application. |
| Application SaaS (is_saas_of_app) | Affiche `1` s'il s'agit d'une application SaaS ou `0` s'il ne s'agit pas d'une application SaaS. |
| État sanctionné de l'application (sanctioned_state_of_app) | Affiche `1` si la candidature est sanctionnée ou `0` si la candidature n'est pas sanctionnée. |

## Champs du journal d'inspection des tunnels

**Format** : FUTURE_USE, Heure de réception, Numéro de série, Type, Sous-type, FUTURE_USE, Heure de génération, Adresse source, Adresse de destination, Adresse IP source NAT, Adresse IP de destination NAT, Nom de la règle, Utilisateur source, Utilisateur de destination, Application, Système virtuel, Zone source, Zone de destination, Interface d'entrée, Interface de sortie, Journal des actions, FUTURE_USE, ID de session, Nombre de répétitions, Port source, Port de destination, Port source NAT, Port de destination NAT, Indicateurs, Protocole, Action, Gravité, Indicateurs d'action, Emplacement source, Emplacement de destination, Hiérarchie de groupes de périphériques niveau 1, Hiérarchie de groupes de périphériques niveau 2, Hiérarchie de groupes de périphériques niveau 3, Hiérarchie de groupes de périphériques niveau 4, Nom du système virtuel, Nom du périphérique, ID/IMSI tunnel, Tag/IMEI surveillance, ID session parent, Heure de début du parent, Type de tunnel, Octets, Octets envoyés, Octets reçus, Paquets, Paquets envoyés, Paquets reçus, Encapsulation maximale, Protocole inconnu, Contrôle strict, Fragment de tunnel, Sessions créées, Sessions fermées, Motif de fin de session, Source d'action, Heure de début, Temps écoulé, Règle d'inspection des tunnels, IP de l'utilisateur distant, ID d'utilisateur distant, UUID de la règle, ID PCAP, Groupe d'utilisateurs dynamiques, Liste dynamique externe source, Liste dynamique externe de destination, Horodatage haute résolution, Différentiateur de tranche A,Type de service de tranche A, ID de session PDU, Sous-catégorie de l'application, Catégorie de l'application, Technologie de l'application, risque lié à l'application, Caractéristique de l'application, Conteneur de l'application, Saas de l'application, Etat sanctionné de l'application

| Nom du champ | Description |
|---|---|
| Heure de réception (receive_time ou cef-formatted-receive_time) | Mois, jour et heure de réception du journal dans le plan de gestion. |
| Numéro de série (serial) | Numéro de série du pare-feu ayant généré le journal. |

| Nom du champ | Description |
|---|---|
| Type (type) | Type de journal pour la session : START ou END. |
| Menace / Type de contenu (sous-type) | Sous-type du journal du trafic ; les valeurs possibles sont start, end, drop et deny<br>• Start — session ouverte<br>• End — session fermée<br>• Drop — session arrêtée avant l'identification de l'application et absence de règle autorisant la session.<br>• Deny — session arrêtée après l'identification de l'application et présence d'une règle de blocage ou absence de règle autorisant la session. |
| Heure de génération (time_generated ou cef-formatted-time_generated) | Heure de génération du journal dans le plan de données. |
| Adresse source (src) | L'adresse IP source des paquets de la session. |
| Adresse de destination (dst) | L'adresse IP de destination des paquets de la session. |
| Adresse IP source NAT (natsrc) | En cas de NAT source, il s'agit de l'adresse IP source post-NAT. |
| IP de destination NAT (natdst) | En cas de NAT de destination, il s'agit de l'adresse IP de destination post-NAT. |
| Nom de la règle (rule) | Le nom de la règle de politique de sécurité en vigueur sur la session. |
| Utilisateur source (srcuser) | L'ID utilisateur source des paquets de la session. |
| Utilisateur de destination (dstuser) | L'ID utilisateur de destination des paquets de la session. |
| Application (app) | Le protocole de mise en tunnel utilisé dans la session. |
| Système virtuel (vsys) | Système virtuel associé à la session. |
| Zone source (from) | La zone source des paquets de la session. |
| Zone de destination (to) | La zone de destination des paquets de la session. |

| Nom du champ | Description |
|---|---|
| Interface entrante (inbound_if) | Interface d'origine de la session. |
| Interface sortante (outbound_if) | Interface à laquelle la session est destinée. |
| Action du journal (logset) | Profil de transfert des journaux appliqué à la session. |
| ID de session (sessionid) | L'ID de session de la session journalisée. |
| Nombre de répétitions (repeatcnt) | Nombre de sessions avec les mêmes adresses IP source et de destination, application et sous-type constatées sur une période de 5 secondes. |
| Port source (sport) | Port source utilisé par la session. |
| Port de destination (dport) | Port de destination utilisé par la session. |
| Port source NAT (natsport) | Port source post-NAT. |
| Port de destination NAT (natdport) | Port de destination post-NAT. |
| Indicateurs (flags) | Champ 32 bits qui fournit des détails sur la session ; ce champ peut être décodé en ajoutant (opérateur AND) les valeurs à la valeur consignée :<br>• 0x80000000 : la session inclut la capture de paquets (PCAP)<br>• 0x02000000 : session IPv6<br>• 0x01000000 : la session SSL a été décryptée (proxy SSL)<br>• 0x00800000 : la session a été refusée via le filtrage des URL<br>• 0x00400000 : la session a exécuté une traduction NAT (NAT)<br>• 0x00200000 : les informations sur l'utilisateur de la session ont été capturées via le portail d'authentification<br>• 0x00080000 : la valeur X-Forwarded-For d'un proxy est contenue dans le champ de l'utilisateur source<br>• 0x00040000 : le journal correspond à une transaction d'une session de proxy http (Proxy Transaction)<br>• 0x00008000 : la session permet d'accéder à une page de conteneur (Container Page) |

| Nom du champ | Description |
|---|---|
| | • 0x00002000 : la session inclut une correspondance temporaire d'une règle pour le traitement implicite des dépendances d'application. Disponible dans PAN-OS 5.0.0 et versions ultérieures.<br>• 0x00000800 : un retour symétrique a été utilisé pour transférer le trafic de cette session |
| Protocole IP (proto) | Protocole IP associé à la session. |
| Action (action) | Action prise pour la session. Les valeurs possibles sont :<br>• Allow — la session a été autorisée par la politique<br>• Deny — la session a été refusée par la politique<br>• Drop — la session a été abandonnée à l'arrière-plan<br>• Drop ICMP — la session a été abandonnée à l'arrière-plan avec un message ICMP inaccessible vers l'hôte ou l'application<br>• Reset both — la session a été terminée et une réinitialisation TCP est envoyée aux deux côtés de la connexion<br>• Reset client — la session a été terminée et une réinitialisation TCP est envoyée au client<br>• Reset server — la session a été terminée et une réinitialisation TCP est envoyée au serveur |
| Gravité (severity) | Gravité associée à l'événement ; les valeurs possibles sont informational, low, medium, high, critical. |
| Numéro de séquence (seqno) | Identifiant d'entrée de journal 64 bits incrémenté de manière séquentielle ; chaque type de journal contient un espace de numéro unique. Ce champ n'est pas pris en charge sur les pare-feu PA-7000 Series. |
| Indicateurs d'action (actionflags) | Champ de bits indiquant si le journal a été transféré à Panorama. |
| Emplacement source (srcloc) | Pays ou région source pour les adresses privées ; 32 octets maximum. |
| Emplacement de destination (dstloc) | Pays ou région de destination pour les adresses privées. 32 octets maximum. |
| Hiérarchie de groupes de périphériques (dg_hier_level_1 à dg_hier_level_4) | Une séquence de numéros d'identification qui indique l'emplacement du groupe de périphériques dans une hiérarchie de groupes de périphériques. Le pare-feu (ou système virtuel) générant le journal inclut le numéro d'identification de chaque ancêtre dans sa hiérarchie de groupes de périphériques. Le groupe de périphériques partagé (niveau 0) n'est pas inclus dans cette structure. |

| Nom du champ | Description |
|---|---|
| | Si les valeurs du journal sont 12, 34, 45, 0, cela signifie que le journal a été généré par un pare-feu (ou système virtuel) appartenant au groupe de périphériques 45, et que ses ancêtres sont 34 et 12. Pour afficher les noms des groupes de périphériques correspondant à la valeur 12, 34 ou 45, utilisez l'une des méthodes suivantes :<br>Requête d'API :<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| Nom du système virtuel (vsys_name) | Le nom du système virtuel associé à la session ; valide uniquement sur les pare-feu pouvant comporter plusieurs systèmes virtuels. |
| Nom du périphérique (device_name) | Le nom d'hôte du pare-feu sur lequel la session a été consignée. |
| ID de tunnel (tunnelid) | L'ID du tunnel inspecté ou International Mobile Subscriber Identity (Identité d'abonné mobile international ; IMSI) ID de l'utilisateur mobile. |
| Balise de surveillance (monitortag) | Le nom de surveillance que vous avez configuré pour la règle de politique d'inspection des tunnels ou l'International Mobile Equipement Identity (Identité d'appareil abonné international ; IMEI) ID de l'appareil mobile. |
| ID de session parent (parent_session_id) | L'ID de la session mise en tunnel. Il s'applique au tunnel interne (s'il y a deux niveaux de tunnellisation) ou au contenu interne (s'il n'y a qu'un seul niveau de tunnellisation) uniquement. |
| Heure de début parent (parent_start_time) | Années/mois/jours heures:minutes:secondes depuis le début de la session de tunnel parent. |
| Type de tunnel (tunnel) | Type de tunnel, par exemple GRE ou IPsec. |
| Octets (bytes) | Le nombre d'octets dans la session. |
| Octets envoyés (bytes_sent) | Nombre d'octets dans le sens client/serveur de la session. |
| Octets reçus (bytes_received) | Nombre d'octets dans le sens serveur/client de la session. |
| Paquets (packets) | Nombre total de paquets (émission et réception) de la session. |

| Nom du champ | Description |
|---|---|
| Paquets envoyés (pkts_sent) | Nombre de paquets client/serveur de la session. |
| Paquets reçus (pkts_received) | Nombre de paquets serveur/client de la session. |
| Encapsulation maximale (max_encap) | Le nombre de paquets que le pare-feu a abandonnés, car ces paquets dépassaient le nombre maximum de niveaux d'encapsulation configuré dans la règle de politique d'inspection des tunnels (Abandonner les paquets au-delà du niveau d'inspection des tunnels maximum). |
| Protocole inconnu (unknown_proto) | Le nombre de paquets que le pare-feu a abandonnés, car ces paquets contenaient un protocole inconnu, comme indiqué dans la règle de politique d'inspection des tunnels (Abandonner les paquets si le protocole est inconnu dans le tunnel). |
| Vérification stricte (strict_check) | Le nombre de paquets que le pare-feu a abandonnés, car l'en-tête de protocole de tunnel dans le paquet n'était pas conforme au RFC pour le protocole de tunnel, comme indiqué dans la règle de politique d'inspection des tunnels (**Drop packet if tunnel protocol fails strict header check (Abandonner les paquets si le protocole ne passe pas le contrôle d'en-tête strict)**). |
| Fragmentation de tunnel (tunnel_fragment) | Le nombre de paquets que le pare-feu a abandonnés en raison d'erreurs de fragmentation. |
| Sessions créées (sessions_created) | Nombre de sessions intérieures créées. |
| Sessions fermées (sessions_closed) | Nombre de sessions intérieures terminées/fermées. |
| Motif de fin de session (session_end_reason) | Le motif pour lequel une session s'est terminée. S'il existe plusieurs motifs, ce champ affiche uniquement le motif principal (celui dont la priorité est la plus élevée). Les valeurs de motif de fin de session possibles sont les suivantes, par ordre de priorité (où la première est la plus élevée) :<br>• threat : le pare-feu a détecté une menace associée à une action de réinitialisation, d'abandon ou de blocage (d'adresse IP).<br>• policy-deny : la session a été mise en correspondance avec une règle de sécurité dont l'action est le refus ou l'abandon.<br>• Decrypt-cert-validation : la session s'est terminée parce que vous avez configuré le pare-feu pour qu'il bloque le décryptage du proxy de transfert SSL ou l'inspection SSL entrante lorsque la session utilise l'authentification du client ou qu'elle utilise un certificat du serveur |

| Nom du champ | Description |
| --- | --- |
| | ayant l'une ou l'autre des conditions suivantes : expiré, émetteur non approuvé, état inconnu ou expiration de la vérification de l'état. Le motif de fin de session s'affiche également lorsque le certificat du serveur produit une alerte d'erreur fatale de type bad_certificate (mauvais certificat), unsupported_certificate (certificat non pris en charge), certificate_revoked (certificat révoqué), access_denied (accès refusé), ou no_certificate_RESERVED (aucun certificat réservé) (uniquement SSLv3).<br>• decrypt-unsupport-param : la session s'est terminée parce que vous avez configuré le pare-feu pour qu'il bloque le décryptage du proxy de transfert SSL ou l'inspection SSL entrante lorsque la session utilise une version de protocole, un cryptage ou un algorithme non pris en charge. Le motif de fin de session s'affiche lorsque la session produit une alerte d'erreur fatale du type unsupported_extension (extension non prise en charge), unexpected_message (message inattendu), ou handshake_failure (échec de la liaison de segmentation).<br>• decrypt-unsupport-param : la session s'est terminée, car vous avez configuré le pare-feu pour qu'il bloque le décryptage du proxy de transfert SSL ou l'inspection SSL entrante lorsque des ressources sur le pare-feu ou le hardware security module (module de sécurité matériel ; HSM) étaient indisponibles. Le motif de fin de session s'affiche lorsque vous configurez le pare-feu pour qu'il bloque le trafic SSL ayant des erreurs SSH ou qui a produit une alerte d'erreur fatale autre que celles énumérées sous les motifs de fin de session decrypt-cert-validation et decrypt-unsupport-param.<br>• tcp-rst-from-client : le client a envoyé une demande de réinitialisation TCP au serveur.<br>• tcp-rst-from-server : le serveur a envoyé une demande de réinitialisation TCP au client.<br>• resources-unavailable : la session a été abandonnée en raison d'une limitation des ressources système. Par exemple, il se peut que la session ait dépassé le nombre de paquets dans le désordre autorisés par flux ou la file d'attente générale des paquets dans le désordre.<br>• tcp-fin : un seul hôte ou les deux hôtes d'une connexion a/ont envoyé un message TCP FIN pour fermer la session.<br>• tcp-reuse : une session a été réutilisée et le pare-feu a fermé la session précédente.<br>• decoder : le décodeur a détecté une nouvelle connexion via le protocole (proxy HTTP, par exemple) et a fermé la connexion précédente.<br>• aged-out : la session a expiré. |

| Nom du champ | Description |
|---|---|
| | • unknown : cette valeur s'applique aux situations suivantes :<br>  • Les fins de sessions non couvertes par les motifs précédents (par exemple, une commande **`clear session all`**).<br>  • Pour les journaux générés dans une version PAN-OS qui ne prend pas en charge le champ Motif de fin de session (versions ultérieures à PAN-OS 6.1), la valeur est **`unknown`** après une mise à niveau vers la version PAN-OS actuelle ou le chargement des journaux sur le pare-feu.<br>  • Dans Panorama, les journaux reçus des pare-feu pour lesquels la version PAN-OS ne prend pas en charge les motifs de fin de session ont la valeur **`unknown`**.<br>• n/a : cette valeur s'applique lorsque le type de journal du trafic n'est pas **`end`**. |
| Source d'action (action_source) | Indique si l'action prise pour autoriser ou bloquer une application a été définie dans l'application ou dans une politique. Les actions peuvent être allow, deny, drop, reset- server, reset-client ou reset-both pour la session. |
| Heure de début (start) | Années/mois/jours heures:minutes:secondes depuis le début de la session. |
| Temps écoulé (elapsed) | Durée écoulée de la session. |
| Règle d'inspection des tunnels (tunnel_insp_rule) | Nom de la règle d'inspection des tunnels associée au trafic de tunnel de texte en clair. |
| IP de l'utilisateur distant (remote_user_ip) | Adresse IPv4 ou IPv6 d'un utilisateur distant. |
| ID de l'utilisateur distant (remote_user_id) | Identité IMSI d'un utilisateur distant et, si disponible, une identité IMEI ou une identité MSISDN. |
| UUID de la règle de la sécurité (rule_uuid) | L'UUID qui identifie la règle de manière permanente. |
| ID pcap (pcap_id) | ID de capture de paquets unique qui définit l'emplacement du fichier pcap sur le pare-feu. |
| Nom de groupe des utilisateurs | Le nom du groupe d'utilisateurs dynamiques qui contient l'utilisateur qui a initié la session. |

| Nom du champ | Description |
|---|---|
| dynamiques (dynusergroup_name) | |
| Liste dynamique externe source (src_edl) | Le nom de la liste dynamique externe qui contient l'adresse IP source du trafic. |
| Liste dynamique externe de destination (dst_edl) | Le nom de la liste dynamique externe qui contient l'adresse IP de destination du trafic. |
| Horodatage haute résolution (high_res_timestamp) | L'heure en milliseconde de réception du journal dans le plan de gestion.<br>Le format pour ce nouveau champ est YYYY-MM-DDThh:ss:sssTZD:<br>• **YYYY**—Année sur quatre chiffres<br>• **MM**—Mois sur deux chiffres<br>• **DD**—Jours du mois sur deux chiffres (01 à 31)<br>• **T**—Indicateur pour le début de l'horodatage<br>• **hh**—Heures sur deux chiffres utilisant le format 24 heures (00 à 23)<br>• **mm**—Minutes sur deux chiffres (00 à 59)<br>• **ss**—Sondes sur deux chiffres (00 à 60)<br>• **sss**—Un ou plusieurs chiffres pour les millisecondes<br>• **TZD**—Indicateur de fuseau horaire (+hh:mm ou -hh:mm)<br>*L'horodatage haute résolution est pris en charge pour les journaux reçus des pare-feux gérés fonctionnant sous PAN-OS 10.1 et les versions ultérieures. Les journaux reçus de pare-feux gérés exécutant PAN-OS 9.1 et les versions antérieures affichent un horodatage `1969-12-31T16:00:00:000-8:00` quelle que soit la date à laquelle le journal a été reçu.* |
| Différenciateur de tranche A (nssai_sd) | Le différenciateur de tranche A de l'ID de tranche de réseau. |
| Un type de service de tranche A (nssai_sd) | Le type de service de tranche A de l'ID de tranche de réseau. |
| ID de session PDU (pdu_session_id) | ID de session pour la collecte de segments L4 à l'intérieur d'un tunnel. |

| Nom du champ | Description |
|---|---|
| Sous-catégorie d'application (subcategory_of_app) | La sous-catégorie d'application spécifiée dans les propriétés de configuration de l'application. |
| Catégorie d'application (category_of_app) | Catégorie d'application spécifiée dans les propriétés de configuration de l'application. Les valeurs sont :<br>• systèmes professionnels<br>• collaboration<br>• Internet grand public<br>• multimédia<br>• Mise en réseau<br>• saas |
| Technologie d'application (technology_of_app) | La technologie d'application spécifiée dans les propriétés de configuration de l'application. Les valeurs sont :<br>• basé sur navigateur<br>• client/serveur<br>• protocole réseau<br>• poste à poste |
| Risque d'application (risk_of_app) | Niveau de risque associé à l'application (1=le plus faible à 5=le plus élevé). |
| Caractéristique de l'application (characteristic_of_app) | Liste séparée par des virgules des caractéristiques applicables de l'application |
| Conteneur d'applications (container_of_app) | L'application parent d'une application. |
| Application SaaS (is_saas_of_app) | Affiche **1** s'il s'agit d'une application SaaS ou **0** s'il ne s'agit pas d'une application SaaS. |
| État sanctionné de l'application (sanctioned_state_of_app) | Affiche **1** si la candidature est sanctionnée ou **0** si la candidature n'est pas sanctionnée. |
| Sous-catégorie d'application (subcategory_of_app) | La sous-catégorie d'application spécifiée dans les propriétés de configuration de l'application. |

## Champs des journaux SCTP

**Format :** FUTURE_USE, Heure de réception, Numéro de série, Type, FUTURE_USE, FUTURE_USE, Heure de génération, Adresse source, Adresse de destination, FUTURE_USE, FUTURE_USE, Nom de la règle, FUTURE_USE, FUTURE_USE, FUTURE_USE, Système virtuel, Zone source, Zone de destination, Interface d'entrée, Interface de sortie, Action des journaux, FUTURE_USE, ID de session, Nombre de répétitions, Port source, Port de destination, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, Protocole IP, Action, Hiérarchie de groupes de périphériques niveau 1, Hiérarchie de groupes de périphériques niveau 2, Hiérarchie de groupes de périphériques niveau 3, Hiérarchie de groupes de périphériques niveau 4, Nom du système virtuel, Nom du périphérique, Numéro de séquence, FUTURE_USE, ID d'association SCTP, ID de protocole de charge utile, Gravité, Type de blocs SCTP, FUTURE_USE, Étiquette de vérification SCTP 1, Étiquette de vérification SCTP 2, Code de cause SCTP, ID d'application Diameter, Code de commande Diameter, Code AVP Diameter, ID du flux SCTP, Motif de fin de l'association SCTP, Code Op, SSN du demandeur du sous-système de commande de connexions sémaphores, Appellation globale du demandeur du sous-système de commande de connexions sémaphores, Filtre SCTP, Blocs SCTP, Blocs SCTP envoyés, Blocs SCTP reçus, Paquets, Paquets envoyés, Paquets reçus, UUID pour la règle, Horodatage haute résolution

| Nom du champ | Description |
|---|---|
| Heure de réception (receive_time ou cef-formatted-receive_time) | Heure de réception du journal dans le panneau de gestion. |
| Numéro de série (serial) | Numéro de série du pare-feu ayant généré le journal. |
| Type (type) | Spécifie le type de journal ; la valeur est SCTP. |
| Heure de génération (time_generated ou cef-formatted-time_generated) | Heure de génération du journal dans le plan de données. |
| Adresse source (src) | Adresse IP source de la session d'origine. |
| Adresse de destination (dst) | Adresse IP de destination de la session d'origine. |
| Nom de la règle (rule) | Le nom de la règle de politique de sécurité en vigueur sur la session. |
| Système virtuel (vsys) | Système virtuel associé à la session. |
| Zone source (from) | Zone d'origine de la session. |
| Zone de destination (to) | Zone à laquelle la session est destinée. |
| Interface entrante (inbound_if) | Interface d'origine de la session. |

| Nom du champ | Description |
|---|---|
| Interface sortante (outbound_if) | Interface à laquelle la session est destinée. |
| Action du journal (logset) | Profil de transfert des journaux appliqué à la session. |
| ID de session (sessionid) | Identificateur numérique interne appliqué à chaque session. |
| Nombre de répétitions (repeatcnt) | Nombre de sessions avec les mêmes adresses IP source et de destination, application et sous-type constatées sur une période de 5 secondes. |
| Port source (sport) | Port source utilisé par la session. |
| Port de destination (dport) | Port de destination utilisé par la session. |
| Protocole IP (proto) | Protocole IP associé à la session. |
| Action (action) | Action prise pour la session. Les valeurs possibles sont :<br>• allow — la session a été autorisée par la politique<br>• deny — la session a été refusée par la politique |
| Hiérarchie de groupes de périphériques (dg_hier_level_1 à dg_hier_level_4) | Une séquence de numéros d'identification qui indique l'emplacement du groupe de périphériques dans une hiérarchie de groupes de périphériques. Le pare-feu (ou système virtuel) générant le journal inclut le numéro d'identification de chaque ancêtre dans sa hiérarchie de groupes de périphériques. Le groupe de périphériques partagé (niveau 0) n'est pas inclus dans cette structure.<br>Si les valeurs du journal sont 12, 34, 45, 0, cela signifie que le journal a été généré par un pare-feu (ou système virtuel) appartenant au groupe de périphériques 45, et que ses ancêtres sont 34 et 12. Pour afficher les noms des groupes de périphériques correspondant à la valeur 12, 34 ou 45, utilisez l'une des méthodes suivantes :<br>Requête d'API :<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| Nom du système virtuel (vsys_name) | Le nom du système virtuel associé à la session ; valide uniquement sur les pare-feu pouvant comporter plusieurs systèmes virtuels. |

| Nom du champ | Description |
|---|---|
| Nom du périphérique (device_name) | Le nom d'hôte du pare-feu sur lequel la session a été consignée. |
| Numéro de séquence (seqno) | Identifiant d'entrée de journal 64 bits incrémenté de manière séquentielle ; chaque type de journal contient un espace de numéro unique. |
| ID d'association SCTP (assoc_id) | Un identifiant logique numérique interne de 56 bits appliqué à chaque association SCTP. |
| ID de protocole de charge utile (ppid) | Identifie le Payload Protocol ID (ID de protocole de charge utile ; PPID) dans le bloc de données qui a déclenché cet événement. Le PPID est attribué par la Internet Assigned Numbers Authority (IANA). |
| Gravité (severity) | Gravité associée à l'événement ; les valeurs possibles sont informational, low, medium, high, critical. |
| Type de blocs SCTP (sctp_chunk_type) | Décrit le type d'informations contenues dans un bloc, comme le contrôle ou les données. |
| Type d'événement SCTP (sctp_event_type) | Définit l'événement déclenché par un paquet ou un bloc SCTP lorsque le profil de protection SCTP est appliqué au trafic SCTP. Il est également déclenché par le début ou la fin d'une association SCTP. |
| Étiquette de vérification SCTP 1 (verif_tag_1) | Utilisée par le point de terminaison 1 qui initie l'association pour vérifier si le paquet SCTP reçu appartient à l'association SCTP actuelle et pour valider le point de terminaison 2. |
| Étiquette de vérification SCTP 2 (verif_tag_2) | Utilisée par le point de terminaison 2 pour vérifier si le paquet SCTP reçu appartient à l'association SCTP actuelle et pour valider le point de terminaison 1. |
| Code de cause SCTP (sctp_cause_code) | Envoyé par un point de terminaison pour préciser la raison d'une condition d'erreur à un autre point de terminaison de la même association SCTP. |
| ID d'application Diameter (diam_app_id) | L'application Diameter du bloc de données qui a déclenché l'événement. L'ID d'application Diameter est attribué par la Internet Assigned Numbers Authority (IANA). |
| Code de commande Diameter (diam_cmd_code) | Le code de commande Diameter du bloc de données qui a déclenché l'événement. Le Code de commande Diameter est attribué par la Internet Assigned Numbers Authority (IANA). |

| Nom du champ | Description |
|---|---|
| Code AVP Diameter (diam_avp_code) | Le code AVP Diameter du bloc de données qui a déclenché l'événement. |
| ID du flux SCTP (stream_id) | ID du flux qui transporte le bloc de données qui a déclenché l'événement. |
| Motif de fin de l'association SCTP (assoc_end_reason) | La raison pour laquelle une association a pris fin. Si l'arrêt comporte plusieurs causes, celle qui possède la priorité la plus élevée s'affiche. Les raisons éventuelles pouvant expliquer la fin de la session en ordre descendant de priorité sont :<br>• shutdown-from-endpoint (highest) (arrêt depuis le point de terminaison (la plus élevée) : le point de terminaison envoie **SHUTDOWN**<br>• Abort-from-endpoint (interruption depuis le point de terminaison) : le point de terminaison envoie **ABORT**<br>• unknown (lowest) (inconnue (la plus faible) : l'association a expiré ou la raison de fin de l'association n'est pas couverte par l'un des motifs précédents (par exemple, une commande clear session all). |
| Code d'opération (op_code) | Identifie le code d'opération des protocoles de couche SS7, comme MAP ou CAP, dans le bloc de données qui a déclenché l'événement. |
| SSN du demandeur du sous-système de commande de connexions sémaphores (sccp_calling_ssn) | Le Subsystem Number (numéro du sous-système ; SSN) du demandeur Signalling Connection Control Part (SCCP) dans le bloc de données qui a déclenché l'événement. |
| Appellation globale du demandeur du sous-système de commande de connexions sémaphores (sccp_calling_gt) | L'appellation globale du demandeur Signalling Connection Control Part (SCCP) dans le bloc de données qui a déclenché l'événement. |
| Filtre SCTP (sctp_filter) | Nom du filtre auquel le bloc SCTP correspond. |
| Blocs SCTP (chunks) | Nombre total de blocs (émission et réception) de l'association. |
| Blocs SCTP envoyés (chunks_sent) | Nombre de blocs point de terminaison 1 (qui a lancé l'association)-point de terminaison 2 de l'association. |
| Blocs SCTP reçus (chunks_received) | Nombre de blocs point de terminaison 2 (qui a lancé l'association)-point de terminaison 1 de l'association. |
| Paquets (packets) | Nombre total de paquets (émission et réception) de la session. |

| Nom du champ | Description |
|---|---|
| Paquets envoyés (pkts_sent) | Nombre de paquets client/serveur de la session. |
| Paquets reçus (pkts_received) | Nombre de paquets serveur/client de la session. |
| UUID pour la règle (rule_uuid) | L'UUID qui identifie la règle de manière permanente. |
| Horodatage haute résolution (high_res_timestamp) | L'heure en milliseconde de réception du journal dans le plan de gestion.<br>Le format pour ce nouveau champ est YYYY-MM-DDThh:ss:sssTZD:<br>• **YYYY**—Année sur quatre chiffres<br>• **MM**—Mois sur deux chiffres<br>• **DD**—Jours du mois sur deux chiffres (01 à 31)<br>• **T**—Indicateur pour le début de l'horodatage<br>• **hh**—Heures sur deux chiffres utilisant le format 24 heures (00 à 23)<br>• **mm**—Minutes sur deux chiffres (00 à 59)<br>• **ss**—Sondes sur deux chiffres (00 à 60)<br>• **sss**—Un ou plusieurs chiffres pour les millisecondes<br>• **TZD**—Indicateur de fuseau horaire (+hh:mm ou -hh:mm)<br>*L'horodatage haute résolution est pris en charge pour les journaux reçus des pare-feux gérés fonctionnant sous PAN-OS 10.1 et les versions ultérieures. Les journaux reçus de pare-feux gérés exécutant PAN-OS 9.1 et les versions antérieures affichent un horodatage `1969-12-31T16:00:00:000-8:00` quelle que soit la date à laquelle le journal a été reçu.* |

## Champs des journaux d'authentification

**Format :** FUTURE_USE, Heure de réception, Numéro de série, Type, Type de menace/contenu, FUTURE_USE, Heure de génération, Système virtuel, IP source, Utilisateur, Normaliser l'utilisateur, Objet, Politique d'authentification, Nombre de répétitions, ID d'authentification, Fournisseur, Consigner l'action, Profil de serveur, Description, Type de client, Type d'événement, Nombre de facteurs, Nombre de séquences, Indicateurs d'action, Hiérarchie de groupes de périphériques niveau 1, Hiérarchie de groupes de périphériques niveau 2, Hiérarchie de groupes de périphériques niveau 3, Hiérarchie de groupes de périphériques niveau 4, Nom du système virtuel, Nom du périphérique, ID du système virtuel, Protocole d'authentification, UUID pour la règle, Horodatage haute résolution, Catégorie de périphérique source, Profil de périphérique source, Modèle de périphérique source, Fournisseur de périphérique source, Famille d'OS de périphérique

source, Version d'OS de périphérique source, Nom d'hôte source, Adresse Mac source, Région, FUTURE_USE, Agent utilisateur, ID de session

| Nom du champ | Description |
|---|---|
| Heure de réception (receive_time ou cef-formatted-receive_time) | Heure de réception du journal dans le panneau de gestion. |
| Numéro de série (serial) | Numéro de série du périphérique ayant généré le journal. |
| Type (type) | Spécifie le type de journal ; la valeur est AUTHENTICATION. |
| Menace / Type de contenu (sous-type) | Sous-type du journal système ; fait référence au démon système générant le journal. Les valeurs possibles sont crypto, dhcp, dnsproxy, dos, general, global-protect, ha, hw, nat, ntpd, pbf, port, pppoe, ras, routing, satd, sslmgr, sslvpn, userid, url-filtering, vpn. |
| Heure de génération (time_generated ou cef-formatted-time_generated) | Heure de génération du journal dans le plan de données. |
| Système virtuel (vsys) | Système virtuel associé à la session. |
| IP source (ip) | Adresse IP source de la session d'origine. |
| Utilisateur (user) | Utilisateur final faisant l'objet de l'authentification. |
| Normaliser l'utilisateur (normalize_user) | Version normalisée du nom d'utilisateur faisant l'objet de l'authentification (par exemple, ajout d'un nom de domaine au nom d'utilisateur). |
| Objet (object) | Nom de l'objet associé à l'événement système. |
| Politique d'authentification (authpolicy) | Politique appelée aux fins d'authentification avant d'autoriser l'accès à une ressource protégée. |
| Nombre de répétitions (repeatcnt) | Nombre de sessions avec les mêmes adresses IP source et de destination, application et sous-type constatées sur une période de 5 secondes. |
| ID d'authentification (authid) | ID unique octroyé lors de l'authentification principale et de toute authentification supplémentaire (multifacteur). |

| Nom du champ | Description |
|---|---|
| Fournisseur (vendor) | Fournisseur procurant les facteurs d'authentification additionnels. |
| Action du journal (logset) | Profil de transfert des journaux appliqué à la session. |
| Profil de serveur (serverprofile) | Serveur d'authentification utilisé aux fins de l'authentification. |
| Description (desc) | Informations d'authentification supplémentaires. |
| Type de client (clienttype) | Type de client utilisé pour effectuer l'authentification (comme le portail d'authentification). |
| Type d'événement (event) | Résultat de la tentative d'authentification. |
| Nombre de facteurs (factorno) | Indique l'utilisation de l'authentification principale (1) ou de facteurs supplémentaires (2, 3). |
| Numéro de séquence (seqno) | Identifiant d'entrée de journal 64 bits incrémenté de manière séquentielle. Chaque type de journal dispose d'un espace de numéros unique. |
| Indicateurs d'action (actionflags) | Champ de bits indiquant si le journal a été transféré à Panorama. |
| Hiérarchie de groupes de périphériques (dg_hier_level_1 à dg_hier_level_4) | Une séquence de numéros d'identification qui indique l'emplacement du groupe de périphériques dans une hiérarchie de groupes de périphériques. Le pare-feu (ou système virtuel) générant le journal inclut le numéro d'identification de chaque ancêtre dans sa hiérarchie de groupes de périphériques. Le groupe de périphériques partagé (niveau 0) n'est pas inclus dans cette structure.<br>Si les valeurs du journal sont 12, 34, 45, 0, cela signifie que le journal a été généré par un pare-feu (ou système virtuel) appartenant au groupe de périphériques 45, et que ses ancêtres sont 34 et 12. Pour afficher les noms des groupes de périphériques correspondant à la valeur 12, 34 ou 45, utilisez l'une des méthodes suivantes :<br>Requête d'API :<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| Nom du système virtuel (vsys_name) | Le nom du système virtuel associé à la session ; valide uniquement sur les pare-feu pouvant comporter plusieurs systèmes virtuels. |

| Nom du champ | Description |
|---|---|
| Nom du périphérique (device_name) | Le nom d'hôte du pare-feu sur lequel la session a été consignée. |
| ID du système virtuel (vsys_id) | Un identificateur unique pour un système virtuel sur un pare-feu Palo Alto Networks. |
| Protocole d'authentification (authproto) | Indique le protocole d'authentification utilisé par le serveur. Par exemple, PEAP avec GTC. |
| UUID pour la règle (rule_uuid) | L'UUID qui identifie la règle de manière permanente. |
| Horodatage haute résolution (high_res _timestamp) | L'heure en milliseconde de réception du journal dans le plan de gestion.<br>Le format pour ce nouveau champ est YYYY-MM-DDThh:ss:sssTZD:<br>• **YYYY**—Année sur quatre chiffres<br>• **MM**—Mois sur deux chiffres<br>• **DD**—Jours du mois sur deux chiffres (01 à 31)<br>• **T**—Indicateur pour le début de l'horodatage<br>• **hh**—Heures sur deux chiffres utilisant le format 24 heures (00 à 23)<br>• **mm**—Minutes sur deux chiffres (00 à 59)<br>• **ss**—Sondes sur deux chiffres (00 à 60)<br>• **sss**—Un ou plusieurs chiffres pour les millisecondes<br>• **TZD**—Indicateur de fuseau horaire (+hh:mm ou -hh:mm)<br>*L'horodatage haute résolution est pris en charge pour les journaux reçus des pare-feux gérés fonctionnant sous PAN-OS 10.1 et les versions ultérieures. Les journaux reçus de pare-feux gérés exécutant PAN-OS 9.1 et les versions antérieures affichent un horodatage `1969-12-31T16:00:00:000-8:00` quelle que soit la date à laquelle le journal a été reçu.* |
| Catégorie de périphérique source (src_category) | La catégorie du périphérique que Device-ID identifie comme étant la source du trafic. |
| Profil de périphérique source (src_profile) | Le profil du périphérique que Device-ID identifie comme étant la source du trafic. |

| Nom du champ | Description |
|---|---|
| Modèle de périphérique source (src_model) | Le modèle du périphérique que Device-ID identifie comme étant la source du trafic. |
| Fournisseur du périphérique source (src_vendor) | Le fournisseur du périphérique que Device-ID identifie comme étant la source du trafic. |
| Famille d'OS du périphérique source (src_osfamily) | Le type de système d'exploitation pour le périphérique que Device-ID identifie comme étant la source du trafic. |
| Version d'OS du périphérique source (src_osversion) | La version du système d'exploitation pour le périphérique que Device-ID identifie comme étant la source du trafic. |
| Nom d'hôte source (src_host) | Le nom d'hôte du périphérique que Device-ID identifie comme étant la source du trafic. |
| Adresse MAC source (src_mac) | L'adresse MAC du périphérique que Device-ID identifie comme étant la source du trafic. |
| Région (région) | La région géographique d'où provient le trafic. |
| Agent utilisateur (user_agent) | La chaîne de l'en-tête de requête HTTP `User-Agent (Agent utilisateur)`. |
| ID de session | Une chaîne qui identifie de manière unique la session de trafic. |

## Champs des journaux de configuration

**Format :** FUTURE_USE, Heure de réception, Numéro de série, Type, Sous-type, FUTURE_USE, Heure de génération, Hôte, Système virtuel, Commande, Admin, Client, Résultat, Chemin de configuration, Détail avant modification, Détail après modification, Numéro de séquence, Indicateurs d'action, Hiérarchie de groupes de périphériques niveau 1, Hiérarchie de groupes de périphériques niveau 2, Hiérarchie de groupes de périphériques niveau 3, Hiérarchie de groupes de périphériques niveau 4, Nom du système virtuel, Nom du périphérique, Groupe d'appareils, Commentaire d'audit

| Nom du champ | Description |
|---|---|
| Heure de réception (receive_time ou cef-formatted-receive_time) | Heure de réception du journal dans le panneau de gestion. |

| Nom du champ | Description |
|---|---|
| Numéro de série (serial) | Numéro de série du périphérique ayant généré le journal. |
| Type (type) | Spécifie le type de journal ; la valeur est CONFIG. |
| Menace / Type de contenu (sous-type) | Sous-type du journal de configuration ; non utilisé. |
| Heure de génération (time_generated ou cef-formatted-time_generated) | Heure de génération du journal dans le plan de données. |
| Hôte (host) | Nom d'hôte ou adresse IP de la machine client. |
| Système virtuel (vsys) | Système virtuel associé au journal de configuration. |
| Commande (cmd) | Commande exécutée par l'administrateur ; les valeurs possibles sont add, clone, commit, delete, edit, move, rename, set. |
| Admin (admin) | Nom d'utilisateur de l'administrateur procédant à la configuration. |
| Client (client) | Client utilisé par l'administrateur ; les valeurs possibles sont Web et CLI. |
| Résultat (result) | Résultat de l'action de configuration ; les valeurs possibles sont Submitted, Succeeded, Failed et Unauthorized. |
| Chemin de configuration (path) | Chemin de la commande de configuration exécutée ; 512 octets maximum. |
| Détail avant modification (before_change_detail) | Ce champ s'applique aux journaux personnalisés uniquement, et non au format par défaut.<br>Il contient le xpath complet avant la modification de la configuration. |
| Détail après modification (after_change_detail) | Ce champ s'applique aux journaux personnalisés uniquement, et non au format par défaut.<br>Il contient le xpath complet après la modification de la configuration. |
| Numéro de séquence (seqno) | Identifiant d'entrée du journal 64 bits incrémenté de manière séquentielle ; chaque type de journal contient un espace de numéro unique. |
| Indicateurs d'action (actionflags) | Champ de bits indiquant si le journal a été transféré à Panorama. |

| Nom du champ | Description |
|---|---|
| Hiérarchie de groupes de périphériques (dg_hier_level_1 à dg_hier_level_4) | Une séquence de numéros d'identification qui indique l'emplacement du groupe de périphériques dans une hiérarchie de groupes de périphériques. Le pare-feu (ou système virtuel) générant le journal inclut le numéro d'identification de chaque ancêtre dans sa hiérarchie de groupes de périphériques. Le groupe de périphériques partagé (niveau 0) n'est pas inclus dans cette structure.<br>Si les valeurs du journal sont 12, 34, 45, 0, cela signifie que le journal a été généré par un pare-feu (ou système virtuel) appartenant au groupe de périphériques 45, et que ses ancêtres sont 34 et 12. Pour afficher les noms des groupes de périphériques correspondant à la valeur 12, 34 ou 45, utilisez l'une des méthodes suivantes :<br>Requête d'API :<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| Nom du système virtuel (vsys_name) | Le nom du système virtuel associé à la session ; valide uniquement sur les pare-feu pouvant comporter plusieurs systèmes virtuels. |
| Nom du périphérique (device_name) | Le nom d'hôte du pare-feu sur lequel la session a été consignée. |
| Groupe d'appareils (dg_id) | Le groupe d'appareils auquel le pare-feu appartient s'il est géré par un serveur de gestion Panorama™. |
| Commentaires d'audit (comment) | Le commentaire d'audit est entré dans une modification de la configuration des règles de politique. |

## Paramètres du journal système

**Format :** FUTURE_USE, Heure de réception, Numéro de série, Type, Type de Contenu / de Menace, Sous-type, FUTURE_USE, Heure de génération, Utilisateur source, Système virtuel, ID d'événement, Objet, FUTURE_USE, FUTURE_USE, Module, Gravité, Description, Numéro de séquence, Indicateurs d'action, Hiérarchie de groupes de périphériques niveau 1, Hiérarchie de groupes de périphériques niveau 2, Hiérarchie de groupes de périphériques niveau 3, Hiérarchie de groupes de périphériques niveau 4, Nom du système virtuel, Nom du périphérique, FUTURE_USE, FUTURE_USE, Horodatage haute résolution

| Nom du champ | Description |
|---|---|
| Heure de réception (receive_time ou cef-formatted-receive_time) | Heure de réception du journal dans le panneau de gestion. |

| Nom du champ | Description |
|---|---|
| Numéro de série (serial) | Numéro de série du pare-feu ayant généré le journal. |
| Type (type) | Spécifie le type de journal ; la valeur est SYSTEM. |
| Type de contenu/de menace (subtype) | Sous-type du journal système ; fait référence au démon système générant le journal. Les valeurs possibles sont crypto, dhcp, dnsproxy, dos, general, global-protect, ha, hw, nat, ntpd, pbf, port, pppoe, ras, routing, satd, sslmgr, sslvpn, userid, url-filtering, vpn. |
| Heure de génération (time_generated ou cef-formatted-time_generated) | Heure de génération du journal dans le plan de données. |
| Système virtuel (vsys) | Système virtuel associé au journal de configuration. |
| ID d'événement (eventid) | Chaîne indiquant le nom de l'événement. |
| Objet (object) | Nom de l'objet associé à l'événement système. |
| Module (module) | Ce champ s'applique uniquement lorsque la valeur du champ Sous-type est general. Il fournit des informations supplémentaires sur le sous-système générant le journal ; les valeurs possibles sont general, management, auth, ha, upgrade, chassis. |
| Gravité (severity) | Gravité associée à l'événement ; les valeurs possibles sont informational, low, medium, high, critical. |
| Description (opaque) | Description détaillée de l'événement ; 512 octets maximum. |
| Numéro de séquence (seqno) | Identifiant d'entrée de journal 64 bits incrémenté de manière séquentielle ; chaque type de journal contient un espace de numéro unique. |
| Indicateurs d'action (actionflags) | Champ de bits indiquant si le journal a été transféré à Panorama. |
| Hiérarchie de groupes de périphériques (dg_hier_level_1 à dg_hier_level_4) | Une séquence de numéros d'identification qui indique l'emplacement du groupe de périphériques dans une hiérarchie de groupes de périphériques. Le pare-feu (ou système virtuel) générant le journal inclut le numéro d'identification de chaque ancêtre dans sa hiérarchie de groupes de périphériques. Le groupe de périphériques partagé (niveau 0) n'est pas inclus dans cette structure. |

| Nom du champ | Description |
|---|---|
| | Si les valeurs du journal sont 12, 34, 45, 0, cela signifie que le journal a été généré par un pare-feu (ou système virtuel) appartenant au groupe de périphériques 45, et que ses ancêtres sont 34 et 12. Pour afficher les noms des groupes de périphériques correspondant à la valeur 12, 34 ou 45, utilisez l'une des méthodes suivantes :<br>Requête d'API :<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| Nom du système virtuel (vsys_name) | Le nom du système virtuel associé à la session ; valide uniquement sur les pare-feu pouvant comporter plusieurs systèmes virtuels. |
| Nom du périphérique (device_name) | Le nom d'hôte du pare-feu sur lequel la session a été consignée. |
| Horodatage haute résolution (high_res_timestamp) | L'heure en milliseconde de réception du journal dans le plan de gestion.<br>Le format pour ce nouveau champ est YYYY-MM-DDThh:ss:sssTZD:<br>• **YYYY**—Année sur quatre chiffres<br>• **MM**—Mois sur deux chiffres<br>• **DD**—Jours du mois sur deux chiffres (01 à 31)<br>• **T**—Indicateur pour le début de l'horodatage<br>• **hh**—Heures sur deux chiffres utilisant le format 24 heures (00 à 23)<br>• **mm**—Minutes sur deux chiffres (00 à 59)<br>• **ss**—Sondes sur deux chiffres (00 à 60)<br>• **sss**—Un ou plusieurs chiffres pour les millisecondes<br>• **TZD**—Indicateur de fuseau horaire (+hh:mm ou -hh:mm)<br>*L'horodatage haute résolution est pris en charge pour les journaux reçus des pare-feux gérés fonctionnant sous PAN-OS 10.1 et les versions ultérieures. Les journaux reçus de pare-feux gérés exécutant PAN-OS 9.1 et les versions antérieures affichent un horodatage `1969-12-31T16:00:00:000-8:00` quelle que soit la date à laquelle le journal a été reçu.* |

## Champs des journaux des événements corrélés

**Format :** FUTURE_USE, Heure de réception, Numéro de série, Type, Type de menace/contenu, FUTURE_USE, Heure de génération, Adresse source. Utilisateur source, Système virtuel, Catégorie, Gravité, Hiérarchie de groupes de périphériques niveau 1, Hiérarchie de groupes de périphériques niveau 2, Hiérarchie de groupes de périphériques niveau 3, Hiérarchie de groupes de périphériques

niveau 4, Nom du système virtuel, Nom du périphérique, ID pour le système virtuel, Nom d'objet, ID d'objet, Preuve

| Nom du champ | Description |
|---|---|
| Heure de réception (receive_time ou cef-formatted-receive_time) | Heure de réception du journal dans le panneau de gestion. |
| Numéro de série (serial) | Numéro de série du périphérique ayant généré le journal. |
| Type (type) | Spécifie le type de journal ; la valeur est CORRELATION. |
| Type de contenu/de menace (subtype) | Sous-type du journal système ; fait référence au démon système générant le journal. Les valeurs possibles sont crypto, dhcp, dnsproxy, dos, general, global-protect, ha, hw, nat, ntpd, pbf, port, pppoe, ras, routing, satd, sslmgr, sslvpn, userid, url-filtering, vpn. |
| Heure de génération (time_generated ou cef-formatted-time_generated) | Heure de génération du journal dans le plan de données. |
| Adresse source (src) | Adresse IP de l'utilisateur ayant ouvert l'événement. |
| Utilisateur source (srcuser) | Nom de l'utilisateur ayant ouvert l'événement. |
| Système virtuel (vsys) | Système virtuel associé au journal de configuration. |
| Catégorie (category) | Un récapitulatif du type de menace ou nuisance qui pèse sur le réseau, l'utilisateur ou l'hôte. |
| Gravité (severity) | Gravité associée à l'événement ; les valeurs possibles sont informational, low, medium, high, critical. |
| Hiérarchie de groupes de périphériques (dg_hier_level_1 à dg_hier_level_4) | Une séquence de numéros d'identification qui indique l'emplacement du groupe de périphériques dans une hiérarchie de groupes de périphériques. Le pare-feu (ou système virtuel) générant le journal inclut le numéro d'identification de chaque ancêtre dans sa hiérarchie de groupes de périphériques. Le groupe de périphériques partagé (niveau 0) n'est pas inclus dans cette structure.<br>Si les valeurs du journal sont 12, 34, 45, 0, cela signifie que le journal a été généré par un pare-feu (ou système virtuel) appartenant au groupe de périphériques 45, et que ses ancêtres sont 34 et 12. Pour afficher les |

| Nom du champ | Description |
|---|---|
| | noms des groupes de périphériques correspondant à la valeur 12, 34 ou 45, utilisez l'une des méthodes suivantes :<br>Requête d'API :<br>`/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>` |
| Nom du système virtuel (vsys_name) | Le nom du système virtuel associé à la session ; valide uniquement sur les pare-feu pouvant comporter plusieurs systèmes virtuels. |
| Nom du périphérique (device_name) | Le nom d'hôte du pare-feu sur lequel la session a été consignée. |
| ID du système virtuel (vsys_id) | Un identificateur unique pour un système virtuel sur un pare-feu Palo Alto Networks. |
| Nom de l'objet (objectname) | Nom de l'objet de corrélation qui a fait l'objet d'une correspondance. |
| ID d'objet (object_id) | Nom de l'objet associé à l'événement système. |
| Preuve (evidence) | Un énoncé récapitulatif qui indique le nombre de fois où l'hôte a trouvé des correspondances aux conditions définies dans l'objet de corrélation. Par exemple, l'hôte a visité l'URI malveillante connue (19 fois). |

## Champs des journaux GTP

**Format** : FUTURE_USE, Heure de réception, Numéro de série, FUTURE_USE, FUTURE_USE, FUTURE_USE, Heure de génération, Adresse source, Adresse de destination, FUTURE_USE, FUTURE_USE, Nom de la règle, FUTURE_USE, FUTURE_USE, Application, Système virtuel, Zone source, Zone de destination, Interface d'entrée, Interface de sortie, Action du journal, FUTURE_USE, ID de session, FUTURE_USE, Port source, Port de destination, FUTURE_USE, FUTURE_USE, FUTURE_USE, Protocole, Action, Type d'événement GTP, MSISDN, Nom du point d'accès, Technologie d'accès radio, Type de message GTP, Adresse IP de l'utilisateur final, Identifiant 1 du point de terminaison du tunnel, Identifiant 2 du point de terminaison du tunnel, Interface GTP, Cause GTP, Gravité, Traitement du pays MCC, Traitement du réseau MNC, Indicatif régional, ID de cellule, Code d'événement GTP, FUTURE_USE, FUTURE_USE, Emplacement source, Emplacement de destination, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, ID/IMSI du tunnel, IMEI/Balise de surveillance, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, Heure de début, Temps écoulé, Règle d'inspection des tunnels, IP de l'utilisateur distance, ID de l'utilisateur distant, UUID pour la règle, ID PCAP, Horodatage haute résolution, Type de service de tranche A, Différentiateur de tranche, Sous-catégorie de l'application, Catégorie de l'application, Technologie de l'application, Risque lié à l'application, Caractéristique de l'application, Conteneur de l'application, Saas de l'application, Etat sanctionné de l'application

| Nom du champ | Description |
|---|---|
| Heure de réception (receive_time ou cef-formatted-receive_time) | Mois, jour et heure de réception du journal dans le panneau de gestion. |
| Numéro de série (serial) | Numéro de série du pare-feu ayant généré le journal. |
| Type (type) | Spécifie le type de journal ; la valeur est SCTP. |
| Menace / Type de contenu (sous-type) | Sous-type du journal du trafic ; les valeurs possibles sont start, end, drop et deny<br>• Start — session ouverte<br>• End — session fermée<br>• Drop — session arrêtée avant l'identification de l'application et absence de règle autorisant la session.<br>• Deny — session arrêtée après l'identification de l'application et présence d'une règle de blocage ou absence de règle autorisant la session. |
| Heure de génération (time_generated ou cef-formatted-time_generated) | Heure de génération du journal dans le plan de données. |
| Adresse source (src) | L'adresse IP source des paquets de la session. |
| Adresse de destination (dst) | L'adresse IP de destination des paquets de la session. |
| Nom de la règle (rule) | Le nom de la règle de politique de sécurité en vigueur sur la session. |
| Application (app) | Le protocole de mise en tunnel utilisé dans la session. |
| Système virtuel (vsys) | Système virtuel associé à la session. |
| Zone source (from) | La zone source des paquets de la session. |
| Zone de destination (to) | La zone de destination des paquets de la session. |
| Interface entrante (inbound_if) | Interface d'origine de la session. |
| Interface sortante (outbound_if) | Interface à laquelle la session est destinée. |
| Action du journal (logset) | Profil de transfert des journaux appliqué à la session. |
| ID de session (sessionid) | L'ID de session de la session journalisée. |

| Nom du champ | Description |
|---|---|
| Port source (sport) | Port source utilisé par la session. |
| Port de destination (dport) | Port de destination utilisé par la session. |
| Protocole IP (proto) | Protocole IP associé à la session. |
| Action (action) | Action prise pour la session. Les valeurs possibles sont :<br>• allow — la session a été autorisée par la politique<br>• deny — la session a été refusée par la politique |
| Type d'événement GTP (event_type) | Définit l'événement déclenché par un message GTP lorsque le profil de protection GT est appliqué au trafic GTP. Il peut également être déclenché par le début ou la fin d'une session GTP. |
| MSISDN (msisdn) | Identité du service associé à l'abonné mobile, laquelle se compose d'un code de pays, d'un code de destination nationale et d'un abonné. Il se compose de chiffres décimaux (de 0 à 9) uniquement et d'un maximum de 15 chiffres. |
| Nom du point d'accès (apn) | Fait référence à une Packet Data Network Data Gateway (passerelle de réseau de données par paquets ; PGW) ou à un nœud de prise en charge du GPRS passerelle dans un réseau mobile. Il se compose d'un identifiant de réseau APN obligatoire et d'un identifiant d'opérateur APN facultatif. |
| Technologie d'accès radio (rat) | Le type de technologie utilisé pour l'accès radio. Par exemple, EUTRAN, WLAN, Virtuel, Évolution HSPA, GAN et GERAN. |
| Type de message GTP (msg_type) | Indique le type de message GTP. |
| Adresse IP de fin (end_ip_adr) | L'adresse IP d'un abonné mobile allouée par un PGW/GGSN. |
| Identifiant 1 du point de terminaison du tunnel (teid1) | Identifie le tunnel GTP dans le nœud de réseau. TEID1 est le premier TEID dans le message GTP. |
| Identifiant 2 du point de terminaison du tunnel (teid2) | Identifie le tunnel GTP dans le nœud de réseau. TEID2 est le second TEID dans le message GTP. |
| Interface GTP (gtp_interface) | Interface 3GPP de laquelle un message GTP est reçu. |
| Code de cause GTP (cause_code) | La valeur du code de cause GTP dans les réponses de journaux qui contiennent un élément d'information qui fournit des |

| Nom du champ | Description |
|---|---|
| | informations sur l'acceptation ou le rejet des requêtes GTP par un nœud de réseau. |
| Gravité (severity) | Gravité associée à l'événement ; les valeurs possibles sont informational, low, medium, high, critical. |
| Traitement du réseau MCC (mcc) | Code de pays mobile de l'opérateur du nœud de réseau. |
| Traitement du réseau MNC (mnc) | Code de réseau mobile de l'opérateur du nœud de réseau. |
| Indicatif régional (area_code) | Région au sein d'un Public Land Mobile Network (Réseau mobile terrestre public ; PLMN). |
| ID de cellule (cell_id) | Station de base au sein d'un indicatif régional. |
| Code d'événement GTP (event_code) | Code d'événement décrivant l'événement GTP. |
| Emplacement source (srcloc) | Pays ou région source pour les adresses privées ; 32 octets maximum. |
| Emplacement de destination (dstloc) | Pays ou région de destination pour les adresses privées ; 32 octets maximum. |
| ID/IMSI du tunnel (imsi) | La International Mobile Subscriber Identity (identité internationale d'abonné mobile ; IMSI) est un numéro unique alloué à chaque abonné mobile dans le système GSM/UTTS/EPS. Ce numéro se compose de chiffres décimaux (de 0 à 9) uniquement, et un maximum de 15 chiffres est permis. |
| Balise de surveillance/IMEI (imei) | La International Mobile Equipment Identity (identité internationale d'équipement mobile ; IMEI) est un nombre unique composée de 15 à 16 chiffres qui est alloué à chaque équipement de station mobile. |
| Heure de début (start) | Heure de début de la session. |
| Temps écoulé (elapsed) | Durée écoulée de la session. |
| Règle d'inspection des tunnels (tunnel_insp_rule) | Nom de la règle d'inspection des tunnels associée au trafic de tunnel de texte en clair. |
| IP de l'utilisateur distant (remote_user_ip) | Adresse IPv4 ou IPv6 utilisée par un utilisateur distant. |

| Nom du champ | Description |
|---|---|
| ID de l'utilisateur distant (remote_user_id) | Identité IMSI d'un utilisateur distant et, si disponible, une identité IMEI et/ou une identité MSISDN. |
| UUID pour la règle (rule_uuid) | ID unique universel donné à la règle. |
| ID pcap (pcap_id) | ID de capture de paquets unique qui sert à localiser le fichier pcap enregistré sur le pare-feu. |
| Horodatage haute résolution (high_res_timestamp) | L'heure en milliseconde de réception du journal dans le plan de gestion.<br>Le format pour ce nouveau champ est YYYY-MM-DDThh:ss:sssTZD:<br>• **YYYY**—Année sur quatre chiffres<br>• **MM**—Mois sur deux chiffres<br>• **DD**—Jours du mois sur deux chiffres (01 à 31)<br>• **T**—Indicateur pour le début de l'horodatage<br>• **hh**—Heures sur deux chiffres utilisant le format 24 heures (00 à 23)<br>• **mm**—Minutes sur deux chiffres (00 à 59)<br>• **ss**—Sondes sur deux chiffres (00 à 60)<br>• **sss**—Un ou plusieurs chiffres pour les millisecondes<br>• **TZD**—Indicateur de fuseau horaire (+hh:mm ou -hh:mm)<br>*L'horodatage haute résolution est pris en charge pour les journaux reçus des pare-feux gérés fonctionnant sous PAN-OS 10.1 et les versions ultérieures. Les journaux reçus de pare-feux gérés exécutant PAN-OS 9.1 et les versions antérieures affichent un horodatage `1969-12-31T16:00:00:000-8:00` quelle que soit la date à laquelle le journal a été reçu.* |
| Type de service de tranche A (nsdsai_sst) | Le type de service de tranche A de l'ID de tranche de réseau. |
| Différenciateur de tranche A (nsdsai_sd) | Le différenciateur de tranche A de l'ID de tranche de réseau. |
| Sous-catégorie d'application (subcategory_of_app) | La sous-catégorie d'application spécifiée dans les propriétés de configuration de l'application. |

| Nom du champ | Description |
|---|---|
| Catégorie d'application (category_of_app) | Catégorie d'application spécifiée dans les propriétés de configuration de l'application. Les valeurs sont :<br>• systèmes professionnels<br>• collaboration<br>• Internet grand public<br>• multimédia<br>• Mise en réseau<br>• saas |
| Technologie d'application (technology_of_app) | La technologie d'application spécifiée dans les propriétés de configuration de l'application. Les valeurs sont :<br>• basé sur navigateur<br>• client/serveur<br>• protocole réseau<br>• poste à poste |
| Risque d'application (risk_of_app) | Niveau de risque associé à l'application (1=le plus faible à 5=le plus élevé). |
| Caractéristique de l'application (characteristic_of_app) | Liste séparée par des virgules des caractéristiques applicables de l'application |
| Conteneur d'applications (container_of_app) | L'application parent d'une application. |
| Application SaaS (is_saas_of_app) | Affiche `1` s'il s'agit d'une application SaaS ou `0` s'il ne s'agit pas d'une application SaaS. |
| État sanctionné de l'application (sanctioned_state_of_app) | Affiche `1` si la candidature est sanctionnée ou `0` si la candidature n'est pas sanctionnée. |
| Sous-catégorie d'application (subcategory_of_app) | La sous-catégorie d'application spécifiée dans les propriétés de configuration de l'application. |

## Gravité Syslog

La gravité Syslog est basée sur le type et le contenu du journal.

| Type de journal/gravité | Gravité Syslog |
|---|---|
| Trafic | info |
| Configuration | info |
| Menaces/Système — Informational | info |
| Menaces/Système — Low | Avis |
| Menaces/Système — Medium | Avertissement |
| Menaces/Système — High | Avertissement |
| Menaces/Système — Critical | Critique |

## Format de journal/d'événement personnalisé

Pour simplifier l'intégration dans des systèmes d'analyse de journaux externes, le pare-feu vous permet de personnaliser le format du journal ; il vous permet également d'ajouter des paires d'attributs ***Clé : Valeur*** personnalisées. Des formats de message personnalisés peuvent être configurés dans **Device (Périphérique)** > **Server Profiles (Profils de serveur)** > **Syslog (Syslog)** > **Syslog Server Profile (Profil de serveur Syslog)** > **Custom Log Format (Format de journal personnalisé)**.

Pour la mise en forme de journal compatible avec les Common Event Format (formats d'événements courants ; CEF) ArcSight, reportez-vous au Guide de configuration des CEF.

## Séquences d'échappement

Tout champ contenant une virgule ou des guillemets doubles est englobé dans des guillemets doubles. De plus, si des guillemets doubles apparaissent dans un champ, il est échappé en le faisant précéder d'autres guillemets doubles. Pour des raisons de rétrocompatibilité, le champ Divers du journal des menaces est toujours englobé dans des guillemets doubles.

# Surveillance et pièges SNMP

Les rubriques suivantes décrivent comment les pare-feu, Panorama, et l'équipement WF-500 Palo Alto Networks mettent en œuvre le protocole Simple Network Management Protocol (SNMP), ainsi que les procédures de configuration de la surveillance SNMP et de la distribution des pièges.

- Prise en charge SNMP
- Utilisation d'un gestionnaire SNMP pour parcourir les MIB et les objets
- Activation de services SNMP pour des éléments réseau protégés par un pare-feu
- Surveillance des statistiques à l'aide de SNMP
- Transfert des pièges de pare-feu à un gestionnaire SNMP
- MIB prises en charge

## Prise en charge SNMP

Vous pouvez utiliser un gestionnaire de Simple Network Management Protocol (protocole simple de gestion réseau ; SNMP) afin de surveiller des alertes événementielles et des statistiques opérationnelles pour le pare-feu, Panorama, ou l'équipement WF-500 et pour le trafic qu'ils traitent. Les statistiques et les pièges vous permettent d'identifier les limitations des ressources, les modifications ou défaillances système, et les attaques de logiciels malveillants. Vous configurez les alertes en transférant des données de journal sous forme de pièges, et activez l'envoie des statistiques en réponse à des messages (ou requêtes) GET de votre gestionnaire SNMP. Chaque piège et statistique comporte un identifiant d'objet (OID). Les OID liés sont organisés de manière hiérarchique dans les Management Information Bases (bases d'informations de gestion - MIB) que vous chargez dans votre gestionnaire SNMP pour activer la surveillance.

***Lorsqu'un événement déclenche la génération de pièges SNMP (par exemple, en cas de défaillance d'une interface), le pare-feu, l'équipement virtuel Panorama, l'équipement M-Series et l'équipement WF-500 répondent en mettant à jour l'objet SNMP correspondant (par exemple, les interfaces MIB), plutôt que d'attendre la mise à jour périodique de l'ensemble des objets, qui se produit aux dix secondes. Cette façon de faire garantit que votre gestionnaire SNMP affiche les dernières informations lorsqu'il interroge un objet concernant la confirmation d'un événement.***

Le pare-feu, Panorama et l'équipement WF-500 prennent en charge la version 2c et la version 3 de SNMP. Choisissez celle à utiliser en fonction de la version prise en charge par les autres périphériques de votre réseau et des exigences de sécurité de votre réseau. SNMPv3 est plus sécurisé et offre un contrôle d'accès plus granulaire des statistiques systèmes que SNMPv2c. Le tableau suivant récapitule les fonctions de sécurité de chaque version : Vous sélectionnez la version et vous configurez les fonctionnalités de sécurité dans les sections Surveillance des statistiques à l'aide de SNMP et Transfert des pièges de pare-feu à un gestionnaire SNMP.

| VersionS | Authentification | Confidentialité du message | Intégrité du message | Granularité d'accès à la MIB |
|---|---|---|---|---|
| SNMPv2c | chaîne de communauté | Non (texte en clair) | Non | Accès de communauté SNMP à toutes les MIB d'un périphérique |
| SNMPv3 | ID de moteur, nom d'utilisateur et mot de passe d'authentification (hachage SHA pour le mot de passe) | Mot de passe de confidentialité pour le cryptage AES (128, 192 ou 256) des messages SNMP | Oui | Accès utilisateur basé sur des vues qui incluent ou excluent des OID spécifiques |

L'Implémentation SNMP illustre un déploiement dans lequel les pare-feux transfèrent des pièges à un gestionnaire SNMP tout en transférant également des journaux à des collecteurs de journaux. Vous pourriez également configurer les collecteurs de journaux pour qu'ils transfèrent les pièges de pare-feu au gestionnaire SNMP. Pour plus d'informations sur ces déploiements, reportez-vous aux Options de transfert des journaux dans la Centralisation des Rapports et des Journaux. Dans tous les déploiements, le gestionnaire SNMP obtient les statistiques directement des pare-feux, Panorama ou l'équipement WF-500. Dans cet exemple, un même gestionnaire SNMP collecte les pièges et les statistiques, même si vous pouvez utiliser plusieurs gestionnaires pour ces fonctions si cela convient mieux à votre réseau.

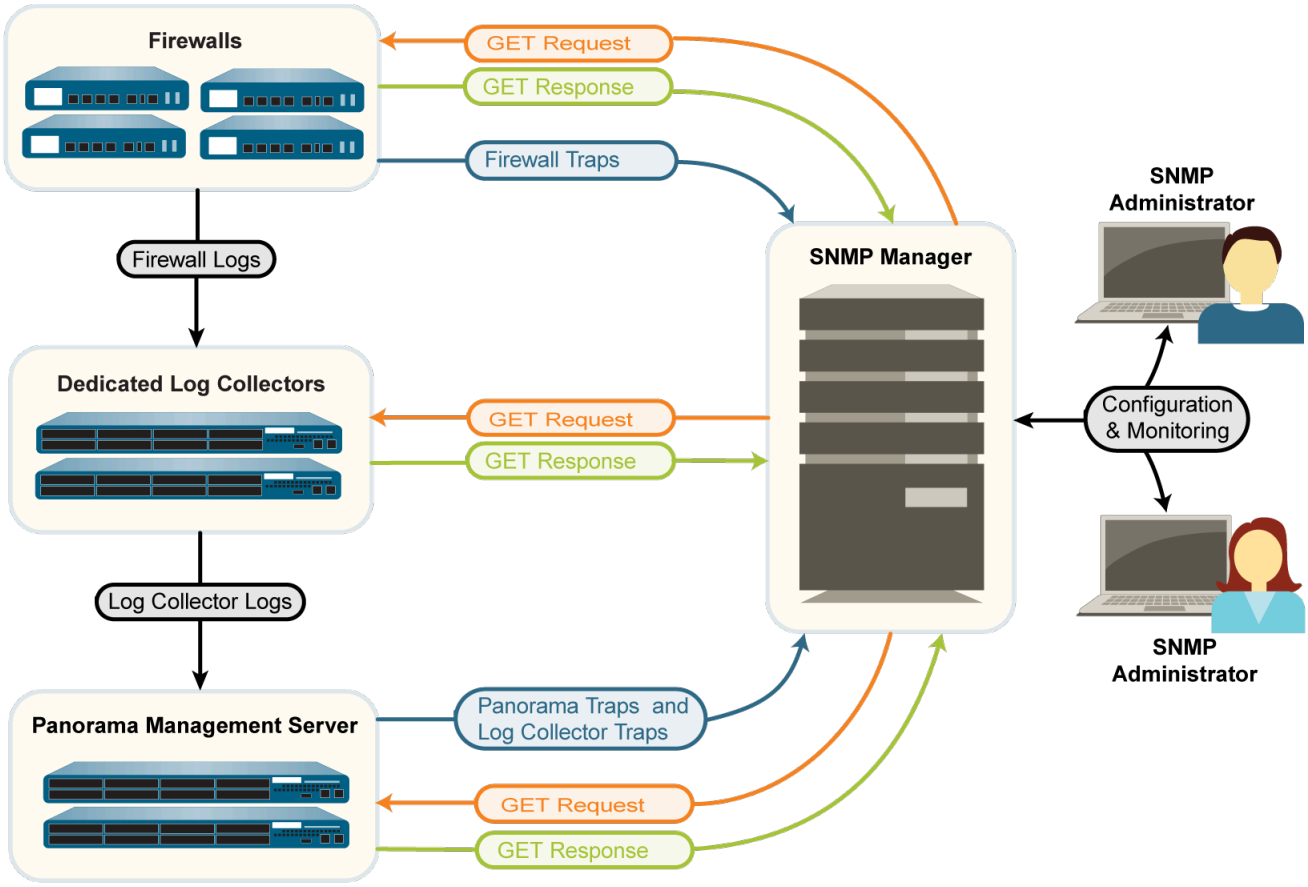



**Figure 2: Implémentation SNMP**

# Utilisation d'un gestionnaire SNMP pour parcourir les MIB et les objets

Pour utiliser SNMP pour surveiller des pare-feu, Panorama ou l'équipement WF-500 de Palo Alto Networks, vous devez tout d'abord charger les MIB prises en charge dans votre gestionnaire SNMP et déterminer les Objects Identifiers (identifiants d'objets ; OID) correspondant aux statistiques et pièges systèmes que vous souhaitez surveiller. Les rubriques suivantes présentent une vue d'ensemble des tâches que vous effectuez pour rechercher des OID et des MIB dans un gestionnaire SNMP. Pour les étapes spécifiques à effectuer pour ces tâches, reportez-vous à la documentation de votre logiciel de gestion SNMP.

- Identification d'une MIB contenant un OID connu
- Parcours d'une MIB
- Identification de l'OID d'une statistique ou d'un piège système

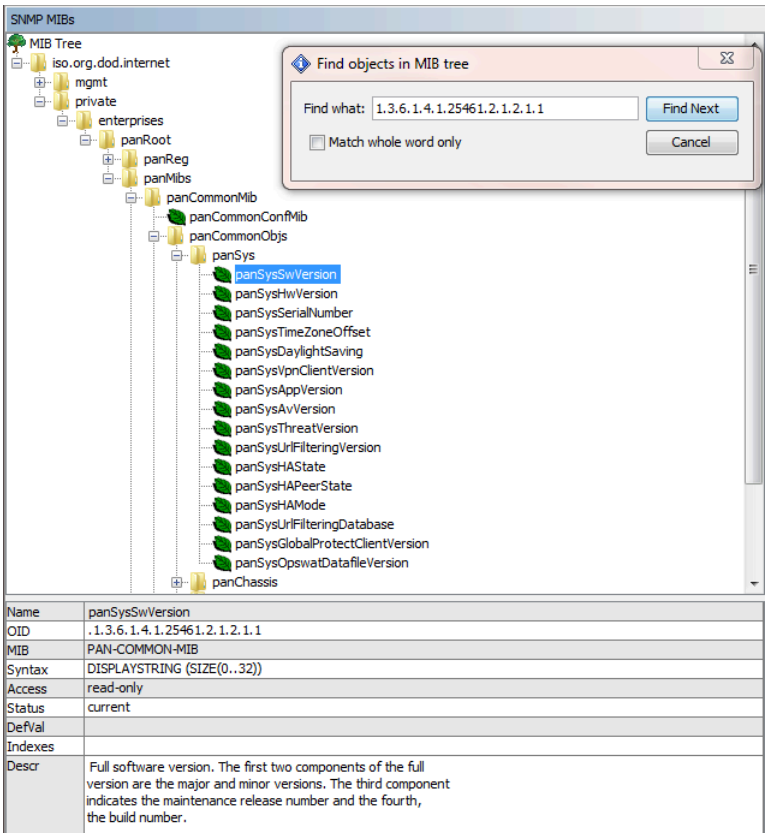
## Identification d'une MIB contenant un OID connu

Si vous connaissez déjà l'OID d'un objet SNMP spécifique (statistique ou piège) et que vous souhaitez connaître les OID d'objets similaires pour pouvoir les surveiller, vous pouvez parcourir la MIB contenant l'OID connu.

**STEP 1 |** Chargez toutes les MIB prises en charge dans votre gestionnaire SNMP.

**STEP 2 |** Recherchez l'OID connue dans l'arborescence de la MIB. Le résultat de la recherche affiche le chemin de l'OID dans la MIB, ainsi que des informations sur l'OID (par exemple, le nom, l'état et la description). Vous pouvez ensuite sélectionner d'autres OID dans la même MIB pour consulter leurs informations.

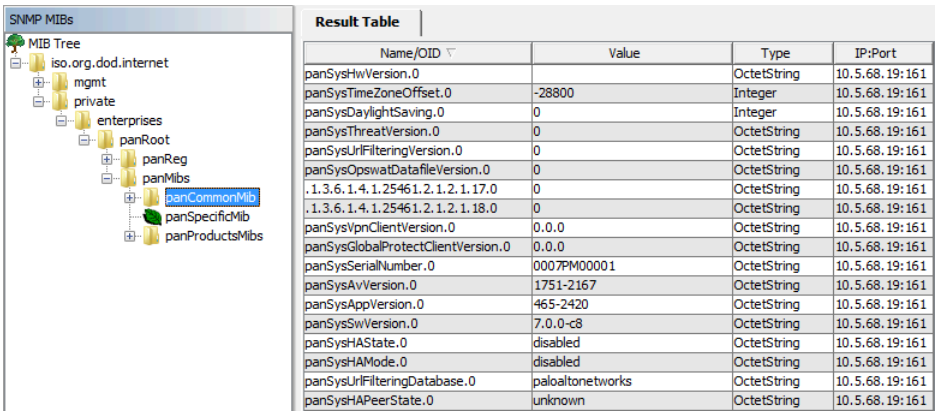



**STEP 3 |** (Facultatif)Le Parcours d'une MIB est possible pour afficher tous ses objets.

## Parcours d'une MIB

Si vous souhaitez voir les objets SNMP (statistiques et pièges systèmes) disponibles pour la surveillance, l'affichage de tous les objets d'une MIB spécifique peut être utile. Pour cela, chargez les MIB prises en charge dans votre gestionnaire SNMP et ***parcourez*** la MIB souhaitée. Pour répertorier les pièges pris en charge par les pare-feu, Panorama et l'équipement WF-500 Palo Alto Networks, parcourez le MIB panCommonEventEventsV2. Dans l'exemple ci-dessous, le parcours de PAN-COMMON-MIB.my affiche la liste suivante d'OID et leurs valeurs pour certaines statistiques :




| Name/OID | Value | Type | IP:Port |
|---|---|---|---|
| panSysHwVersion.0 | | OctetString | 10.5.68.19:161 |
| panSysTimeZoneOffset.0 | -28800 | Integer | 10.5.68.19:161 |
| panSysDaylightSaving.0 | 0 | Integer | 10.5.68.19:161 |
| panSysThreatVersion.0 | 0 | OctetString | 10.5.68.19:161 |
| panSysUrlFilteringVersion.0 | 0 | OctetString | 10.5.68.19:161 |
| panSysOpswatDatafileVersion.0 | 0 | OctetString | 10.5.68.19:161 |
| .1.3.6.1.4.1.25461.2.1.2.1.17.0 | 0 | OctetString | 10.5.68.19:161 |
| .1.3.6.1.4.1.25461.2.1.2.1.18.0 | 0 | OctetString | 10.5.68.19:161 |
| panSysVpnClientVersion.0 | 0.0.0 | OctetString | 10.5.68.19:161 |
| panSysGlobalProtectClientVersion.0 | 0.0.0 | OctetString | 10.5.68.19:161 |
| panSysSerialNumber.0 | 0007PM00001 | OctetString | 10.5.68.19:161 |
| panSysAvVersion.0 | 1751-2167 | OctetString | 10.5.68.19:161 |
| panSysAppVersion.0 | 465-2420 | OctetString | 10.5.68.19:161 |
| panSysSwVersion.0 | 7.0.0-c8 | OctetString | 10.5.68.19:161 |
| panSysHAState.0 | disabled | OctetString | 10.5.68.19:161 |
| panSysHAMode.0 | disabled | OctetString | 10.5.68.19:161 |
| panSysUrlFilteringDatabase.0 | paloaltonetworks | OctetString | 10.5.68.19:161 |
| panSysHAPeerState.0 | unknown | OctetString | 10.5.68.19:161 |

## Identification de l'OID d'une statistique ou d'un piège système

Pour utiliser un gestionnaire SNMP pour surveiller des pare-feu, Panorama, ou l'équipement WF-500, vous devez connaître les OID des statistiques et pièges systèmes que vous souhaitez surveiller.

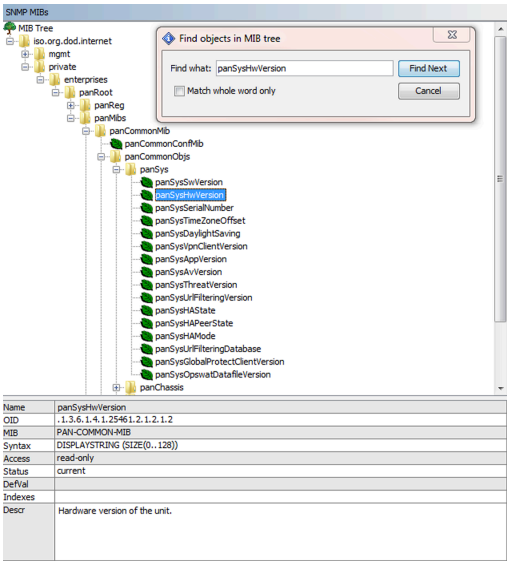
**STEP 1 |** Passez en revue les MIB pris en charge pour déterminer celle qui contient le type de statistique souhaité. Par exemple, PAN-COMMON-MIB.my contient des informations sur la version du matériel. La MIB panCommonEventEventsV2 contient tous les pièges pris en charge par les pare-feu, Panorama et les équipements WF-500 Palo Alto Networks.

**STEP 2 |** Ouvrez la MIB dans un éditeur de texte, puis recherchez un mot-clé. Par exemple, l'utilisation de **Hardware version** comme chaîne de recherche dans PAN-COMMON-MIB identifie l'objet panSysHwVersion :

```
panSysHwVersion OBJECT-TYPE
 SYNTAX DisplayString (SIZE(0..128))
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION
 "Hardware version of the unit."
 ::= {panSys 2}
```

**STEP 3 |** Dans un navigateur MIB, recherchez le nom d'objet identifié dans l'arborescence de la MIB pour afficher son OID. Par exemple, l'objet panSysHwVersion inclut un OID de 1.3.6.1.4.1.25461.2.1.2.1.2.




# Activation de services SNMP pour des éléments réseau protégés par un pare-feu

Si vous devez utiliser le protocole Simple Network Management Protocol (SNMP) pour surveiller ou gérer des éléments réseau (par exemple, des commutateurs et des routeurs) se trouvant dans les zones de sécurité de pare-feu Palo Alto Networks, vous devez créer une règle de sécurité autorisant les services SNMP pour ces éléments.

*Vous n'avez pas besoin d'une règle de sécurité pour activer la surveillance SNMP de pare-feu, de Panorama ou d'équipements WF-500 Palo Alto Networks. Pour plus d'informations, reportez-vous à la section* Surveillance des statistiques à l'aide de SNMP.

**STEP 1 |** Créez un groupe d'applications.

1. Sélectionnez **Objects (Objets)** > **Application Group (Groupe d'applications)** et cliquez sur **Add (Ajouter)**.
2. Saisissez un **Name (Nom)** pour identifier le groupe d'applications.
3. Cliquez sur **Add (Ajouter)**, saisissez **snmp**, puis sélectionnez **snmp (SNMP)** et **snmp-trap (Piège SNMP)** dans la liste déroulante.
4. Cliquez sur **OK (OK)** pour enregistrer le groupe d'applications.

**STEP 2 |** Créez une règle de sécurité pour autoriser les services SNMP.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et cliquez sur **Add (Ajouter)**.
2. Dans l'onglet **General (Général)**, saisissez un **Name (Nom)** pour la règle.
3. Dans les onglets **Source (Source)** et **Destination (Destination)**, cliquez sur **Add (Ajouter)**, puis saisissez une **Source Zone (Zone source)** et une **Destination Zone (Zone de destination)** pour le trafic.
4. Dans l'onglet **Applications (Applications)**, cliquez sur **Add (Ajouter)**, saisissez le nom du groupe d'applications que vous venez de créer, puis sélectionnez-le dans la liste déroulante.
5. Dans l'onglet **Actions (Actions)**, vérifiez que l'**Action (Action)** est définie sur **Allow (Autoriser)**, puis cliquez sur **OK (OK)** et sur **Commit (Valider)**.

## Surveillance des statistiques à l'aide de SNMP

Les statistiques collectées par un gestionnaire Simple Network Management Protocol (protocole simple de gestion réseau ; SNMP) sur les pare-feu Palo Alto Networks vous permettent d'évaluer l'état de santé de votre réseau (systèmes et connexions), d'identifier les limitations des ressources et de surveiller le trafic ou les charges de traitement. Les statistiques incluent des informations telles que les états d'interface (active ou inactive), les sessions utilisateur actives, les sessions simultanées, l'utilisation de la session, la température et la durée active du système.

*Vous ne pouvez pas configurer un gestionnaire SNMP pour contrôler des pare-feu Palo Alto Networks (à l'aide de messages SET), pour collecter uniquement des statistiques sur ceux-ci (à l'aide de messages GET). Pour plus d'informations sur la mise en œuvre de SNMP pour les pare-feu Palo Alto Networks, reportez-vous à la section* Prise en charge SNMP**.**

**STEP 1 |** Configurez le gestionnaire SNMP de manière à obtenir les statistiques des pare-feu.

Les étapes suivantes fournissent une vue d'ensemble des tâches que vous effectuez sur le gestionnaire SNMP. Pour les étapes spécifiques, reportez-vous à la documentation de votre gestionnaire SNMP.

1. Pour permettre au gestionnaire SNMP d'interpréter les statistiques de pare-feu, charger les MIBs pris en charge pour les appareils Palo Alto Networks et les compiler si nécessaire.
2. Pour chaque pare-feu que le gestionnaire SNMP surveillera, définissez les paramètres de connexion (adresse IP et port) et les paramètres d'authentification (chaîne de communauté SNMPv2c ou ID de moteur/nom d'utilisateur/mot de passe SNMPv3) du pare-feu.

   *Tous les pare-feux Palo Alto Networks utilisent le port 161.*

   Le gestionnaire SNMP peut utiliser les mêmes paramètres de connexion et d'authentification, ou des paramètres différents, pour plusieurs pare-feu. Les paramètres doivent correspondre à ceux que vous définissez lors de la configuration de SNMP sur le pare-feu (reportez-vous à l'étape 3). Par exemple, si vous utilisez SNMPv2c, la chaîne de communauté que vous définissez lors de la configuration du pare-feu doit correspondre à la chaîne de communauté que vous définissez sur le gestionnaire SNMP de ce pare-feu.
3. Déterminez les identifiants d'objets (OID) des statistiques que vous souhaitez surveiller. Par exemple, pour surveiller le pourcentage d'utilisation de session d'un

périphérique, un navigateur MIB indique que cette statistique correspond à l'OID 1.3.6.1.4.1.25461.2.1.2.3.1.0 dans PAN-COMMON-MIB.my. Pour plus d'informations, consultez Utilisation d'un gestionnaire SNMP pour explorer les MIBs et les objets.

4. Configurez le gestionnaire SNMP de manière à surveiller les OIDs souhaitées.

**STEP 2 |** Activez le trafic SNMP sur une interface de pare-feu.

Il s'agit de l'interface qui recevra les requêtes de statistiques du gestionnaire SNMP.

*PAN-OS ne synchronise pas les paramètres de l'interface de gestion (MGT) pour les pare-feu dans une configuration High Availability (haute disponibilité ; HA). Vous devez configurer l'interface de chaque homologue HA.*

Effectuez cette étape dans l'interface Web du pare-feu.

- Pour activer le trafic SNMP sur l'interface MGT, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)**, modifiez l'interface de **Management (Gestion)**, sélectionnez **SNMP**, puis cliquez sur **OK** sur et **Commit (Valider)**.
- Pour activer le trafic SNMP sur les autres interfaces, créez un profil de gestion d'interface pour les services SNMP et attribuez le profil à l'interface qui recevra les requêtes SNMP. Le type d'interface doit être Ethernet Couche 3.

**STEP 3 |** Configurez le pare-feu pour qu'il réponde aux requêtes de statistiques d'un gestionnaire SNMP.

*PAN-OS ne synchronise pas les paramètres de réponse SNMP pour les pare-feu dans une configuration High Availability (haute disponibilité ; HA). Vous devez configurer ces paramètres pour chaque homologue HA.*

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)** puis, dans la section Miscellaneous (Divers), cliquez sur **SNMP Setup (Configuration SNMP)**.
2. Sélectionnez la **Version** de SNMP et configurez les valeurs d'authentification de la manière suivante. Pour les détails de version, consultez SNMP Support (support SNMP).
   - **V2c** : saisissez la **SNMP Community String (Chaîne de communauté SNMP)** qui identifie une communauté de gestionnaires SNMP et de périphériques surveillés, et qui sert de mot de passe pour authentifier les membres de la communauté entre eux.

     *Il convient de ne pas utiliser la chaîne de communauté par défaut, **`public`** ; elle est bien connue et donc non sûre.*
   - **V3**— créer au moins un groupe d'affichage SNMP et un utilisateur. Les comptes utilisateur et les vues fournissent l'authentification, la confidentialité et le contrôle d'accès lorsque des pare-feu transfèrent des pièges et que des gestionnaires SNMP obtiennent des statistiques de pare-feu.
     - **Vues** : chaque vue est constituée d'une paire OID et un masque de niveau bit : l'OID définit une MIB et le masque (au format hexadécimal) définit les objets qui sont accessibles à l'intérieur (incluant la correspondance) ou à l'extérieur (excluant correspondance) de cette MIB. Cliquez sur **Add (Ajouter)** dans la première liste et entrez un **Name (nom)** pour le groupe de vues. Pour chaque vue dans le groupe, cliquez sur **Add (Ajouter)** et configurer la vue **Name (nom)**, **OID (OID)**,

correspondant à **Option (Option)** (**include (inclure)** ou **exclude (exclure)**) et **Mask (masque)**.

- **Utilisateurs**: Cliquez sur **Add (Ajouter)** dans la deuxième liste, entrez un nom d'utilisateur sous **Users (Utilisateurs)**, sélectionnez le groupe **View (Affichage)** dans la liste déroulante, saisissez le mot de passe d'authentification (**Auth Password (Mot de passe d'authentification)**) utilisé pour s'authentifier sur le gestionnaire SNMP, puis saisissez le mot de passe de confidentialité (**Priv Password (Mot de passe de confidentialité)**) utilisé pour crypter les messages SNMP vers le gestionnaire SNMP.

3. Cliquez sur **OK**, puis sur **Commit (Valider)**.

**STEP 4 |** Surveillez les statistiques du pare-feu à l'aide d'un gestionnaire SNMP.

Reportez-vous à la documentation de votre gestionnaire SNMP pour les détails.

*Lorsque vous surveillez des statistiques liées aux interfaces du pare-feu, vous devez faire correspondre les index d'interfaces dans le gestionnaire SNMP avec les noms d'interfaces dans l'interface Web du pare-feu. Pour obtenir de plus amples précisions, reportez-vous à la section* Identifiants d'interface de pare-feu dans les gestionnaires SNMP et les collecteurs NetFlow.

## Transfert des pièges de pare-feu à un gestionnaire SNMP

Les pièges Simple Network Management Protocol (protocole simple de gestion réseau ; SNMP) peuvent vous alerter d'événements système (défaillances ou modifications matérielles ou logicielles de pare-feu Palo Alto Networks) ou de menaces (trafic correspondant à une règle de sécurité de pare-feu) qui demandent une attention immédiate.

*Pour afficher la liste des pièges pris en charge par les pare-feu Palo Alto Networks, utilisez le gestionnaire SNMP pour accéder à la MIB panCommonEventEventsV2. Pour plus d'informations, consultez* Utilisation d'un gestionnaire SNMP pour explorer les MIBs et les objets.

*Pour plus d'informations sur la mise en œuvre de SNMP par les pare-feu Palo Alto Networks, reportez-vous à la section* support SNMP.

**STEP 1 |** Activez le gestionnaire SNMP pour interpréter les pièges qu'il reçoit.

Chargez les MIB pris en charge pour les pare-feu de Palo Alto Networks et, le cas échéant, compilez-les. Pour les étapes spécifiques, reportez-vous à la documentation de votre gestionnaire SNMP.

**STEP 2 |** Configurez un profil de serveur SNMP Trap.

Le profil définit comment le pare-feu accède aux gestionnaires SNMP (serveurs de pièges). Vous pouvez définir jusqu'à quatre gestionnaires SNMP pour chaque profil.

*(Facultatif) Configurez plusieurs profils de serveurs de pièges SNMP pour différents types de journaux, niveaux de gravité et verdicts WildFire.*

1. Connectez-vous à l'interface Web du pare-feu.
2. Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveur)** > **SNMP Trap (Piège SNMP)**.

3. Cliquez sur **Add (Ajouter)** et entrez un **Name (Nom)** pour le profil.
4. Si le pare-feu comporte plusieurs systèmes virtuels (vsys), sélectionnez le **Location(Emplacement)** (vsys ou **Shared (Partagé)**) où ce profil est disponible.
5. Sélectionnez la **Version** de SNMP et configurez les valeurs d'authentification de la manière suivante. Pour les détails de version, consultez SNMP Support (support SNMP).

   - **V2c (V2c)** : pour chaque serveur, cliquez sur **Add (Ajouter)** et saisissez le **Name (Nom)** de serveur, l'adresse IP ((**SNMP Manager (Gestionnaire SNMP)** ainsi que la **Community String (Chaîne de communauté)**. La chaîne de communauté identifie une communauté de gestionnaires SNMP et de périphériques surveillés, et sert de mot de passe pour authentifier les membres de la communauté entre eux.

     *Il convient de ne pas utiliser la chaîne de communauté par défaut, **`public`** ; elle est bien connue et donc non sûre.*

   - **V3 (V3)** : pour chaque serveur, cliquez sur **Add (Ajouter)** et entrez le **Name (Nom)** de serveur, l'adresse IP (SNMP Manager (Gestionnaire SNMP)), le compte User (Utilisateur) SNMP (il doit correspondre à un nom d'utilisateur défini dans le gestionnaire SNMP), le **SNMP Manager (Gestionnaire SNMP)**), le compte **User (Utilisateur)** SNMP (il doit correspondre à un nom d'utilisateur défini dans le gestionnaire SNMP), le **EngineID (ID de moteur)** utilisé pour identifier de manière unique le pare-feu (vous pouvez laisser ce champ vide pour utiliser le numéro de série du pare-feu), le mot de passe d'authentification (**Auth Password (Mot de passe d'authentification)**) utilisé pour s'authentifier au serveur, et le mot de passe de confidentialité (**Priv Password (Mot de passe de confidentialité)**) utilisé pour crypter les messages SNMP vers le serveur.
6. Cliquez sur **OK** pour enregistrer le profil de serveur.

**STEP 3 |** Configurez le transfert des journaux.

1. Configurez les destinations des pièges du trafic, des menaces et WildFire :
   1. Création d'un profil de transfert des journaux. Pour chaque type de journal et chaque niveau de gravité ou verdict WildFire, sélectionnez le profil de serveur **SNMP Trap (Piège SNMP)**.
   2. Affectation du profil de transfert des journaux aux règles de politique et aux zones réseau. Les règles et les zones déclencheront la génération et le transfert de pièges.
2. Configurez les destinations des journaux système, de configuration, de User-ID, de correspondance HIP et de corrélation. Pour chaque type de journal (piège) et niveau de gravité, sélectionnez le profil de serveur **SNMP Trap (Piège SNMP)**.
3. Cliquez sur **Commit (Valider)**.

**STEP 4 |** Surveillez les pièges à l'aide d'un gestionnaire SNMP.

Reportez-vous à la documentation de votre gestionnaire SNMP.

*Lorsque vous surveillez des pièges liés aux interfaces du pare-feu, vous devez faire correspondre les index d'interfaces dans le gestionnaire SNMP avec les noms d'interfaces dans l'interface Web du pare-feu. Pour obtenir de plus amples précisions, reportez-vous à la section* Identifiants d'interface de pare-feu dans les gestionnaires SNMP et les collecteurs NetFlow.

# MIB prises en charge

Le tableau suivant dresse la liste des Management Information Base (base d'informations de gestion ; MIB) Simple Network Management Protocol (protocole simple de gestion réseau ; SNMP) que les pare-feu, Panorama et les équipement WF-500 Palo Alto Networks prennent en charge. Vous devez charger ces MIB dans votre gestionnaire SNMP pour surveiller les objets (statistiques et pièges systèmes) définis dans les MIB. Pour plus d'informations, consultez Utilisation d'un gestionnaire SNMP pour explorer les MIBs et les objets.

| Type de MIB | MIB prises en charge |
|---|---|
| **Standard** : l'Internet Engineering Task Force (IETF) gère la plupart des MIB standard. Vous pouvez télécharger les MIB sur le site Web de l'IETF.<br><br>*Les pare-feu, Panorama et les équipements WF-500 Palo Alto Networks ne prennent pas en charge tous les objets (OID) de chacune de ces MIB. Reportez-vous aux liens des MIB prises en charges pour obtenir une vue d'ensemble des OID pris en charge.* | MIB-II<br>IF-MIB<br>HOST-RESOURCES-MIB<br>ENTITY-MIB<br>ENTITY-SENSOR-MIB<br>ENTITY-STATE-MIB<br>MIB LAG IEEE 802.3<br>LLDP-V2-MIB.my<br>BFD-STD-MIB |
| **Entreprise** : vous pouvez télécharger les MIB d'entreprise sur le portail de Documentation Technique de Palo Alto Networks. | PAN-COMMON-MIB.my<br>PAN-GLOBAL-REG-MIB.my<br>PAN-GLOBAL-TC-MIB.my<br>PAN-LC-MIB.my<br>PAN-PRODUCT-MIB.my<br>PAN-ENTITY-EXT-MIB.my |

| Type de MIB | MIB prises en charge |
|---|---|
| | PAN-TRAPS.my |

## MIB-II

MIB-II fournit des identifiants d'objets (OID) pour des protocoles de gestion réseau dans des réseaux TCP/IP. Utilisez cette MIB pour surveiller des informations générales sur les systèmes et les interfaces. Par exemple, vous pouvez analyser des tendances d'utilisation de bande passante par type d'interface (objet ifType) pour déterminer si le pare-feu a besoin de plus d'interfaces de ce type pour supporter les pics de volume de trafic.

Les pare-feu, Panorama et les équipements WF-500 Palo Alto Networks ne prennent en charge que les groupes d'objets suivants :

| Groupe d'objets | Description |
|---|---|
| système | Fournit des informations sur le système comme le modèle de matériel, la durée active du système, le FQDN et l'emplacement physique. |
| Interfaces | Fournit des statistiques pour des interfaces physiques et logiques comme le type, la bande passante actuelle (vitesse), l'état opérationnel (par exemple, active ou inactive) et les paquets ignorés. La prise en charge d'interface logique inclut les tunnels VPN, les groupes agrégés, les sous-interfaces de Couche 2, les sous-interfaces de Couche 3, les interfaces en boucle et les interfaces VLAN. |

RFC 1213 définit cette MIB.

## IF-MIB

IF-MIB prend en charge des types d'interfaces (physiques et logiques) et des compteurs plus importants (64K) en plus de ceux définis dans MIB-II. Utilisez cette MIB pour surveiller les statistiques d'interface en plus de celles proposées par MIB-II. Par exemple, pour surveiller la bande passante actuelle d'interfaces à vitesse élevée (plus de 2,2 Gbits/s) comme les interfaces 10G des pare-feu PA-5200 Series, vous devez vérifier l'objet ifHighSpeed d'IF-MIB plutôt que l'objet ifSpeed de MIB-II. Les statistiques d'IF-MIB peuvent être utiles lors de l'évaluation de la capacité de votre réseau.

Les pare-feu, Panorama et les équipements WF-500 Palo Alto Networks prennent uniquement en charge ifXTable d'IF-MIB, qui fournit des informations sur l'interface comme le nombre de paquets multicast et de diffusion transmis et reçus, si une interface est en mode de promiscuité, et si une interface est dotée d'un connecteur physique.

RFC 2863 définit cette MIB.

## HOST-RESOURCES-MIB

HOST-RESOURCES-MIB fournit des informations pour les ressources d'ordinateur hôte. Utilisez cette MIB pour surveiller des statistiques d'utilisation du processeur et de la mémoire. Par exemple,

le fait de vérifier la charge du processeur actuelle (objet hrProcessorLoad) peut vous permettre de résoudre des problèmes de performances sur le pare-feu.

Les pare-feu, Panorama et les équipements WF-500 de Palo Alto Networks prennent en charge des parties des groupes d'objets suivants :

| Groupe d'objets | Description |
|---|---|
| hrDevice | Fournit des informations comme la charge du processeur, la capacité de stockage et la taille de la partition. Les OID hrProcessorLoad fournissent une moyenne des cœurs traitant les paquets.<br>Pour les pare-feux des séries PA-7000 et PA-5200, qui ont plusieurs plans de données (DP), vous pouvez surveiller l'utilisation de chaque processeur de plan de données. Définissez des alertes lorsque l'utilisation atteint un seuil spécifique pour chaque processeur DP afin d'éviter les problèmes de disponibilité du service. |
| hrSystem | Fournit des informations comme la durée active du système, le nombre de sessions utilisateur actuelles et le nombre de processus actuels. |
| hrStorage | Fournit des informations comme la quantité de stockage utilisé. |

RFC 2790 définit cette MIB.

## ENTITY-MIB

ENTITY-MIB fournit les OID de plusieurs composants logiques et physiques. Utilisez cette MIB pour déterminer les composants physiques chargés sur un système (par exemple, les ventilateurs et les sondes de température) et consultez des informations liées comme les modèles et les numéros de série. Vous pouvez également utiliser les numéros d'index de ces composants pour déterminer leur état opérationnel dans ENTITY-SENSOR-MIB et ENTITY-STATE-MIB.

Les pare-feu, Panorama et les équipements WF-500 Palo Alto Networks ne prennent en charge que des parties du groupe entPhysicalTable :

| object | Description |
|---|---|
| entPhysicalIndex | Un espace de noms unique qui inclut les logements de disques et les disques durs. |
| entPhysicalDescr | La description du composant. |
| entPhysicalVendorType | Le sysObjectID (reportez-vous à la section PAN-PRODUCT-MIB.my) si disponible (objets de châssis et module). |
| entPhysicalContainedIn | La valeur entPhysicalIndex du composant contenant ce composant. |
| entPhysicalClass | Le châssis (3), le conteneur (5) d'un logement, le bloc d'alimentation (6), le ventilateur (7), la sonde (8) de chaque température ou autre |

| object | Description |
|---|---|
| | caractéristique environnementale, et le module (9) de chaque carte de ligne. |
| entPhysicalParentRelPos | La position relative de ce composant ***enfant*** parmi ses composants ***frères et sœurs***. Les composants frères et sœurs sont définis comme des composants entPhysicalEntry partageant les mêmes valeurs d'instance de chacun des objets entPhysicalContainedIn et entPhysicalClass. |
| entPhysicalName | Pris en charge uniquement si l'interface de gestion (MGT) autorise la dénomination de la carte de ligne. |
| entPhysicalHardwareRev | La révision matérielle spécifique au fournisseur du composant. |
| entPhysicalFirwareRev | La révision du micrologiciel spécifique au fournisseur du composant. |
| entPhysicalSoftwareRev | La révision logicielle spécifique au fournisseur du composant. |
| entPhysicalSerialNum | Le numéro de série spécifique au fournisseur du composant. |
| entPhysicalMfgName | Le nom du fabricant du composant. |
| entPhysicalMfgDate | La date de fabrication du composant. |
| entPhysicalModelName | Le numéro de modèle de disque. |
| entPhysicalAlias | Un alias spécifié par le gestionnaire du réseau pour le composant. |
| entPhysicalAssetID | Un identifiant de suivi d'actif attribué à l'utilisateur, spécifié par le gestionnaire du réseau pour le composant. |
| entPhysicalIsFRU | Indique si le composant est une Field Replaceable Unit (unité remplaçable sur site - FRU). |
| entPhysicalUris | Le numéro Common Language Equipment Identifier (identifiant d'équipement en langage commun - CLEI) du composant (par exemple, URN:CLEI:CNME120ARA). |

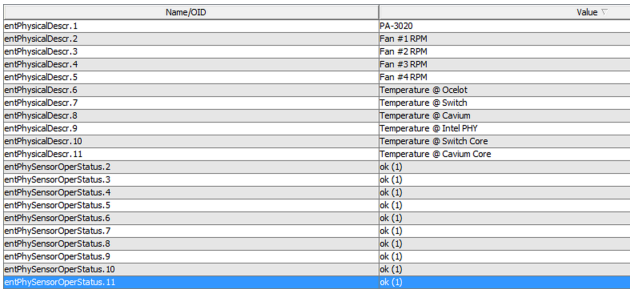
RFC 4133 définit cette MIB.

## ENTITY-SENSOR-MIB

ENTITY-SENSOR-MIB ajoute la prise en charge des sondes physiques pour l'équipement de mise en réseau en plus de ce qu'ENTITY-MIB définit. Utilisez cette MIB avec ENTITY-MIB pour surveiller l'état opérationnel des composants physiques d'un système (par exemple, les ventilateurs et les sondes de température). Par exemple, pour résoudre des problèmes pouvant être dus aux conditions environnementales, vous pouvez faire correspondre les index d'entité d'ENTITY-MIB (objet entPhysicalDescr) aux valeurs d'état opérationnel (objet entPhysSensorOperStatus) d'ENTITY-

SENSOR-MIB. Dans l'exemple suivant, tous les ventilateurs et toutes les sondes de température d'un pare-feu PA-3020 sont opérationnels :



| Name/OID | Value |
|---|---|
| entPhysicalDescr.1 | PA-3020 |
| entPhysicalDescr.2 | Fan #1 RPM |
| entPhysicalDescr.3 | Fan #2 RPM |
| entPhysicalDescr.4 | Fan #3 RPM |
| entPhysicalDescr.5 | Fan #4 RPM |
| entPhysicalDescr.6 | Temperature @ Ocelot |
| entPhysicalDescr.7 | Temperature @ Switch |
| entPhysicalDescr.8 | Temperature @ Cavium |
| entPhysicalDescr.9 | Temperature @ Intel PHY |
| entPhysicalDescr.10 | Temperature @ Switch Core |
| entPhysicalDescr.11 | Temperature @ Cavium Core |
| entPhySensorOperStatus.2 | ok (1) |
| entPhySensorOperStatus.3 | ok (1) |
| entPhySensorOperStatus.4 | ok (1) |
| entPhySensorOperStatus.5 | ok (1) |
| entPhySensorOperStatus.6 | ok (1) |
| entPhySensorOperStatus.7 | ok (1) |
| entPhySensorOperStatus.8 | ok (1) |
| entPhySensorOperStatus.9 | ok (1) |
| entPhySensorOperStatus.10 | ok (1) |
| entPhySensorOperStatus.11 | ok (1) |

***Le même OID peut faire référence à différentes sondes sur des plates-formes variées. Utilisez ENTITY-MIB pour que la plate-forme ciblée corresponde à la valeur de la description.***

Les pare-feu, Panorama et les équipements WF-500 Palo Alto Networks ne prennent en charge que des parties du groupe entPhySensorTable. Les parties prises en charge varient selon la plate-forme et comprennent uniquement les sondes thermiques (températures en Celsius) et de ventilateur (en tr/min.).

RFC 3433 définit ENTITY-SENSOR-MIB.

## ENTITY-STATE-MIB

ENTITY-STATE-MIB fournit des informations sur l'état de composants physique en plus de ce qu'ENTITY-MIB définit, notamment l'état administratif et opérationnel de composants de plates-formes sur châssis. Utilisez cette MIB avec ENTITY-MIB pour surveiller l'état opérationnel des composants d'un pare-feu PA-7000 Series (par exemple, les cartes de ligne, les tiroirs de ventilation et les blocs d'alimentation). Par exemple, pour résoudre des problèmes liés au transfert des journaux des menaces, vous pouvez faire correspondre les index de Log Processing Card (carte de traitement des journaux - LPC) d'ENTITY-MIB (objet entPhysicalDescr) aux valeurs d'état opérationnel (objet entStateOper) d'ENTITY-STATE-MIB. Les valeurs d'état opérationnel utilisent des nombres pour indiquer l'état : 1 pour inconnu, 2 pour désactivé, 3 pour activé et 4 pour test. Les pare-feu PA-7000 Series sont les seuls pare-feu Palo Alto Networks à prendre en charge cette MIB.

RFC 4268 définit ENTITY-STATE-MIB.

## MIB LAG IEEE 802.3

Utilisez la MIB IEEE 802.3 LAG pour surveiller l'état des groupes agrégés pour lesquels Link Aggregation Control Protocol (LACP in an Aggregate Interface Group (LACP dans un groupe d'interfaces agrégées)) est activé. Lorsque le pare-feu consigne des événements LACP, il génère également des pièges utiles au dépannage. Par exemple, les pièges peuvent vous indiquer si des interruptions de trafic entre le pare-feu et un homologue LACP ont été dues à une perte de connectivité ou à une différence de valeurs de vitesse et de duplex d'interface.

PAN-OS met en œuvre les tables SNMP suivantes pour LACP.

***L'objet dot3adTablesLastChanged indique l'heure de la dernière modification apportée à dot3adAggTable, dot3adAggPortListTable et à dot3adAggPortTable.***

| Table | Description |
|---|---|
| Table de configuration de l'agrégateur (dot3adAggTable) | Cette table contient des informations sur chaque groupe agrégé associé à un pare-feu. Chaque groupe agrégé inclut une entrée.<br>Certains d'objet de la table présentent des restrictions, qui sont décrites par l'objet dot3adAggIndex. Cet index correspond à l'identifiant unique que le système local affecte au groupe agrégé. Il identifie une instance de groupe agrégé par les objets gérés subordonnés de l'objet contenant. L'identifiant est en lecture seule.<br>***La MIB ifTable (une liste d'entrées d'interface) ne prend pas en charge les interfaces logiques, et n'inclut donc pas d'entrée de groupe agrégé.*** |
| Table de liste de ports d'agrégation (dot3adAggPortListTable) | Cette table dresse la liste des ports associés à chaque groupe agrégé d'un pare-feu. Chaque groupe agrégé inclut une entrée.<br>L'attribut dot3adAggPortListPorts répertorie l'ensemble complet de ports associés à un groupe agrégé. Chaque jeu de bits de la liste représente un membre de port. Pour les plates-formes non sur châssis, il s'agit d'une valeur 64 bits. Pour les plates-formes sur châssis, la valeur est un ensemble de huit entrées 64 bits. |
| Table de ports d'agrégation (dot3adAggPortTable) | Cette table contient des informations de configuration LACP sur chaque port associé à un groupe agrégé d'un pare-feu. Chaque port inclut une entrée. La table n'inclut pas d'entrées pour les ports non associés à un groupe agrégé. |
| Table de statistiques LACP (dot3adAggPortStatsTable) | Cette table contient des informations d'agrégation de lien sur chaque port associé à un groupe agrégé d'un pare-feu. Chaque port inclut une ligne. La table n'inclut pas d'entrées pour les ports non associés à un groupe agrégé. |

La MIB LAG IEEE 802.3 inclut les pièges liés à LACP suivants :

| Nom du piège | Description |
|---|---|
| panLACPLostConnectivityTrap | L'homologue a perdu la connectivité au pare-feu. |
| panLACPUnresponsiveTrap | L'homologue ne répond pas au pare-feu. |
| panLACPNegoFailTrap | La négociation LACP avec l'homologue a échoué. |
| panLACPSpeedDuplexTrap | Les paramètres de vitesse de liaison et de duplex sur le pare-feu et l'homologue ne correspondent pas. |
| panLACPLinkDownTrap | Une interface du groupe agrégé est inactive. |

| Nom du piège | Description |
|---|---|
| panLACPLacpDownTrap | Une interface a été supprimée du groupe agrégé. |
| panLACPLacpUpTrap | Une interface a été ajoutée au groupe agrégé. |

Pour les définitions de la MIB, reportez-vous à IEEE 802.3 LAG MIB.

## LLDP-V2-MIB.my

Utilisez LLDP-V2-MIB pour surveiller les événements Link Layer Discovery Protocol (protocole de découverte de la couche de liaison (LLDP). Par exemple, vous pouvez vérifier l'objet lldpV2StatsRxPortFramesDiscardedTotal pour connaître le nombre de trames LLDP ignorées pour une quelconque raison. Le pare-feu Palo Alto Networks utilise LLDP pour détecter les périphériques voisins et leurs fonctionnalités. LLDP facilite la résolution des problèmes, en particulier pour les déploiements de câble virtuel où les utilitaires ping et traceroute ne détectent pas le pare-feu.

Les pare-feu Palo Alto Networks prennent en charge tous les objets LLDP-V2-MIB sauf :

- Les objets lldpV2Statistics suivants :
  - lldpV2StatsRemTablesLastChangeTime
  - lldpV2StatsRemTablesInserts
  - lldpV2StatsRemTablesDeletes
  - lldpV2StatsRemTablesDrops
  - lldpV2StatsRemTablesAgeouts
- Les objets lldpV2RemoteSystemsData suivants :
  - La table lldpV2RemOrgDefInfoTable
  - Dans la table lldpV2RemTable : lldpV2RemTimeMark

RFC 4957 définit cette MIB.

## BFD-STD-MIB

Servez-vous de la MIB de la Bidirectional Forwarding Detection (détection de transfert bidirectionnel ; BFD) pour surveiller et recevoir des alertes d'échec concernant le chemin bidirectionnel qui existe entre deux moteurs d'acheminement, comme des interfaces, des liaisons de données ou les moteurs en tant que tel. Par exemple, vous pouvez vérifier l'objet bfdSessState pour connaître l'état d'une session BFD entre des moteurs d'acheminement. Dans l'implémentation Palo Alto Networks, l'un des moteurs d'acheminement est une interface de pare-feu et l'autre est un homologue BFD adjacent qui a été configuré.

RFC 7331 définit cette MIB.

## PAN-COMMON-MIB.my

Utilisez PAN-COMMON-MIB pour surveiller les informations suivantes des pare-feu, de Panorama et des équipements WF-500 Palo Alto Networks :

| Groupe d'objets | Description |
|---|---|
| panSys | Contient des objets tels que les versions logicielle/matérielle du système, les versions de contenu dynamiques, le numéro de série, le mode/l'état HA et les compteurs généraux.<br><br>Les compteurs généraux incluent les compteurs liés au Denial of Service (déni de service ; DoS), la fragmentation IP, l'état TCP et les paquets abandonnés. Le suivi de ces compteurs vous permet de surveiller les irrégularités de trafic résultant d'attaques DoS, de pannes de système ou de connexion, ou de limitations des ressources. PAN-COMMON-MIB prend en charge les compteurs généraux pour les pare-feu mais pas pour Panorama. |
| panChassis | Type de châssis et mode d'appareil M-Series (Panorama ou Collecteur de journaux). |
| panSession | Informations d'utilisation de session. Par exemple, le nombre total de sessions actives sur le pare-feu ou un système virtuel spécifique. |
| panMgmt | État de la connexion entre le pare-feu et le serveur de gestion Panorama. |
| panGlobalProtect | Utilisation de la passerelle GlobalProtect en pourcentage, nombre maximum de tunnels autorisés et nombre de tunnels actifs. |
| panLogCollector | Les statistiques de journalisation pour chaque collecteur de journaux, y compris le taux de journalisation, les quotas de journal, l'utilisation du disque, les périodes de rétention, les redondance de journal (activé ou désactivé), l'état de transfert des pare-feux aux collecteur de journaux, l'état de transfert des collecteurs de journaux aux services externes, et l'état des connexions du pare-feu au collecteur de journaux. |
| panDeviceLogging | Les statistiques de journalisation pour chaque pare-feu, y compris le taux de journalisation, l'utilisation du disque, les périodes de rétention, l'état de transfert des pare-feux individuels vers Panorama et les serveurs externes et l'état des connexions du pare-feu au collecteur de journaux. |

## PAN-GLOBAL-REG-MIB.my

PAN-GLOBAL-REG-MIB.my contient des définitions d'OID de niveau supérieur générales pour diverses sous-arborescences de modules MIB d'entreprise Palo Alto Networks. Cette MIB ne contient pas d'objets que vous pouvez surveiller ; elle est requise uniquement pour être référencée par d'autres MIB.

## PAN-GLOBAL-TC-MIB.my

PAN-GLOBAL-TC-MIB.my définit des conventions (par exemple, la longueur de caractère et les caractères autorisés) des valeurs de texte d'objets de modules MIB d'entreprise Palo Alto Networks. Tous les produits Palo Alto Networks utilisent ces conventions. Cette MIB ne contient pas d'objets que vous pouvez surveiller ; elle est requise uniquement pour être référencée par d'autres MIB.

## PAN-LC-MIB.my

PAN-LC-MIB.my contient des définitions d'objets gérés que les Collecteurs de journaux (appareils M-Series en mode Collecteur de journaux) mettent en œuvre. Utilisez cette MIB pour surveiller le taux de journalisation, la durée de stockage de la base de données de journaux (en jours) et l'utilisation de disque (en Mo) de chaque disque logique (jusqu'à quatre) sur un collecteur de journaux. Par exemple, vous pouvez utiliser ces informations pour déterminer si vous devez ajouter plus de collecteurs de journaux ou transférer les journaux à un serveur externe (un serveur Syslog par exemple) à des fins d'archivage.

## PAN-PRODUCT-MIB.my

PAN-PRODUCT-MIB.my définit des OID sysObjectID pour tous les produits Palo Alto Networks. Cette MIB ne contient pas d'objets que vous pouvez surveiller ; elle est requise uniquement pour être référencée par d'autres MIB.

## PAN-ENTITY-EXT-MIB.my

Utilisez PAN-ENTITY-EXT-MIB.my avec ENTITY-MIB pour surveiller la consommation énergétique des composants physiques d'un pare-feu PA-7000 Series (par exemple, les tiroirs de ventilation et les blocs d'alimentation), qui est le seul pare-feu Palo Alto Networks à prendre en charge cette MIB. Par exemple, lors de la résolution de problèmes liés au transfert des journaux, vous souhaiterez peut-être vérifier la consommation énergétique des Log Processing Cards (cartes de traitement des journaux - LPC) : vous pouvez faire correspondre les index LCP d'ENTITY-MIB (objet entPhysicalDescr) aux valeurs de PAN-ENTITY-EXT-MIB (objet panEntryFRUModelPowerUsed).

## PAN-TRAPS.my

Utilisez PAN-TRAPS.my pour consulter la liste complète de tous les pièges générés et leurs informations (une description par exemple). Pour obtenir la liste des pièges pris en charge par les pare-feu, par Panorama et par les équipements WF-500 Palo Alto Networks, reportez-vous à l'objet PAN-COMMON-MIB.my **panCommonEvents** > **panCommonEventsEvents** > **panCommonEventEventsV2**.

# Transfert des journaux vers une destination HTTP/S

Le pare-feu et Panorama™ peuvent transférer des journaux vers un serveur HTTP/S. Lorsqu'un événement se produit, vous pouvez choisir de transférer tous les journaux ou certains journaux pour déclencher une action sur un service HTTP externe. Lorsque vous transférez des journaux vers un serveur HTTP, configurez le pare-feu pour qu'il envoie directement une requête API HTTP à un service tiers afin de déclencher une action en fonction des attributs qui figurent dans le journal du pare-feu. Vous pouvez configurer le pare-feu pour qu'il fonctionne avec tout service HTTP qui expose une API et vous pouvez modifier l'URL, l'en-tête HTTP, les paramètres et la charge utile dans la requête HTTP pour répondre à vos besoins d'intégration.

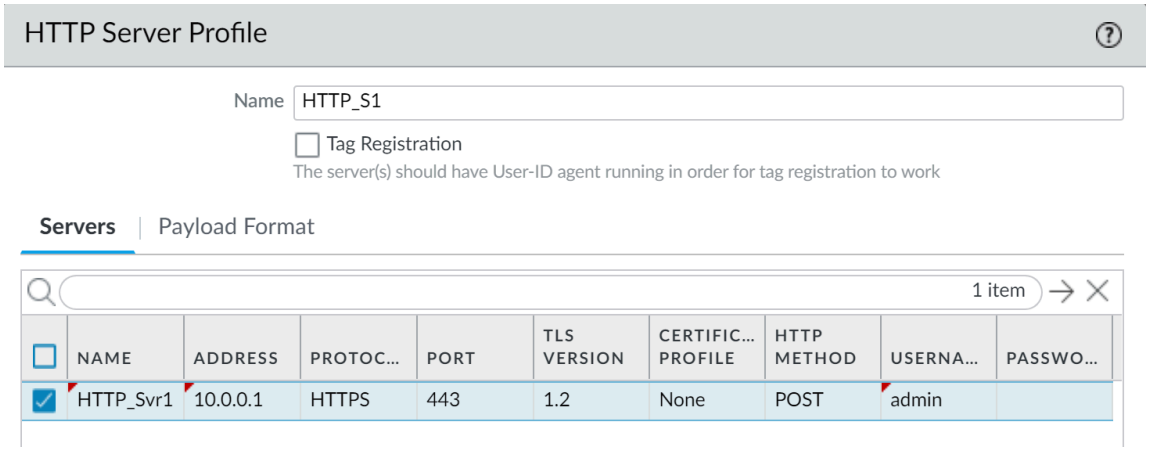
**STEP 1 |** Créez un profil de serveur HTTP pour transférer des journaux vers une destination HTTP/S.

Le profil de serveur HTTP vous permet d'indiquer la manière d'accéder au serveur et de définir le format à utiliser pour le transfert des journaux vers une destination HTTP/S. Par défaut, le pare-feu utilise le port de gestion pour transférer ces journaux. Vous pouvez toutefois affecter une adresse IP et une interface source différentes sous **Device (Périphérique)** > **Setup (Configuration)** > **Services (Services)** > **Service Route Configuration (Configuration de l'itinéraire de service)**.

1. Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveur)** > **HTTP** et **Add (Ajoutez)** un nouveau profil.
2. Donnez un **Name (Nom)** au profil de serveur et sélectionnez un **Location (Emplacement)**. Le profil peut être **Shared (Partagé)** par tous les systèmes virtuels ou appartenir à un système virtuel donné.
3. **Add (Ajoutez)** les détails de chaque serveur. Chaque profil peut comporter un maximum de quatre serveurs.
4. Entrez un **Name (Nom)** et une **Address (Adresse IP)**.
5. Sélectionnez le **Protocol (Protocole)** (**HTTP** ou **HTTPS**). Le **Port** par défaut est 80 ou 443, respectivement ; mais vous pouvez modifier le numéro de port pour qu'il corresponde au port d'écoute de votre serveur HTTP.
6. Sélectionnez la **TLS Version (Version TLS)** prise en charge sur le serveur : **1.0**, **1.1**, or **1.2** (par défaut).
7. Sélectionnez le **Certificate Profile (Profil de certificat)** à utiliser pour la connexion TLS avec le serveur.
8. Sélectionnez la **HTTP Method (Méthode HTTP)** que le service tiers prend en charge : **DELETE**,**GET**, **POST** (par défaut) ou **PUT**.
9. (Facultatif) Saisissez le **Username (Nom d'utilisateur)** et le **Password (Mot de passe)**) pour l'authentification auprès du serveur, au besoin.

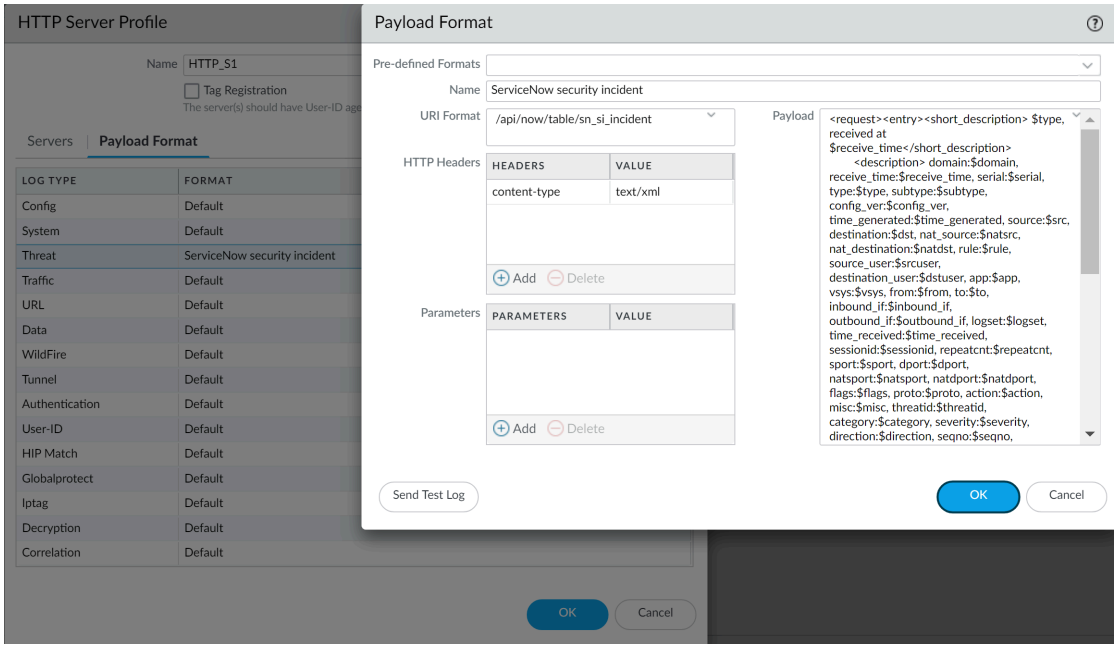
10. (Facultatif) Sélectionnez **Test Server Connection (Tester la connexion au serveur)** pour vérifier la connectivité réseau entre le pare-feu et le serveur HTTP/S.




**STEP 2 |** Sélectionnez le **Payload Format (Format de la charge)** de la requête HTTP.

1. Sélectionnez le lien **Log Type (Type de journal)** de chaque type de journal dont vous souhaitez définir le format de requête HTTP.
2. Sélectionnez les **Pre-defined Formats (Formats prédéfinis)** (disponibles via les mises à jour de contenu) ou créez un format personnalisé.

   Si vous créez un format personnalisé, l'**URI (URI)** est le terminal de ressource pour le service HTTP. Le pare-feu ajoute l'URI à l'adresse IP que vous avez définie précédemment pour construire l'URL de la requête HTTP. Assurez-vous que le format de l'URI et de la charge utile correspond à la syntaxe requise par votre fournisseur tiers. Vous pouvez utiliser n'importe quel attribut pris en charge sur le type de journal sélectionné dans l'en-tête HTTP, les paramètres, les paires de valeurs et la charge utile requise.



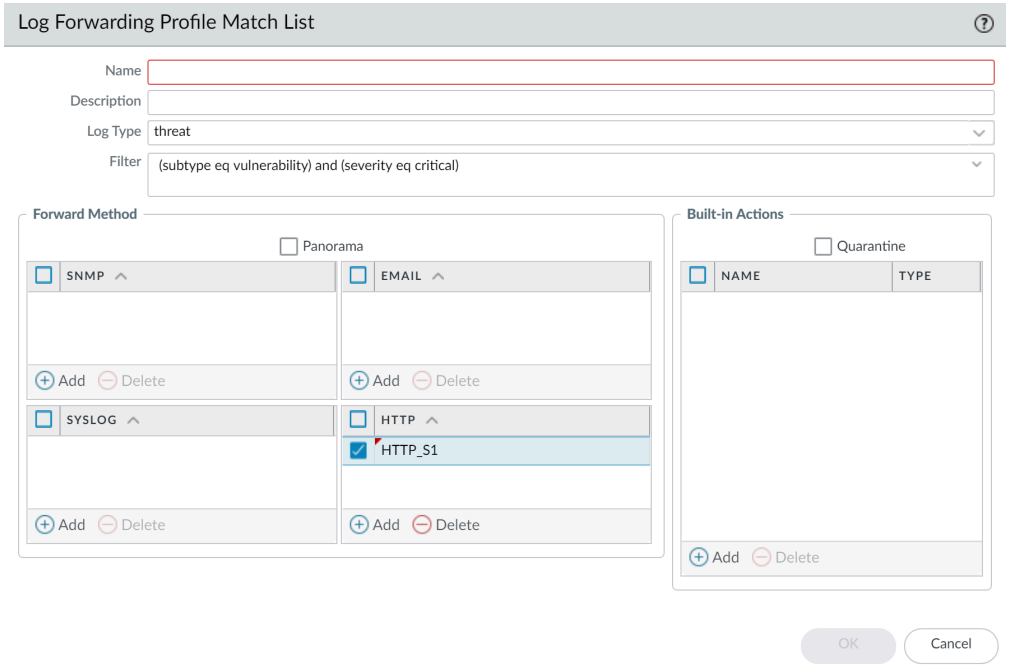

3. **Send Test Log (Envoyer un journal de test)** pour vérifier que le serveur HTTP reçoit la requête. Lorsque vous envoyez interactivement un journal de test, le pare-feu utilise le

format tel quel et ne remplace pas la variable par une valeur tirée du journal du pare-feu. Si votre serveur HTTP envoie une réponse 404, indiquez des valeurs aux paramètres pour que le serveur puisse traiter la requête avec succès.

**STEP 3 |** Définissez les critères de correspondance qui détermineront les situations où le pare-feu transférera les journaux au serveur HTTP et associez le profil de serveur HTTP à utiliser.

1. Sélectionnez les types de journaux pour lesquels vous souhaitez qu'un flux de travail soit déclenché :
   - Ajoutez un profil de transfert des journaux (**Objects (Objets)** > **Log Forwarding (Transfert des journaux)**) aux journaux qui concernent l'activité des utilisateurs (par exemple, journaux du trafic, des menaces ou d'authentification).
   - Sélectionnez **Device (Périphérique)** > **Log Settings (Paramètres des journaux)** pour les journaux qui concernent les événements système, comme les journaux système ou de configuration.
2. Sélectionnez le type de journal et utilisez le nouveau **Filter Builder (Générateur de filtres)** pour définir les critères de correspondance.
3. **Add (Ajoutez)** le profil de serveur HTTP pour transférer des journaux vers une destination HTTP.



# Surveillance de NetFlow

NetFlow est un protocole du secteur que le pare-feu peut utiliser pour exporter des statistiques sur le trafic IP entrant dans ses interfaces. Le pare-feu exporte les statistiques sous forme de champs NetFlow vers un collecteur NetFlow. Le collecteur NetFlow est un serveur que vous utilisez pour analyser le trafic réseau pour la sécurité, l'administration, la comptabilité et le dépannage. Tous les pare-feu de Palo Alto Networks prennent en charge la version 9 de NetFlow. Les pare-feu ne prennent en charge que le protocole NetFlow unidirectionnel, et non bidirectionnel. Les pare-feu effectuent le traitement de NetFlow sur tous les paquets IP des interfaces et ne prennent pas en charge le NetFlow échantillonné. Vous pouvez exporter des enregistrements NetFlow pour les interfaces Niveau3, Niveau 2, câble virtuel, tap, VLAN, loopback et tunnel. Pour les sous-interfaces Ethernet agrégées, vous pouvez exporter les sous-interfaces individuelles via lesquelles les données transitent dans le groupe. Pour identifier les interfaces de pare-feu d'un collecteur NetFlow, reportez-vous à la section Identifiants d'interface de pare-feu dans les gestionnaires SNMP et les collecteurs NetFlow. Les pare-feu prennent en charge les Modèles NetFlow standards et d'entreprise (propres à PAN-OS), qui sont utilisés par les collecteurs NetFlow pour déchiffrer les champs NetFlow.

- Configuration des exportations NetFlow
- Modèles NetFlow

## Configuration des exportations NetFlow

Si vous souhaitez utiliser un collecteur NetFlow pour analyser le trafic réseau sur les interfaces entrantes du pare-feu, suivez les étapes suivantes pour configurer l'exportation des enregistrements NetFlow.

**STEP 1 |** Créez un profil de serveur NetFlow.

Le profil définit les collecteurs NetFlow qui recevront les enregistrements exportés et précise les paramètres d'exportation.

1. Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveur)** > **NetFlow (NetFlow)** et **Add (Ajoutez)** un profil.
2. Saisissez un **Name (Nom)** pour identifier le profil.
3. Spécifiez la fréquence à laquelle le pare-feu actualise les modèles NetFlow en **Minutes (Minutes)** (par défaut 30) ou en **Packets (Paquets)** (pour les enregistrements exportés,

la valeur par défaut est 20), selon les exigences de votre collecteur NetFlow. Le pare-feu actualise les modèles après que le seuil est dépassé.

4. Spécifiez le **Active Timeout (Délai d'expiration actif)**, c'est-à-dire la fréquence en minutes à laquelle le pare-feu exporte les enregistrements (par défaut 5).
5. Sélectionnez **PAN-OS Field Types (Types de champs PAN-OS)** si vous souhaitez que le pare-feu exporte les champs App-ID et User-ID.
6. **Add (Ajoutez)** chaque collecteur NetFlow (maximum de deux par profil) qui recevra les enregistrements. Spécifiez les éléments suivants pour chaque collecteur :
   - Le **Name (Nom)** qui permet d'identifier le collecteur.
   - Le nom d'hôte ou l'adresse IP du **NetFlow Server (Serveur NetFlow)**.
   - Le **Port (Port)** d'accès (par défaut 2055).
7. Cliquez sur **OK** pour enregistrer le profil.

**STEP 2 |** Associez le profil de serveur NetFlow aux interfaces du pare-feu lorsque le trafic que vous souhaitez analyser entre.

Dans cet exemple, vous associez le profil à une interface Ethernet existante.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)** et cliquez sur le nom d'une interface pour la modifier.

   *Vous pouvez exporter des enregistrements NetFlow pour les interfaces Niveau3, Niveau 2, câble virtuel, tap, VLAN, loopback et tunnel. Pour les interfaces Ethernet agrégées, vous pouvez exporter les sous-interfaces individuelles via lesquelles les données transitent dans le groupe.*
2. Sélectionnez le profil de serveur NetFlow (**NetFlow Profile (Profil NetFlow**) que vous avez configuré et cliquez sur **OK (OK)**.

**STEP 3 |** **(Obligatoire pour les pare-feu PA-7000 Series, PA-5400 Series et PA-5400 Series)** Configurez un itinéraire de service pour l'interface que le pare-feu utilisera pour envoyer les enregistrements NetFlow.

Vous ne pouvez utiliser l'interface de gestion (MGT) pour envoyer les enregistrements NetFlow à partir des pare-feu PA-7000 Series, PA-5400 et PA-5400 Series. Un itinéraire de service est facultatif pour les autres modèles de pare-feu. Pour tous les pare-feu, il n'est pas nécessaire que l'interface qui envoie les enregistrements NetFlow soit celle pour laquelle le pare-feu recueille les enregistrements.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Services**

2. **(Pare-feu ayant des systèmes virtuels multiples)** Sélectionnez l'une des options suivantes :
   - **Global (Global)** : sélectionnez cette option si l'itinéraire de service s'applique à tous les systèmes virtuels du pare-feu.
   - **Virtual Systems (Systèmes virtuels)** : sélectionnez cette option si l'itinéraire de service s'applique à un système virtuel donné. Définissez le **Location (Emplacement)** sur le système virtuel.
3. Sélectionnez **Service Route Configuration (Configuration de l'itinéraire de service)** et personnalisez-le.
4. Sélectionnez le protocole (**IPv4 (IPv4)** ou **IPv6 (IPv6)**) que l'interface utilise. Au besoin, vous pouvez configurer l'itinéraire de service des deux protocoles.
5. Cliquez sur **NetFlow (NetFlow)** dans la colonne Service (Service).
6. Sélectionner la **Source Interface (Interface source)**.

   ***Any (Indifférent)**, **Use default (Utiliser les paramètres par défaut)** et **MGT (MGT)** ne sont pas des options d'interface valides pour l'envoi des enregistrements NetFlow à partir des pare-feu PA-7000 Series, PA-5400 Series ou PA-5200..*
7. Sélectionnez une **Source Address (Adresse source)** (adresse IP).
8. Cliquez deux fois sur **OK** pour enregistrer vos modifications.

**STEP 4 |** **Commit (Validez)** vos modifications.

**STEP 5 |** Surveillez le trafic du pare-feu à l'aide d'un collecteur NetFlow.

Reportez-vous à la documentation de votre collecteur NetFlow.

*Lorsque vous surveillez des statistiques, vous devez faire correspondre les index d'interfaces dans le collecteur NetFlow avec les noms d'interfaces dans l'interface Web du pare-feu. Pour obtenir de plus amples précisions, reportez-vous à la section* Identifiants d'interface de pare-feu dans les gestionnaires SNMP et les collecteurs NetFlow.

Pour résoudre des problèmes d'envoi NetFlow, utilisez la commande de la CLI suivante : **`debug log-receiver netflow statistics`**.

## Modèles NetFlow

Les collecteurs NetFlow utilisent des modèles pour déchiffrer les champs exportés par le pare-feu. Le pare-feu choisit un modèle en fonction du type de données exportées : trafic IPv4 ou IPv6, avec ou sans NAT, et avec des champs (spécifiques à PAN-OS) standard ou entreprise. Le pare-feu actualise régulièrement les modèles pour réévaluer le modèle à utiliser (en cas de changement du type de données exportées) et pour appliquer les modifications nécessaires aux champs du modèle sélectionné. Lorsque vous procédez à la Configuration des exportations NetFlow, définissez le taux d'actualisation en fonction d'un intervalle de temps et un nombre d'enregistrements exportés respectant les exigences de votre collecteur NetFlow. Le pare-feu actualise les modèles après que le seuil est dépassé.

Le pare-feu Palo Alto Networks prend en charge les modèles NetFlow suivants :

| Modèle | ID |
|---|---|
| Norme IPv4 | 256 |
| IPv4 Enterprise | 257 |
| Norme IPv6 | 258 |
| IPv6 Enterprise | 259 |
| IPv4 avec NAT Standard | 260 |
| IPv4 avec NAT Enterprise | 261 |
| IPv6 avec NAT Standard | 262 |
| IPv6 avec NAT Enterprise | 263 |

Le tableau suivant répertorie les champs NetFlow que le pare-feu peut envoyer, ainsi que le modèle qui les définit :

| Valeu | Champ | Description | Modèles |
|---|---|---|---|
| 1 | IN_BYTES | Compteur entrant avec une longueur de N * 8 bits pour le nombre d'octets associés à un flux IP. La valeur par défaut de N est 4. | Tous les modèles |
| 2 | IN_PKTS | Compteur entrant avec une longueur de N * 8 bits pour le nombre de paquets associés à un flux IP. La valeur par défaut de N est 4. | Tous les modèles |
| 4 | PROTOCOL | Octet du protocole IP. | Tous les modèles |
| 5 | TOS | Paramètre d'octet du type de service d'entrée de l'interface d'entrée. | Tous les modèles |
| 6 | TCP_FLAGS | Total de tous les indicateurs TCP de ce flux. | Tous les modèles |
| 7 | L4_SRC_PORT | Numéro de port source TCP/UDP (par exemple, FTP, Telnet ou équivalent). | Tous les modèles |

| Valeu | Champ | Description | Modèles |
|---|---|---|---|
| 8 | IPV4_SRC_ADDR | Adresse source IPv4 | À la norme IPv4<br>IPv4 Enterprise<br>IPv4 avec NAT Standard<br>IPv4 avec NAT Enterprise |
| 10 | INPUT_SNMP | Index d'interface d'entrée. La valeur de longueur par défaut est de 2 octets, mais des valeurs supérieures sont possibles. Pour obtenir plus de précisions sur la manière dont les pare-feu Palo Alto Networks génèrent des index d'interface, reportez-vous à la section Identifiants d'interface de pare-feu dans les gestionnaires SNMP et les collecteurs NetFlow. | Tous les modèles |
| 11 | L4_DST_PORT | Numéro de port de destination TCP/UDP (par exemple, FTP, Telnet ou équivalent). | Tous les modèles |
| 12 | IPV4_DST_ADDR | Adresse de destination IPv4 | À la norme IPv4<br>IPv4 Enterprise<br>IPv4 avec NAT Standard<br>IPv4 avec NAT Enterprise |
| 14 | OUTPUT_SNMP | Index d'interface de sortie. La valeur de longueur par défaut est de 2 octets, mais des valeurs supérieures sont possibles. Pour obtenir plus de précisions sur la manière dont les pare-feu Palo Alto Networks génèrent des index d'interface, reportez-vous à la section Identifiants d'interface de pare-feu dans les gestionnaires SNMP et les collecteurs NetFlow. | Tous les modèles |

| Valeu | Champ | Description | Modèles |
|---|---|---|---|
| 21 | LAST_SWITCHED | Durée active du système, en millisecondes, lors du basculement du dernier paquet de ce flux. | Tous les modèles |
| 22 | FIRST_SWITCHED | Durée active du système, en millisecondes, lors du basculement du premier paquet de ce flux. | Tous les modèles |
| 27 | IPV6_SRC_ADDR | Adresse source IPv6 | Norme IPv6<br>IPv6 Enterprise<br>IPv6 avec NAT Standard<br>IPv6 avec NAT Enterprise |
| 28 | IPV6_DST_ADDR | Adresse de destination IPv6 | Norme IPv6<br>IPv6 Enterprise<br>IPv6 avec NAT Standard<br>IPv6 avec NAT Enterprise |
| 32 | ICMP_TYPE | Type de paquet Internet Control Message Protocol (protocole de message de contrôle Internet ; ICMP). Il est rapporté sous la forme suivante :<br>Type ICMP * 256 + code ICMP | Tous les modèles |
| 61 | DIRECTION | Sens du flux :<br>• 0 = entrée<br>• 1 = sortie | Tous les modèles |
| 148 | flowId | Identifiant d'un flux unique dans un domaine d'observation. Vous pouvez utiliser cet élément d'information pour distinguer différents flux si des clés de flux comme des adresses IP et des numéros de ports sont rapportées ou non dans des enregistrements distincts. Le flowID (l'identifiant de flux) correspond au champ | Tous les modèles |

| Valeu | Champ | Description | Modèles |
|---|---|---|---|
| | | d'identifiant de session dans les journaux de trafic et de menace. | |
| 233 | firewallEvent | Indique un événement de pare-feu :<br>• 0 = Ignorer (invalide) : Non utilisé.<br>• 1 = Flux créé : L'enregistrement de données NetFlow est destiné à un nouveau flux.<br>• 2 = Flux supprimé : L'enregistrement de données NetFlow correspond à la fin d'un flux.<br>• 3 = Flux refusé : L'enregistrement de données NetFlow indique un flux refusé par la politique de pare-feu.<br>• 4 = Alerte de flux : Non utilisé.<br>• 5 = Mise à jour du flux : l'enregistrement de données NetFlow est envoyé pour un flux de ***longue durée***, qui est un flux qui dure plus longtemps que l'intervalle du **Active Timeout (délai d'attente de l'activité)** configuré dans le Profil du serveur NetFlow. | Tous les modèles |
| 225 | postNATSourceIPv4Address | La définition de cet élément d'information est identique à celle de sourceIPv4Address, à l'exception qu'il rapporte une valeur modifiée produite par le pare-feu pendant la traduction d'adresse réseau après que le paquet a traversé l'interface. | IPv4 avec NAT Standard<br>IPv4 avec NAT Enterprise |
| 226 | postNATDestinationIPv4Address | La définition de cet élément d'information est identique à celle de destinationIPv4Address, à l'exception qu'il rapporte une valeur modifiée produite par le pare-feu pendant la traduction d'adresse réseau après que le paquet a traversé l'interface. | IPv4 avec NAT Standard<br>IPv4 avec NAT Enterprise |

| Valeu | Champ | Description | Modèles |
|---|---|---|---|
| 227 | postNAPTSourceTransportPort | La définition de cet élément d'information est identique à celle de sourceTransportPort, à l'exception qu'il rapporte une valeur modifiée produite par le pare-feu pendant la traduction de port d'adresse réseau après que le paquet a traversé l'interface. | IPv4 avec NAT Standard<br>IPv4 avec NAT Enterprise |
| 228 | postNAPTDestinationTransportPort | La définition de cet élément d'information est identique à celle de destinationTransportPort, à l'exception qu'il rapporte une valeur modifiée produite par le pare-feu pendant la traduction de port d'adresse réseau après que le paquet a traversé l'interface. | IPv4 avec NAT Standard<br>IPv4 avec NAT Enterprise |
| 281 | postNATSourceIPv6Address | La définition de cet élément d'information est identique à la définition de l'élément d'information sourceIPv6Address, à l'exception qu'il rapporte une valeur modifiée produite par le pare-feu pendant la traduction d'adresse réseau NAT64 après que le paquet a traversé l'interface. Reportez-vous à RFC 2460 pour la définition du champ d'adresse source dans l'en-tête IPv6. Reportez-vous à RFC 6146 pour la spécification NAT64. | IPv6 avec NAT Standard<br>IPv6 avec NAT Enterprise |
| 282 | postNATDestinationIPv6Address | La définition de cet élément d'information est identique à la définition de l'élément d'information destinationIPv6Address, à l'exception qu'il rapporte une valeur modifiée produite par le pare-feu pendant la traduction d'adresse réseau NAT64 après que le paquet a traversé l'interface. Reportez-vous à RFC 2460 pour la définition du champ d'adresse de destination dans l'en-tête IPv6. Reportez-vous à RFC 6146 pour la spécification NAT64. | IPv6 avec NAT Standard<br>IPv6 avec NAT Enterprise |

| Valeu | Champ | Description | Modèles |
|---|---|---|---|
| 346 | privateEnterpriseNumber | Il s'agit d'un numéro d'entreprise privée unique identifiant Palo Alto Networks : 25461. | IPv4 Enterprise<br>IPv4 avec NAT Enterprise<br>IPv6 Enterprise<br>IPv6 avec NAT Enterprise |
| 56701 | App-ID | Nom d'une application identifiée par un App-ID. Le nom peut comporter jusqu'à 32 octets. | IPv4 Enterprise<br>IPv4 avec NAT Enterprise<br>IPv6 Enterprise<br>IPv6 avec NAT Enterprise |
| 56702 | User-id | Nom d'utilisateur identifié par un User-ID. Le nom peut comporter jusqu'à 64 octets. | IPv4 Enterprise<br>IPv4 avec NAT Enterprise<br>IPv6 Enterprise<br>IPv6 avec NAT Enterprise |

# Identifiants d'interface de pare-feu dans les gestionnaires SNMP et les collecteurs NetFlow

Lorsque vous utilisez un collecteur NetFlow (reportez-vous à la section Surveillance de NetFlow) ou un gestionnaire SNMP (reportez-vous à la section Surveillance et pièges SNMP)) pour surveiller le pare-feu Palo Alto Networks, un index d'interface (objet ifindex SNMP) identifie l'interface qui a transporté un flux spécifique (reportez-vous à la section Index d'interfaces dans un gestionnaire SNMP). Au contraire, l'interface Web du pare-feu utilise des noms d'interfaces comme identifiants (par exemple, ethernet1/1), et non des index. Pour savoir quelles statistiques affichées dans un collecteur NetFlow ou un gestionnaire SNMP s'appliquent à telle interface de pare-feu, vous devez faire correspondre les index d'interfaces et les noms d'interfaces.

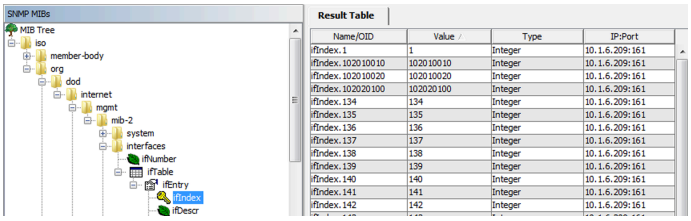



**Figure 3: Index d'interfaces dans un gestionnaire SNMP**

Vous pouvez faire correspondre les index aux noms grâce aux formules utilisées par le pare-feu pour calculer les index. Les formules varient en fonction de la plate-forme et du type d'interface : physique ou logique.

La plage d'index d'interfaces physiques est comprise entre 1 et 9999, que le pare-feu calcule comme suit :

| Plate-forme de pare-feu | Calcul | Exemple d'index d'interface |
|---|---|---|
| VM-Series | Nombre de ports de gestion + décalage de port physique<br>• **Nombre de ports de gestion** : constante de 1.<br>• **Décalage de port physique** : numéro de port physique. | Pare-feu VM-100, Eth1/4 =<br>1 (nombre de ports de gestion) + 4 (ports physiques) = **5** |
| PA-220, PA-220R, PA-800 Series | Nombre de ports de gestion + décalage de port physique<br>• **Nombre de ports de gestion** : constante de 5.<br>• **Décalage de port physique** : numéro de port physique. | Pare-feu PA-5200 Series, Eth1/4 =<br>5 (nombre de ports de gestion) + 4 (ports physiques) = **9** |
| PA-3200 Series, PA-5200 Series | Nombre de ports de gestion + décalage de port physique | Pare-feu PA-5200 Series, Eth1/4 = |

| Plate-forme de pare-feu | Calcul | Exemple d'index d'interface |
|---|---|---|
| | • **Nombre de ports de gestion** : constante de 4.<br>• **Décalage de port physique** : numéro de port physique. | 4 (nombre de ports de gestion) + 4 (ports physiques) = **8** |
| PA-7000 Series | (ports max. * logement) + décalage de port physique + nombre de ports de gestion<br>• **Ports maximum** : constante de 64.<br>• **Logement** : numéro de logement châssis de la carte d'interface réseau.<br>• **Décalage de port physique** : numéro de port physique.<br>• **Nombre de ports de gestion** : constante de 5. | Pare-feu PA-7000 Series, Eth3/9 =<br>[64 (ports max.) * 3 (logements)] + 9 (ports physiques) + 5 (nombre de ports de gestion) = **206** |

Les index d'interfaces logiques pour toutes les plates-formes sont des nombres à 9 chiffres que le pare-feu calcule comme suit :

| Type d'interfac | Intervalle | Chiffr | Chiffres 7 | Chiffres 5 | Chiffres 1-4 | Exemple d'index d'interface |
|---|---|---|---|---|---|---|
| Sous-interface de niveau 3 | 101010001 et 199999999. | Type : 1 | Logement de l'interface : 1-9 (01-09) | Port de l'interface : 1-9 (01-09) | Sous-interface : suffixe 1-9999 (0001-9999) | Eth1/5.22 = 100000000 (type) + 100000 (logement) + 50000 (port) + 22 (suffixe) = **101050022** |
| Sous-interface de couche 2 | 101010001 et 199999999. | Type : 1 | Logement de l'interface : 1-9 (01-09) | Port de l'interface : 1-9 (01-09) | Sous-interface : suffixe 1-9999 (0001-9999) | Eth2/3.6 = 100000000 (type) + 200000 (logement) + 30000 (port) + 6 (suffixe) = **102030006** |
| Sous-interface câble virtuel | 101010001 et 199999999. | Type : 1 | Logement de l'interface : 1-9 (01-09) | Port de l'interface : 1-9 (01-09) | Sous-interface : suffixe 1-9999 (0001-9999) | Eth4/2.312 = 100000000 (type) + 400000 (logement) + 20000 (port) + 312 (suffixe) = **104020312** |

| Type d'interfac | Intervalle | Chiffre | Chiffres 7 | Chiffres 5 | Chiffres 1-4 | Exemple d'index d'interface |
|---|---|---|---|---|---|---|
| Réseau local virtuel | 200000001 et 200009999. | Type : 2 | 00 | 00 | Suffixe VLAN : 1-9999 (0001-9999) | VLAN.55 = 200000000 (type) + 55 (suffixe) = **200000055** |
| en boucle | 300000001-300009999 | Type : 3 | 00 | 00 | Suffixe de connexion en boucle : 1-9999 (0001-9999) | Connexion en boucle.55 = 300000000 (type) + 55 (suffixe) = **300000055** |
| Tunnel | 400000001-400009999 | Type : 4 | 00 | 00 | Suffixe de tunnel : 1-9999 (0001-9999) | Tunnel.55 = 400000000 (type) + 55 (suffixe) = **400000055** |
| Groupe agrégé | 500010001-500089999 | Type : 5 | 00 | Suffixe AE : 1-8 (01-08) | Sous-interface : suffixe 1-9999 (0001-9999) | AE5.99 = 500000000 (type) + 50000 (suffixe AE) + 99 (suffixe) = **500050099** |

# Surveillance des émetteurs-récepteurs

Vous pouvez surveiller l'état des émetteurs-récepteurs de votre appareil ou périphérique physique afin de faciliter l'installation et le dépannage. Les diagnostics qui peuvent être visualisés sont le courant de polarisation transmis, la puissance transmise, la puissance reçue, la température de l'émetteur-récepteur et la tension d'alimentation. Consultez ci-dessous la liste des dispositifs qui prennent en charge la surveillance des émetteurs-récepteurs.

- PA-800 Series
- PA-3200 Series
- PA-5200 Series
- PA-7000 Series

Utilisez l'interface de ligne de commande pour exécuter la surveillance de l'émetteur-récepteur. Consultez le tableau suivant pour toutes les commandes CLI disponibles.

*Si vous exécutez des commandes sur un émetteur-récepteur incompatible, la CLI renvoie « n/a » pour toute information de diagnostic qu'elle ne peut pas lire.*

| CLI | Definition |
|---|---|
| `show transceiver <interface name>` | Consultez un résumé de l'émetteur-récepteur spécifié avec les valeurs pour chaque diagnostic.<br>Exemple :<br>`admin@PA-7080> show transceiver ethernet11/25`<br>La CLI renvoie des valeurs pour la température, la tension, le courant, la puissance d'émission et la puissance de réception. |
| `show transceiver-detail <interface name>` | Recevez des spécifications plus détaillées sur l'émetteur-récepteur, y compris des informations sur les fournisseurs et la longueur des liens. La CLI fournira également des informations diagnostiques plus détaillées. |
| `show transceiver all` | Consultez la liste de tous les émetteurs-récepteurs actifs ainsi qu'un résumé de chacun de leurs diagnostics. |
| `show transceiver-detail all` | Obtenez des détails complets sur chaque émetteur-récepteur du périphérique. |

# User-id

L'identité de l'utilisateur, contrairement à l'adresse IP, fait partie intégrante d'une infrastructure de sécurité efficace. Le fait de savoir précisément qui utilise chacune des applications de votre réseau, qui a potentiellement introduit une menace ou qui transfert des fichiers, permet de renforcer vos règles de sécurité et de réduire les délais de réponse aux incidents. User-ID™, une fonctionnalité standard sur les pare-feu Palo Alto Networks vous permet de tirer parti des informations utilisateur stockées dans un large éventail de référentiels. Les rubriques suivantes fournissent plus d'informations sur User-ID et sa configuration :

# Présentation de User-ID

User-ID™ vous permet d'identifier tous les utilisateurs sur votre réseau à l'aide de diverses techniques afin de pouvoir identifier des utilisateurs à tous les emplacements en utilisant diverses méthodes d'accès et systèmes d'exploitation, dont Microsoft Windows, Apple iOS, Mac OS, Android, et Linux®/UNIX. Savoir qui sont vos utilisateurs au lieu de simplement avoir leur adresse IP offre les avantages suivants :

- **Visibilité** : Une meilleure visibilité sur l'utilisation des applications du point de vue des utilisateurs offre une idée plus précise de l'activité réseau. La puissance de l'User-ID devient évidente lorsque vous remarquez une application étrange ou inconnue sur votre réseau. Le cas échéant, votre équipe de sécurité peut, grâce à ACC ou au visualiseur de fichiers journaux, identifier l'application, connaître l'identité de l'utilisateur, la bande passante consommée, la session utilisée, ainsi que l'origine et la destination du trafic qui transite par cette application, ainsi que toute menace correspondante.
- **Contrôle de politique** : Lier les informations utilisateur aux règles de la politique de sécurité améliore la mise en œuvre sécuritaire des applications traversant le réseau et garantit que seuls les utilisateurs ayant besoin d'une application à des fins professionnelles y ont accès. Par exemple, certaines applications, comme les applications SaaS qui autorisent l'accès aux services de Ressources humaines (tels que Workday ou Service Now) doivent être disponibles à tous les utilisateurs connus de votre réseau. Toutefois, dans le cas d'applications plus sensibles, vous pouvez réduire votre surface d'attaque en vous assurant que seuls les utilisateurs qui ont besoin de ces applications puissent y accéder. Par exemple, le personnel de soutien informatique pourrait avoir besoin d'accéder, en toute légitimité, aux applications d'accès à des bureaux à distance ; ce n'est toutefois pas le cas de la majorité de vos utilisateurs.
- **Journalisation, génération de rapports et analyses** : Si un incident de sécurité se produit, une analyse des preuves accompagnée d'un rapport intégrant des informations sur les utilisateurs plutôt que de simples adresses IP fournit une image plus complète de l'incident. Par exemple, vous pouvez utiliser l'activité utilisateur/de groupe prédéfinie pour voir un résumé de l'activité Web d'utilisateurs individuels ou groupes d'utilisateurs, ou le rapport d'utilisation de l'application SaaS pour voir quels utilisateurs transfèrent le plus de données sur des applications SaaS non autorisées.

Pour appliquer les politiques basées sur l'utilisateur et le groupe, le pare-feu doit être en mesure de faire correspondre les adresses IP contenues dans les paquets qu'il reçoit avec des noms d'utilisateurs. User-ID fournit de nombreuses méthodes pour collecter ces informations de Mappage d'utilisateur. Par exemple, l'agent User-ID surveille les événements de connexion dans les journaux de serveur et écoute les messages Syslog des services d'authentification. Pour identifier les mappages des adresses IP non mappées par l'agent, vous pouvez configurer Politique d'authentification pour rediriger les requêtes HTTP vers une connexion au portail d'authentification. Vous pouvez adapter les mécanismes de mappage d'utilisateur pour correspondre à votre environnement, et même utiliser différents mécanismes sur différents sites pour vous assurer que vous accédez de façon sûre aux applications pour tous les utilisateurs, à tous les emplacements, à tout moment.

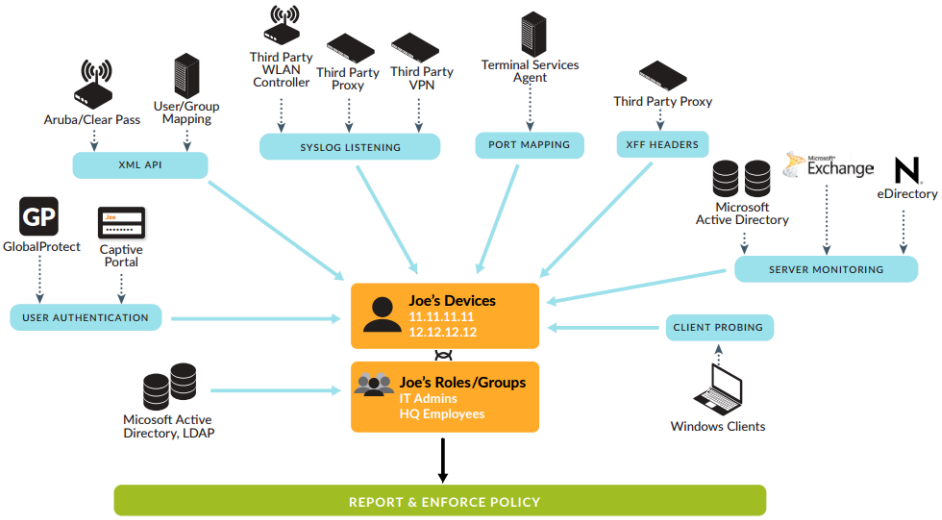



**Figure 4: User-id**

Pour activer l'application des politiques basée sur l'utilisateur et le groupe, le pare-feu requiert la liste de tous les utilisateurs disponibles et de leurs appartenances de groupe correspondantes pour que vous puissiez ensuite sélectionner les groupes lors de la définition de vos règles de politique. Le pare-feu collecte les informations de mappage de groupe en se connectant directement à votre serveur d'annuaire LDAP ou en utilisant l'intégration de l'API XML avec votre serveur d'annuaire.

Reportez-vous à la section Concepts de User-ID pour plus d'informations sur le fonctionnement de User-ID et à la section Activation de User-ID pour obtenir des instructions sur la configuration de User-ID.

*User-ID ne fonctionne pas dans les environnements où les adresses IP source des utilisateurs sont soumises à une traduction NAT avant que le pare-feu ne mappe les adresses IP aux noms d'utilisateurs.*

# Concepts de User-ID



## mappage de groupe

Pour définir des règles de politique basées sur l'utilisateur ou le groupe, vous créez tout d'abord un profil de serveur LDAP qui définit comment le pare-feu se connecte et s'authentifie auprès de votre serveur d'annuaire. Le pare-feu prend en charge divers serveurs d'annuaires, notamment Microsoft Active Directory (AD), Novell eDirectory et Sun ONE Directory Server. Le profil de serveur définit également comment le pare-feu recherche dans l'annuaire pour récupérer la liste des groupes et la liste des membres correspondante. Si vous utilisez un serveur d'annuaire qui n'est pas pris en charge nativement par le pare-feu, vous pouvez intégrer la fonction de mappage de groupe à l'aide de l'API XML. Vous pouvez ensuite créer une configuration de mappage de groupe pour procéder au Mappage d'utilisateurs à des groupes et à l'Activation d'une politique basée sur l'utilisateur et le groupe.

La définition de règles de politique basées sur l'appartenance à un groupe plutôt que sur des utilisateurs individuels simplifie l'administration car vous ne devez pas mettre à jour les règles lors de l'ajout de nouveaux utilisateurs à un groupe. Lors de la configuration d'un mappage de groupe, vous pouvez limiter les groupes disponibles dans des règles de politique. Vous pouvez préciser des groupes existant déjà dans votre service d'annuaires ou définir des groupes personnalisés sur la base de filtres LDAP. La définition de groupes personnalisés peut être plus rapide que la création de nouveaux groupes ou la modification de groupes existants sur un serveur LDAP. L'intervention d'un administrateur LDAP n'est en outre pas nécessaire. User-ID mappe tous les utilisateurs de l'annuaire LDAP correspondant au filtre du groupe personnalisé. Par exemple, vous souhaiterez peut-être disposer d'une politique de sécurité autorisant les sous-traitants du service marketing à accéder à des sites de réseaux sociaux. S'il n'existe aucun groupe Active Directory pour ce service, vous pouvez configurer un filtre LDAP mettant en correspondance les utilisateurs dont l'attribut LDAP Service est défini sur Marketing. Les requêtes de journal et les rapports basés sur un groupe d'utilisateurs incluront les groupes personnalisés.

## Mappage d'utilisateur

Connaître les noms d'utilisateur et de groupe n'est qu'une pièce du puzzle. Le pare-feu doit également connaître les adresses IP correspondant aux utilisateurs pour pouvoir appliquer les règles de sécurité de manière appropriée. Présentation de User-ID illustre les différentes méthodes utilisées pour identifier les utilisateurs et les groupes sur votre réseau ; elle indique comment le mappage d'utilisateur et le mappage de groupe fonctionnent conjointement pour permettre la visibilité et la mise en œuvre de la sécurité en fonction de l'utilisateur et du groupe. Les rubriques suivantes décrivent les différentes méthodes de mappage d'utilisateur :



- Politique d'authentification et portail d'authentification
- GlobalProtect
- Api XML
- Sondage du client

## Surveillance du serveur

Lors de la surveillance du serveur, un agent User-ID (un agent Windows exécuté sur un serveur de domaine de votre réseau, ou l'agent User-ID intégré à PAN-OS exécuté sur votre pare-feu) surveille les événements de connexion dans les journaux des événements de sécurité des serveurs Microsoft Exchange Servers, des Contrôleurs de Domaines ou des serveurs Novell eDirectory spécifiés. Par exemple, dans un environnement AD, vous pouvez configurer l'agent User-ID pour surveiller l'octroi ou le renouvellement de tickets Kerberos dans les journaux de sécurité, l'accès au serveur Exchange (si configuré), ainsi que les connexions aux services de fichiers et d'impressions. Pour que ces événements soient enregistrés dans le journal de sécurité, le domaine AD doit être configuré pour la journalisation des événements de connexion de compte. De plus, comme les utilisateurs peuvent se connecter à n'importe quel serveur du domaine, vous devez configurer la surveillance du serveur pour tous les serveurs afin de capturer tous les événements de connexion utilisateur. Pour plus d'informations, reportez-vous à la section Configuration du mappage d'utilisateur à l'aide de l'agent User-ID Windows ou Configuration du mappage d'utilisateur à l'aide de l'agent User-ID intégré à PAN-OS

## Mappage de port

Dans les environnements de systèmes multi-utilisateurs (Microsoft Terminal Server ou Citrix, par exemple), de nombreux utilisateurs partagent la même adresse IP. Dans ce cas, le processus de mappage d'adresse IP/nom d'utilisateur doit connaître le port source de chaque client. Pour procéder à ce type de mappage, vous devez installer l'agent Terminal Server Palo Alto Networks sur le serveur de terminaux Windows/Citrix afin de transmettre l'affectation des ports source aux divers processus utilisateur. Pour des serveurs de terminaux qui ne prennent pas en charge l'agent Terminal Server, tels que les serveurs de terminaux Linux, vous pouvez utiliser l'API XML pour envoyer des informations de mappage d'utilisateur relatifs aux événements de connexion et de déconnexion à User-ID. Pour plus d'informations sur la configuration, reportez-vous à la section Configuration du mappage d'utilisateur pour les utilisateurs de serveurs de terminaux.

## En-têtes XFF

Si vous disposez d'un serveur proxy déployé entre les utilisateurs de votre réseau et le pare-feu, ce dernier peut voir l'adresse IP du serveur proxy comme adresse IP source du trafic HTTP/HTTPS que le proxy transfère plutôt que l'adresse IP du client qui a demandé le contenu. Dans de nombreux cas, le serveur proxy ajoute un en-tête X-Forwarded-For (XFF) aux paquets de trafic, lequel contient l'adresse IPv4 ou IPv6 réelle du client qui a effectué la demande de contenu ou duquel elle provient. Dans de tels cas, vous pouvez configurer le pare-feu pour qu'il extraie l'adresse IP du XFF pour que l'agent User-ID puisse mapper l'adresse IP à un nom d'utilisateur. Cette façon de faire vous permet d'Utiliser les valeurs XFF pour les politiques et les utilisateurs sources de journalisation pour appliquer la politique basée sur les utilisateurs et ainsi autoriser en toute sécurité vos utilisateurs à accéder au Web derrière un serveur proxy.

## Insertion de l'en-tête du nom d'utilisateur

Lorsque vous configurez un périphérique d'application secondaire avec votre pare-feu Palo Alto Networks pour appliquer la politique basée sur les utilisateurs, le périphérique secondaire pourrait ne pas avoir le mappage nom d'utilisateur/adresse IP du pare-feu. Pour transmettre l'identité de l'utilisateur à des périphériques en aval, vous pourriez avoir besoin de déployer des périphériques supplémentaires, comme des proxys. De plus la transmission de l'identité pourrait nuire à l'expérience utilisateur (par exemple, les utilisateurs pourraient être forcés de se connecter à plusieurs reprises). Vous pouvez ajouter dynamiquement le domaine et le nom d'utilisateur à l'en-tête HTTP du trafic sortant de l'utilisateur et permettre ainsi aux périphériques secondaires que vous utilisez avec votre pare-feu Palo Alto Networks de recevoir les informations de l'utilisateur et d'appliquer la politique basée sur les utilisateurs. L'inclusion de l'identité de l'utilisateur en insérant le nom d'utilisateur et le domaine dans les en-têtes de trafic permet l'application de la politique basée sur les utilisateurs sans avoir de conséquences négatives sur l'expérience utilisateur ou sur le déploiement de l'infrastructure supplémentaire.

## Politique d'authentification et portail d'authentification

Dans certains cas, l'agent User-ID n'est pas en mesure de faire correspondre une adresse IP et un nom d'utilisateur au moyen de la surveillance du serveur ou de toute autre méthode. Par exemple, si l'utilisateur n'est pas connecté ou s'il utilise un système d'exploitation tel que Linux non pris en charge par vos serveurs de domaines. Dans d'autres cas, vous pourriez souhaiter que vos utilisateurs s'authentifient lorsqu'ils accèdent à des applications sensibles, quelles que soient les méthodes utilisées par l'agent User-ID pour effectuer le mappage d'utilisateur. Dans tous ces cas, vous pouvez procéder à la Configuration de la politique d'Authentification et configurer le Mappage d'adresses IP à des noms d'utilisateurs à l'aide du portail d'authentification. Tout trafic Web (HTTP ou HTTPS) qui correspond à une règle de politique d'authentification invite l'utilisateur à s'authentifier via le portail d'authentification. Vous pouvez utiliser les Méthodes d'authentification du portail d'authentification suivantes :

- Défi de navigation : utilisez l'ouverture de session unique Kerberos si vous souhaitez réduire le nombre de tentatives de connexions auxquelles les utilisateurs doivent répondre.
- Formulaire Web— Utilisez l'Authentification multifacteur, l'ouverture de session unique SAML, Kerberos, TACACS+, RADIUS, LDAP ou l'Authentification locale.
- Authentification du certificat client.

## Syslog

Votre environnement peut être doté de services réseau qui authentifient les utilisateurs. Des services tels que les contrôleurs sans fil, les périphériques 802.1x, les serveurs Apple Open Directory, les serveurs proxy et d'autres mécanismes Network Access Control (contrôle d'accès au réseau ; NAC), Vous pouvez configurer ces services afin qu'ils vous envoient des messages Syslog contenant des informations sur les événements de connexion et de déconnexion et configurer User-ID afin qu'il analyse ces messages. L'agent User-ID analyse les événements de connexion pour mapper des adresses IP à des noms d'utilisateurs et analyse les événements de déconnexion pour supprimer des mappages obsolètes. La suppression de mappages obsolètes est particulièrement utile dans les environnements où les affectations d'adresses IP changent souvent.

Aussi bien l'agent User-ID intégré à PAN-OS que l'agent User-ID Windows utilisent des filtres Syslog pour analyser des messages Syslog. Dans des environnements où les services envoient des messages dans des formats différents, vous pouvez créer un profil personnalisé pour chaque format et associer plusieurs profils à chaque expéditeur Syslog. Si vous utilisez l'agent User-ID intégré à PAN-OS, vous

pouvez également utiliser des filtres prédéfinis fournis par Palo Alto Networks à travers des mises à jour de contenu d'applications.

Les messages Syslog doivent respecter les critères suivants pour qu'un agent User-ID les analyse :

- Chaque message doit être une chaîne de texte sur une seule ligne. Les délimiteurs autorisés pour les sauts de ligne sont une nouvelle ligne (**\n**) ou un retour chariot plus une nouvelle ligne (**\r\n**).
- La taille maximum pour les messages individuels est de 8 000 octets.
- Les messages envoyés via UDP doivent être contenus dans un seul paquet ; les messages envoyés via SSL peuvent couvrir plusieurs paquets. Un seul paquet peut contenir plusieurs messages.

Pour plus d'informations sur la configuration, reportez-vous à la section Configuration de User-ID pour la surveillance des expéditeurs Syslog lors du mappage d'utilisateur.

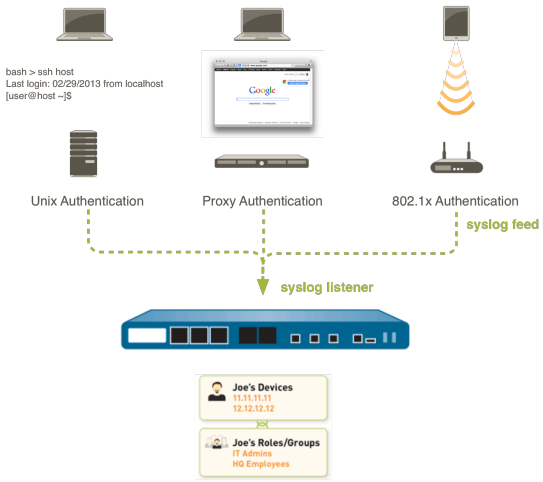



**Figure 5: Intégration de User-ID à Syslog**

## GlobalProtect

Pour les utilisateurs mobiles ou itinérants, les points de terminaison GlobalProtect fournissent directement les informations de mappage d'utilisateur au pare-feu. Dans ce cas, chaque utilisateur GlobalProtect doit saisir ses informations d'identification de connexion auprès du pare-feu pour accéder à une application en cours d'exécution sur le VPN. Ces informations de connexion sont ensuite ajoutées à la table de mappage d'utilisateur User-ID sur le pare-feu pour permettre la visibilité et la mise en œuvre de politiques de sécurité basées sur l'utilisateur. Comme les utilisateurs GlobalProtect doivent s'authentifier pour accéder au réseau, le mappage d'adresse IP/nom d'utilisateur est explicitement connu. Il s'agit de la meilleure solution dans les environnements sensibles où vous devez vous assurer de l'identité d'un utilisateur pour lui autoriser l'accès à une application ou un service. Pour plus d'informations sur la configuration de GlobalProtect, reportez-vous au Guide de l'administrateur GlobalProtect.

## Api XML

Le portail d'authentification et les autres méthodes standard de mappage d'utilisateur pourraient ne pas fonctionner pour certains types d'accès utilisateur. Par exemple, les méthodes standard ne peuvent ajouter le mappage des utilisateurs qui se connectent via une solution VPN tiers ou le

mappage des utilisateurs qui se connectent à un réseau sans fil sur lequel 802.1x est activé. Dans de tels cas, vous pouvez utiliser l'API XML PAN-OS pour capturer les événements de connexion et les envoyer à l'agent User-ID intégré à PAN-OS. Pour plus d'informations, reportez-vous à la sectionEnvoi de mappages d'utilisateurs à User-ID à l'aide de l'API XML.

## Sondage du client

***Palo Alto Networks recommande fortement de désactiver le sondage client car il ne s'agit pas d'une méthode recommandée pour obtenir des informations d'ID utilisateur dans un réseau de haute sécurité.***

Palo Alto Networks ne recommande pas d'utiliser le sondage client en raison des risques potentiels suivants :

- Étant donné que le sondage client fait confiance aux données renvoyées par le point de terminaison, il peut vous exposer à des risques de sécurité en cas de mauvaise configuration. Si vous l'activez sur des interfaces externes non approuvées, car cela provoquerait l'envoi des sondes client contenant des informations sensibles par l'agent en dehors de votre réseau, par exemple le nom d'utilisateur, le nom de domaine et le hachage du mot de passe du compte de service de l'agent User-ID. Si vous ne configurez pas correctement le compte de service, les informations d'identification pourraient être exploitées par un attaquant pour pénétrer le réseau afin d'obtenir un accès supplémentaire.
- Le sondage du client a été conçu pour les réseaux hérités sur lesquels la plupart des utilisateurs travaillaient sur des postes de travail Windows sur le réseau interne. Il est toutefois peu adapté aux réseaux modernes d'aujourd'hui qui prennent en charge une base d'utilisateurs mobiles et itinérants qui utilisent une diversité de périphériques et de systèmes d'exploitation.
- Le sondage client peut générer une grande quantité de trafic réseau (en fonction du nombre total d'adresses IP mappées).

Au lieu de cela, Palo Alto Networks recommande fortement d'utiliser les méthodes alternatives suivantes pour le mappage des utilisateurs :

- Utilisation de sources plus isolées et fiables, telles que des contrôleurs de domaine et des intégrations avec Syslog ou XML API (API XML), pour capturer en toute sécurité les informations de mappage des utilisateurs à partir de n'importe quel type de périphérique ou système d'exploitation.
- Configuration de la Authentication Policy and Authentication Portal (politique d'authentification et du portail d'authentification) pour vous assurer que vous n'autorisez l'accès qu'aux utilisateurs autorisés.

L'agent User-ID prend en charge deux types de sondage client :

- Sondage NetBIOS, qui utilise l'agent d'ID utilisateur Windows.
- Sondage WMI, qui utilise soit l'agent User-ID intégré PAN-OS, soit l'agent Windows User-ID.

***Le sondage client n'est pas recommandé comme méthode de mappage utilisateur, mais si vous prévoyez de l'activer, Palo Alto Networks recommande fortement d'utiliser le sondage WMI sur le sondage NetBIOS.***

Dans un environnement Microsoft Windows, vous pouvez configurer l'agent User-ID pour qu'il sonde les systèmes clients via Windows Management Instrumentation (WMI) ou le sondage

NetBIOS à des intervalles réguliers pour vérifier qu'un mappage d'utilisateur existant est toujours valide ou pour obtenir le nom d'utilisateur d'une adresse IP qui n'est toujours pas mappée.

Si vous décidez d'activer la fonction de sondage dans vos zones approuvées, l'agent sonde régulièrement chaque adresse IP reconnue (toutes les 20 minutes par défaut ; paramètre modifiable) pour vérifier que le même utilisateur est toujours connecté. De plus, lorsque le pare-feu rencontre une adresse IP pour laquelle il ne dispose pas de mappage d'utilisateur, il envoie l'adresse à l'agent pour sondage immédiat.

Voir Configure User Mapping Using the Windows User-ID Agent (Configurer le mappage d'utilisateurs à l'aide de l'agent d'ID utilisateur Windows) ou Configure User Mapping Using the PAN-OS Integrated User-ID Agent (Configurer le mappage d'utilisateurs à l'aide de l'agent d'ID utilisateur intégré PAN-OS) pour plus de détails.

# Activation de User-ID

L'identité de l'utilisateur, contrairement à l'adresse IP, fait partie intégrante d'une infrastructure de sécurité efficace. Le fait de savoir précisément qui utilise chacune des applications de votre réseau, qui a potentiellement introduit une menace ou qui transfert des fichiers, permet de renforcer votre politique de sécurité et de réduire les délais de réponse aux incidents. User-ID vous permet d'utiliser les informations utilisateurs qui sont stockées dans une vaste gamme de répertoires afin d'obtenir une certaine visibilité et un contrôle sur les politiques basées sur les utilisateurs et les groupes ainsi que d'améliorer la journalisation, les rapports et les analyses :

**STEP 1 |** Activez l'agent User-ID sur les zones source contenant les utilisateurs qui enverront des requêtes qui nécessitent des contrôles d'accès basés sur l'utilisateur.

> ***Activez User-ID uniquement sur les zones approuvées. Si vous activez User-ID et le sondage du client sur une zone externe non approuvée (comme Internet), des sondages pourraient être envoyés en dehors de votre réseau protégé, ce qui entraînerait une divulgation des informations du nom de compte du service de l'agent User-ID, du nom de domaine et du hachage du mot de passe crypté, ce qui pourrait permettre à un pirate d'obtenir un accès non autorisé aux services et applications protégés.***

1. Sélectionnez **Network (Réseau)** > **Zones (Zones)**, puis cliquez sur le **Name (Nom)** de la zone.
2. **Enable User Identification (Activez l'identification de l'utilisateur)**, puis cliquez sur **OK (OK)**.

**STEP 2 |** Création d'un compte de service dédié pour l'agent User-ID.

> ***Il est recommandé de créer un compte de service disposant du nombre minimal de permissions requises pour prendre en charge les options User-ID que vous activez pour réduire votre surface d'attaque dans l'éventualité où votre compte de service est infecté.***

Cette étape est obligatoire si vous prévoyez d'utiliser l'agent User-ID Windows ou l'agent User-ID intégré à PAN-OS pour surveiller la présence d'événements de connexion et de déconnexion utilisateur sur les contrôleurs de domaine, les serveurs Microsoft Exchange ou les clients Windows.

**STEP 3 |** Mappage d'utilisateurs à des groupes.

Le pare-feu pourra alors se connecter à votre annuaire LDAP et de récupérer les informations de Mappage des groupes afin de vous permettre de sélectionner les noms d'utilisateurs et les noms de groupes lors de la création de la politique.

**STEP 4 |** Mappage d'adresses IP à des utilisateurs.

***Il est recommandé de ne pas activer l'interrogation du client sur les réseaux haute sécurité. L'interrogation du client peut générer une grande quantité de trafic sur le réseau et peut constituer une menace pour la sécurité lorsqu'il est mal configuré.***

La façon de procéder dépend de l'emplacement de vos utilisateurs et des types de systèmes qu'ils utilisent ainsi que des systèmes qui recueillent les événements de connexion et de déconnexion utilisateur sur votre réseau. Vous devez configurer au moins un agent User-ID pour activer le Mappage d'utilisateur :

- Configuration du mappage d'utilisateur à l'aide de l'agent User-ID Windows.
- Configure le Mappage d'utilisateur à l'aide de l'Agent User-ID intégré à PAN-OS.
- Configuration de User-ID pour la surveillance des expéditeurs Syslog lors du mappage d'utilisateur.
- Configuration du mappage d'utilisateur pour les utilisateurs de serveurs de terminaux.
- Envoi de mappages d'utilisateurs à User-ID à l'aide de l'API XML.
- Insertion du nom d'utilisateur dans les en-têtes HTTP.

**STEP 5 |** Indiquez les réseaux à inclure et à exclure du mappage d'utilisateur.

***Il est recommandé de toujours indiquer les réseaux à inclure et à exclure de User-ID. Ainsi, vous pouvez vous assurer que seuls vos actifs de confiance sont sondés et que les mappages d'utilisateur non désirés ne sont pas créés de façon inopinée.***

La manière dont vous précisez les réseaux à inclure et à exclure dépend de l'agent User-ID que vous utilisiez : soit l'agent User-ID Windows ou l'agent User-ID intégré à PAN-OS.

**STEP 6 |** Configuration de Authentication Policy and Authentication Portal (Politique d'authentification et portail d'authentification).

Le pare-feu utilise le portail d'authentification pour authentifier les utilisateurs finaux lorsqu'ils demandent des services, des applications ou des catégories d'URL qui correspondent à des règles de politique d'authentification. Selon les informations utilisateurs recueillies lors de l'authentification, le pare-feu crée de nouveaux mappages d'utilisateur ou met à jour les mappages existants. Les informations de mappage recueillies lors de l'authentification remplacent les informations recueillies par d'autres méthodes de User-ID.

1. Configuration du portail d'authentification.
2. Configuration de la politique d'authentification.

**STEP 7 |** Activez la mise en œuvre d'une politique basée sur un utilisateur et sur un groupe.

***Créez des règles en fonction d'un groupe plutôt que d'un utilisateur lorsque cela est possible. Cela vous évite de continuellement mettre à jour vos règles (ce qui nécessite une validation) lorsque votre base de données d'utilisateurs change.***

Une fois l'agent User-ID configuré, vous pouvez choisir un nom d'utilisateur ou un nom de groupe lors de la définition de la source ou de la destination d'une règle de sécurité :

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis **Add (Ajoutez)** une nouvelle règle ou cliquez sur le nom d'une règle existante pour la modifier.
2. Sélectionnez **User (Utilisateur)** et spécifiez les utilisateurs et les groupes à mettre en correspondance dans la règle de l'une des manières suivantes :
   - Si vous souhaitez sélectionner des utilisateurs/groupes spécifiques comme critères de recherche, cliquez sur **Add (Ajouter)** dans la section Source User (Utilisateur source) pour afficher la liste des utilisateurs et des groupes détectés par la fonction de mappage de groupe du pare-feu. Sélectionnez les utilisateurs ou les groupes à ajouter à la règle.
   - Si vous souhaitez faire correspondre à tout utilisateur qui a été authentifié ou non et que vous n'avez pas besoin de connaître le nom de l'utilisateur ou du groupe spécifique, sélectionnez **known-user (Utilisateur connu)** ou **unknown (Utilisateur inconnu)** dans la liste déroulante Source User (Utilisateur source).
3. Configurez les autres éléments de la règle si nécessaire, puis cliquez sur **OK (OK)** pour l'enregistrer. Pour plus d'informations sur les autres champs de la règle de sécurité, reportez-vous à la section Configuration d'une politique de sécurité de base.

**STEP 8 |** Créez les règles de politique de sécurité pour activer User-ID en toute sécurité au sein des zones approuvées et empêcher le trafic User-ID de sortir de votre réseau.

Suivez les Meilleures pratiques de politique de sécurité de la passerelle Internet pour vous assurer que l'application User-ID (`paloalto-userid-agent`) n'est autorisée que dans les zones où les agents (tant vos agents Windows que vos agents intégrés à PAN-OS) surveillent les services et distribuent les mappages aux pare-feu. Plus précisément :

- Autorisez l'application `paloalto-userid-agent` entre les zones où sont situés vos agents et celles où sont situés les serveurs faisant l'objet d'une surveillance (ou, mieux encore, entre les systèmes particuliers qui hébergent l'agent et les serveurs faisant l'objet d'une surveillance).
- Autorisez l'application `paloalto-userid-agent` entre les agents et les pare-feux qui ont besoin des mappages d'utilisateur et entre les pare-feu qui redistribuent les mappages d'utilisateur et les pare-feux qui reçoivent les informations.
- Refusez l'application `paloalto-userid-agent` sur toute zone externe, comme votre zone Internet.

**STEP 9 |** Configurez le pare-feu pour qu'il obtienne les adresses IP des utilisateurs des en-têtes X-Forwarded-For (XFF) .

Lorsque le pare-feu se trouve entre l'Internet et un serveur proxy, les adresses IP contenues dans les paquets que le pare-feu voit sont celles du serveur proxy et non des utilisateurs. Pour avoir une visibilité des adresses IP des utilisateurs, configurez le pare-feu pour qu'il utilise les en-têtes XFF pour le mappage d'utilisateur. Lorsque cette option est activée, le pare-feu met les adresses IP en correspondance avec les noms d'utilisateurs indiqués dans la politique afin de permettre

le contrôle et la visibilité des utilisateurs et des groupes qui y sont associés. Pour plus de détails, reportez-vous à la section Identification des utilisateurs connectés via un serveur proxy.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Content-ID (Content-ID)** et modifiez les paramètres d'en-tête X-Forwarded-For.
2. Sélectionnez **X-Forwarded-For Header in User-ID (En-tête X-Forwarded-For dans User-ID)**.

   *La sélection de l'option **Strip-X-Forwarded-For Header (Extraire l'en-tête X-Forwarded-For)** ne désactive pas l'utilisation d'en-têtes XFF pour l'attribution d'utilisateur dans des règles de politique ; le pare-feu réinitialise la valeur XFF uniquement après l'avoir utilisée pour l'attribution d'utilisateur.*
3. Cliquez sur **OK** pour enregistrer vos modifications.

**STEP 10 |** Si vous utilisez une configuration haute disponibilité, activez la synchronisation.

*Il est recommandé de toujours activer l'option **Enable Config Sync (Activer la synchronisation de la configuration)**d'une configuration HA pour vous assurer que les mappages de groupe et les mappages d'utilisateur sont synchronisés entre le pare-feu actif et le pare-feu passif.*

1. Sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Général)**, puis modifiez la section Setup (Configuration).
2. Sélectionnez **Enable HD (Activer la HD)**.
3. Sélectionnez **Enable Config Sync (Activer la synchronisation de la configuration)**.
4. Saisissez la **Peer HA1 IP Address (Adresse IP de l'homologue HA1)**, à savoir l'adresse IP de la liaison de contrôle HA1 sur le pare-feu homologue.
5. (Facultatif) Saisissez la valeur pour **Backup Peer HA1 IP Address (Adresse IP de l'homologue HA1 de sauvegarde)**, à savoir l'adresse IP de la liaison de contrôle de sauvegarde du pare-feu de l'homologue.
6. Cliquez sur **OK**.

**STEP 11 |** Validez vos modifications.

**Commit (Validez)** vos modifications pour les rendre actives.

**STEP 12 |** Vérification de la configuration de User-ID.

Après avoir configuré les mappages d'utilisateur et les mappages de groupes, vérifiez que la configuration fonctionne correctement et que vous pouvez activer et surveiller en toute sécurité l'accès des utilisateurs et des groupes à vos applications et services.

# Mappage d'utilisateurs à des groupes

La définition de règles de politique basées sur l'appartenance à un groupe d'utilisateurs plutôt que sur des utilisateurs individuels simplifie l'administration car vous ne devez pas mettre à jour les règles lorsque l'appartenance à un groupe change. Le nombre de groupes distincts d'utilisateurs que chaque pare-feu ou Panorama peut référencer parmi toutes les politiques varie selon le modèle. Pour plus d'informations, reportez-vous à la matrice de compatibilité.

Utilisez la procédure suivante pour permettre au pare-feu de se connecter à votre annuaire LDAP et de récupérer les informations de mappage de groupe. Vous pouvez ensuite activer la stratégie basée sur l'utilisateur et le groupe.

*Vous trouverez ci-dessous les recommandations relatives au mappage de groupe dans un environnement Active Directory (AD) :*

- *Si vous avez un seul domaine, vous n'avez besoin que d'une configuration de mappage de groupe avec un profil de serveur LDAP qui connecte le pare-feu au contrôleur de domaine avec la meilleure connectivité. Vous pouvez ajouter jusqu'à quatre contrôleurs de domaine au profil de serveur LDAP pour la redondance. Notez que vous ne pouvez pas augmenter la redondance au-delà de quatre contrôleurs de domaine pour un seul domaine en ajoutant plusieurs configurations de mappage de groupe pour ce domaine.*
- *Si vous disposez de plusieurs domaines et/ou forêts, vous devez créer une configuration de mappage de groupe avec un profil de serveur LDAP qui connecte le pare-feu à un serveur de domaine dans chaque domaine / forêt. Assurez-vous que les noms d'utilisateurs sont uniques dans chaque forêt.*
- *Si vous disposez de groupes universels, créez un profil de serveur LDAP pour vous connecter au domaine racine du serveur du Catalogue global sur le port 3268 ou 3269 pour SSL, puis créez un autre profil de serveur LDAP pour vous connecter aux contrôleurs du domaine racine sur le port 389. Vous vous assurez ainsi que les informations sur les groupes et les utilisateurs sont disponibles pour tous les domaines et sous-domaines.*
- *Avant d'utiliser le mappage de groupe, configurez **un nom d'utilisateur principal** pour les stratégies de sécurité basées sur l'utilisateur, car cet attribut identifiera les utilisateurs dans la configuration de la politique, les journaux et les rapports.*

**STEP 1 |** Ajoutez un profil de serveur LDAP.

Le profil précise comment le pare-feu se connecte aux serveurs d'annuaires desquels il collecte les informations de mappage de groupe.

*Si vous créez plusieurs configurations de mappage de groupe qui utilisent le même nom unique (DN) ou le même serveur LDAP de base, les configurations de mappage de groupe ne peuvent pas contenir des groupes qui se chevauchent (par exemple, la Liste d'inclusion d'une configuration de mappage de groupe n peut pas contenir un groupe qui est aussi dans une configuration de mappage de groupe différente).*

1. Sélectionnez **Device (périphérique)** > **Server Profiles (Profils de serveur)** > **LDAP** et **Add (ajouter)** un profil de serveur.
2. Saisissez un **Profile Name (Nom de profil)** pour identifier le profil de serveur.
3. **Add (Ajoutez)** les serveurs LDAP. Vous pouvez ajouter jusqu'à quatre serveurs au profil mais ils doivent être du même **Type (Type)**. Donnez un **Name (Nom)** à chaque serveur (pour l'identifier), ainsi qu'une adresse IP de **LDAP Server (Serveur LDAP)** ou un FQDN ainsi que le **Port (Port)** du serveur (valeur par défaut : 389).
4. Sélectionnez le **Type (type)** de serveur.

   En fonction de ce que vous avez sélectionné (par exemple, **active-directory (annuaire actif)**), le pare-feu remplit automatiquement les attributs LDAP appropriés dans les paramètres de mappage de groupe. Toutefois, si vous avez personnalisé votre schéma LDAP, vous devrez peut-être modifier les paramètres par défaut.
5. Pour le champ **Base DN (DN de base)**, sélectionnez le Distinguished Name (nom unique ; DN) de l'emplacement de l'arborescence LDAP à partir duquel vous souhaitez que le pare-feu commence sa recherche d'informations relatives à l'utilisateur et au groupe.
6. Pour les champs **Bind DN (DN de Liaison)**, **Password (Mot de passe)** et **Confirm Password (Confirmez le mot de passe)**, entrez les informations d'authentification pour la liaison à l'arborescence LDAP.

   Le **Bind DN (DN de liaison)** peut être un nom LDAP complet (par exemple, `cn=administrator,cn=users,dc=acme,dc=local` ou un nom principal d'utilisateur (par exemple, `administrator@acme.local`).
7. Entrez le **Bind Timeout (Délai de liaison)** et le **Délai de recherche** en secondes (la valeur par défaut est 30 pour les deux).
8. Cliquez sur **OK** pour enregistrer le profil de serveur.

**STEP 2 |** Configurez les paramètres du serveur dans une configuration de mappage de groupe.

1. Sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Group Mapping Settings (Paramètres de mappage de groupe)**.
2. **Add (Ajouter)** la configuration du mappage de groupe.
3. Saisissez un **Name (Nom)** unique pour identifier la configuration du mappage de groupe.
4. Sélectionnez le **Server Profile (Profil de serveur)** LDAP que vous venez de créer.
5. (Facultatif) Spécifiez l'**Update Interval (Intervalle de mise à jour)** (en secondes). Entrez une valeur (plage de 60 à 86 400, par défaut 3 600) basée sur la fréquence à laquelle le pare-feu doit vérifier la source LDAP pour les mises à jour de la configuration du mappage de groupe. Si la source LDAP contient de nombreux groupes, une valeur trop faible peut ne pas laisser assez de temps pour mapper tous les groupes.
6. (Facultatif) Par défaut, le champ **User Domain (Domaine d'utilisateur)** est vide : le pare-feu détecte automatiquement les noms de domaines des serveurs Active Directory (annuaire

actif ; AD). Si vous saisissez une valeur, elle remplacera tout nom de domaine que le pare-feu récupère de la source LDAP. Pour la plupart des configurations, si vous devez saisir une valeur, saisissez le nom de domaine NetBIOS (par exemple, **`example`**, et non pas **`example.com`**).

Si vous utilisez le catalogue global, la saisie d'une valeur remplace le nom de domaine pour tous les utilisateurs et groupes de ce serveur, y compris ceux d'autres domaines.

7. (Facultatif) Pour filtrer les groupes que le pare-feu suit pour le mappage de groupe, dans la section Objets du groupe, saisissez un **Search Filter (Filtre de recherche)** (requête LDAP) et une **Object Class (Classe d'objet)** (définition du groupe).
8. (Facultatif) Pour filtrer les utilisateurs que le pare-feu suit pour le mappage de groupe, dans la section Objets de l'utilisateur, saisissez un **Search Filter (Filtre de recherche)** (requête LDAP), une **Object Class (Classe d'objet)** (définition de l'utilisateur).
9. Assurez-vous que la configuration du mappage de groupe est **Enabled (Activée)** (est activée par défaut).

**STEP 3 |** (Facultatif) Définissez les attributs d'utilisateur et de groupe à collecter pour le mappage d'utilisateur et de groupe. Cette étape est obligatoire si vous souhaitez mapper des utilisateurs en fonction d'attributs de répertoire autres que le domaine.

1. Si vos sources ID utilisateur n'envoient que le nom d'utilisateur et que le nom d'utilisateur est unique dans l'organisation, sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **User Mapping (Mappage d'utilisateur)** > **Setup (Paramètres)** et **Edit (Modifier)** ;a section paramètres pour **Allow matching usernames without domains (Autoriser les noms d'utilisateur correspondants sans domaines)** pour permettre au pare-feu de vérifier si les noms d'utilisateur uniques collectés sur le serveur LDAP lors du mappage de groupe correspondent aux utilisateurs associés à une stratégie et d'éviter d'écraser le domaine dans votre profil source.

   *Avant d'activer cette option, configurez le mappage de groupe pour le groupe LDAP qui inclut l'ID utilisateur source (comme GlobalProtect ou le portail d'authentification) qui collecte les mappages. Après avoir validé les modifications, l'ID utilisateur source renseigne les noms d'utilisateur sans domaine. Seuls les noms d'utilisateur collectés lors de la mise en correspondance de groupes peuvent être associés sans domaine. Si vos ID utilisateur source envoient des informations utilisateur dans plusieurs formats et que vous activez cette option, vérifiez que les attributs collectés par le pare-feu ont un préfixe unique. Pour vous assurer que les utilisateurs sont correctement identifiés si vous activez cette option, tous les attributs du mappage de groupe doivent être uniques. Si le nom d'utilisateur n'est pas unique, le pare-feu enregistre une erreur dans les journaux de débogage.*
2. Sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Group Mapping Settings (Paramètres de mappage de groupe)** > **Add (Ajouter)** > **User and Group Attributes (Attributs de l'utilisateur et du groupe)** > **User Attributes(Attributs de l'utilisateur)** et saisissez le **Directory Attribute (Répertoire de l'attribut)** que vous voulez collecter aux fins d'identification de l'utilisateur. Spécifiez un **Primary Username (Nom d'utilisateur principal)** pour identifier l'utilisateur sur le pare-feu et pour représenter

l'utilisateur dans les rapports et les journaux et pour exercer un contrôle prioritaire sur les autres formats que le pare-feu reçoit de la source User-ID.

Lorsque vous sélectionnez le **Type** de profil de serveur, le pare-feu renseigne automatiquement les valeurs des attributs de l'utilisateur et du groupe. En fonction des informations utilisateur envoyées par vos sources d'ID utilisateur, vous devrez peut-être configurer les attributs corrects :

- **User Principal Name (UPN) (Nom principal de l'utilisateur (UPN))** : **`userPrincipalName`**
- **NetBios Name (Nom NetBios)** : **`sAMAccountName`**
- **Email ID (ID du e-mail)**: Le répertoire d'attribut pour ce e-mail
- **Multiple formats (Formats multiples)**: Récupérez les attributs de mappage utilisateur du répertoire utilisateur avant d'activer vos sources d'ID utilisateur.

Si vous n'indiquez pas de nom d'utilisateur principal, le pare-feu utilise les valeurs par défaut suivantes pour chaque type de profil de serveur :

| Attribut | Active Directory | Novell eDirectory ou Sun ONE Directory Server |
|---|---|---|
| Nom d'utilisateur principal | `sAMAccountName` | `uid` |
| E-mail | `mail` | `mail` |
| Nom d'utilisateur alternatif 1 | `userPrincipalName` | Aucun. |
| Nom du groupe | `name` | `cn` |
| Membre du groupe | `member` | `member` |

3. (Facultatif) Spécifiez un format d'adresse **e-mail** et jusqu'à trois formats de **Alternate Username (nom d'utilisateur alternatif)**.
4. Sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Group Mapping Settings (Paramètres de mappage de groupe)** > **Add (Ajouter)** > **User and Group Attributes (Attributs de l'utilisateur et du groupe)** > **Group Attributes (Attributs de groupe)** et spécifiez le **Group Name (Nom de groupe)**, le **Group Member (Membre du groupe)** et le format d'adresse **e-mail**.

   Vous devez valider avant que le pare-feu ne collecte les attributs d'annuaire auprès du serveur LDAP.

**STEP 4 |** Limitez les groupes disponibles dans des règles de politique.

Requis uniquement si vous souhaitez limiter des règles de politique à des groupes spécifiques. Le maximum combiné pour les listes **Group Include List (Liste d'inclusion de groupe)** et **Custom Group (Groupe personnalisé)** correspond à 640 saisies pour chaque configuration d'association de groupe. Chaque entrée peut correspondre à un seul groupe ou à une liste de groupes. Par

défaut, si vous ne spécifiez pas de groupes, tous les groupes sont disponibles dans les règles de politique.

*Les groupes personnalisés que vous créez seront également disponibles dans la liste d'autorisation des profils d'authentification (Configurer un profil et une séquence d'authentification).*

1. Ajoutez des profils existants du service d'annuaire :
   1. Sélectionnez **Group Include List (Liste d'inclusion de groupe)**.
   2. Sélectionnez les groupes disponibles que vous souhaitez afficher dans les règles de politique et ajoutez-les (⊕) aux groupes inclus.
2. Si vous souhaitez baser des règles de politique sur des attributs utilisateur ne correspondant pas à des groupes d'utilisateurs existants, créez des groupes personnalisés basés sur des filtres LDAP :
   1. Sélectionnez **Custom Group (Groupe personnalisé)** et **Add (Ajoutez)** le groupe.
   2. Donnez un **Name (Nom)** unique au groupe dans la configuration du mappage de groupe pour le pare-feu ou le système virtuel actuel.

      Si le **Name (Nom)** a la même valeur que le nom unique (DN) d'un groupe de domaines AD existant, le pare-feu utilise le groupe personnalisé dans toutes les références à ce nom (par exemple, dans les politiques et les journaux).
   3. Spécifiez un **LDAP Filter (Filtre LDAP)** de 2 048 caractères UTF-8 maximum et cliquez sur **OK**.

      Le pare-feu ne valide pas les filtres LDAP, vous devez vous assurer qu'ils sont exacts.

      *Pour minimiser l'impact des performances sur le serveur d'annuaires LDAP, n'utilisez que des attributs indexés dans le filtre.*
3. Cliquez sur **OK** pour enregistrer vos modifications.

   Vous devez valider pour que les groupes personnalisés soient disponibles dans des politiques et des objets.

**STEP 5 |** **Commit (Validez)** vos modifications.

Vous devez valider avant de pouvoir utiliser des groupes personnalisés dans les stratégies et les objets et avant que le pare-feu puisse collecter les attributs du serveur LDAP.

*Après avoir configuré le pare-feu pour extraire les informations de mappage de groupe d'un serveur LDAP, mais avant de configurer les stratégies en fonction des groupes récupérés, il est préférable d'attendre que le pare-feu actualise son cache de mappages de groupes ou actualise manuellement le cache. Pour vérifier les groupes que vous pouvez actuellement utiliser dans les politiques, accédez à la CLI du pare-feu et exécutez la commande* ***`show user group`****. Pour déterminer quand le pare-feu actualisera le cache des mappages de groupes, exécutez la commande* ***`show user group-mapping statistics`*** *et vérifiez la* `Next Action` *(action suivante). Pour actualiser manuellement le cache, exécutez la commande* ***`debug user-id refresh group-mapping all`****.*

**STEP 6 |** Vérifiez que le mappage de l'utilisateur et du groupe a correctement identifié les utilisateurs.

1. Sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Group Mapping (Mappage de groupe)** > **Group Include List (Liste d'inclusion de groupe)** pour confirmer que le pare-feu a récupéré tous les groupes.
2. Pour vérifier que tous les attributs utilisateur ont été capturés correctement, utilisez la commande CLI suivante :

   ```
   show user user-attributes user all
   ```

   Le format normalisé pour le nom d'utilisateur principal (UPN), le nom d'utilisateur principal, les attributs de e-mail et tous les noms d'utilisateur alternatifs configurés s'affichent pour tous les utilisateurs :

   ```
   admin@PA-VM-8.1> show user user-attributes user all
   ```

   ```
   Primary: nam\sam-user   Email: sam-user@nam.com
   ```

   ```
   Alt User Names:1) nam.com\sam-user
   ```

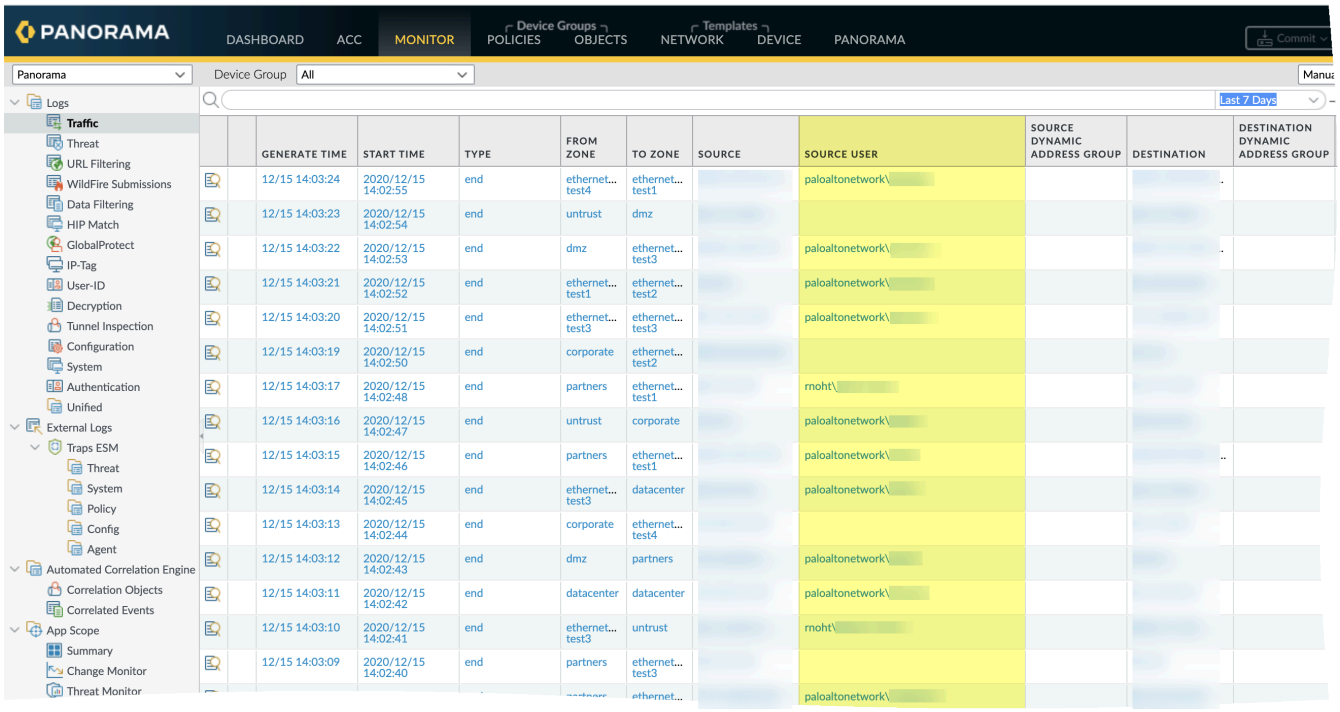
   ```
   2) nam\sam-user-upn
   ```

   ```
   3) sam-user-upn@nam.local
   ```

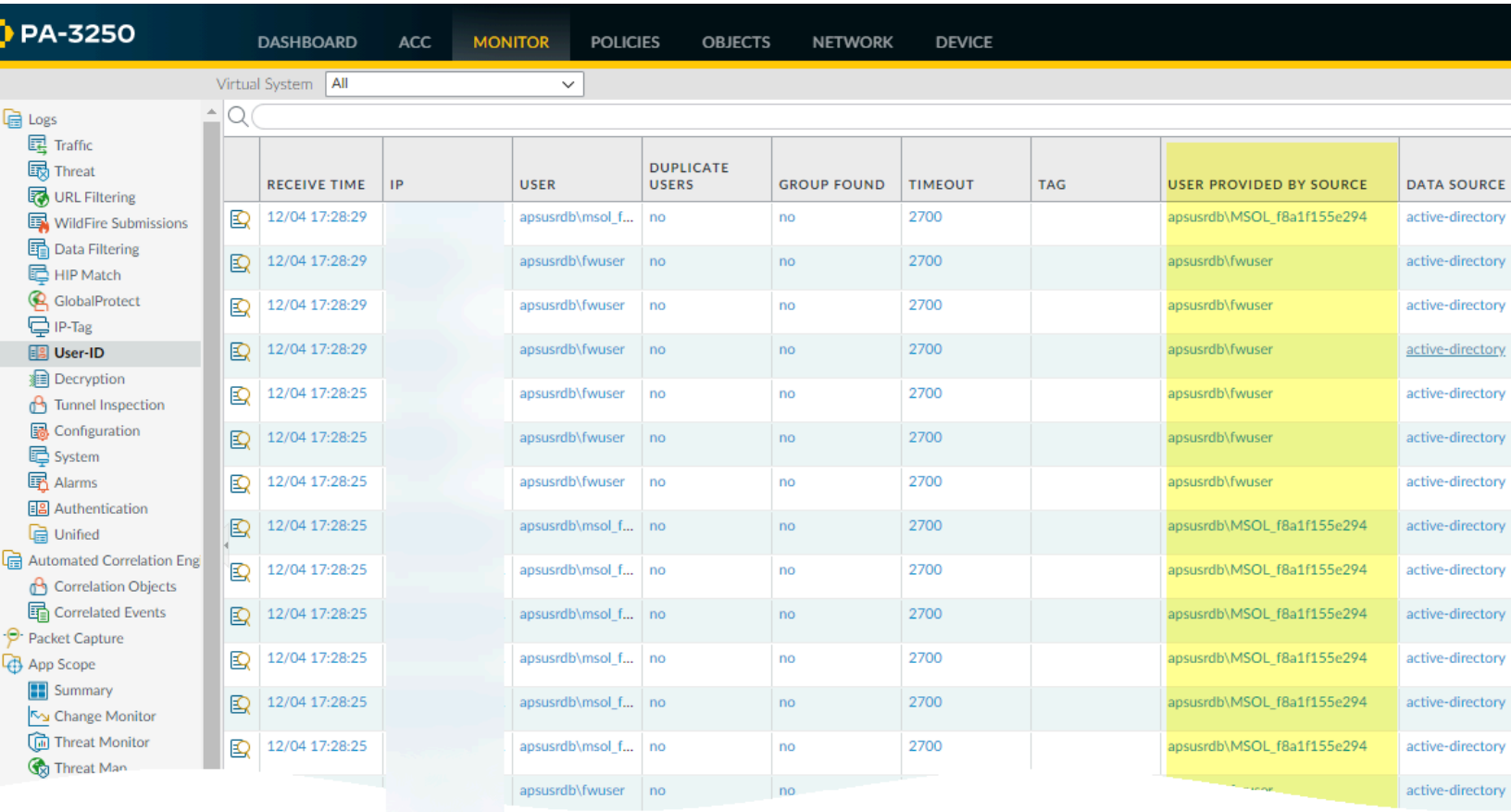
   ```
   4) sam-user@nam.com
   ```

3. Vérifiez que les noms d'utilisateur sont correctement affichés dans la colonne **Source User (Utilisateur source)** sous **Monitor (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafique)**.




4. Vérifiez que les utilisateurs sont mappés sur les noms d'utilisateur corrects dans la colonne **User Provided by Source (Utilisateur fourni par la source)** sous **Monitor (Surveillance)** > **Logs (Journaux)** > **User-ID (ID de l'utilisateur)**.



# Mappage d'adresses IP à des utilisateurs

User-ID fournit de nombreuses méthodes différentes pour mapper les adresses IP aux noms d'utilisateur. Avant de commencer à configurer le mappage utilisateur, tenez compte de la provenance de vos utilisateurs, des services auxquels ils accèdent et des applications et données dont vous avez besoin pour contrôler l'accès. Cela vous indiquera quels types d'agents ou d'intégrations vous permettront le mieux d'identifier vos utilisateurs.

Une fois que vous avez votre plan, vous pouvez commencer à configurer le mappage des utilisateurs en utilisant une ou plusieurs des méthodes suivantes, selon les besoins, pour activer l'accès et la visibilité des applications et des ressources par les utilisateurs :

- Si vous avez des utilisateurs avec des systèmes clients qui ne sont pas connectés à vos serveurs de domaine (par exemple, les utilisateurs exécutant des clients Linux qui ne se connectent pas au domaine), vous pouvez mapper les adresses IP aux noms d'utilisateur via le portail d'authentification. L'utilisation du portail d'authentification conjointement avec la Politique d'authentification garantit également que tous les utilisateurs s'authentifient pour accéder à vos applications et données les plus sensibles.
- Pour faire correspondre des utilisateurs lorsqu'ils se connectent à vos serveurs Exchange, eDirectory, contrôleurs de domaines ou clients Windows, vous devez configurer un agent User-ID :
  - Configuration du mappage d'utilisateur à l'aide de l'agent User-ID intégré à PAN-OS
  - Configuration du mappage d'utilisateur à l'aide de l'agent User-ID Windows
- Si vous disposez de clients qui exécutent des systèmes multi-utilisateurs dans un environnement Windows, tels que Microsoft Terminal Server, Citrix Metaframe Presentation Server ou XenApp, reportez-vous à la section Configuration de l'agent Terminal Server (TS) Palo Alto Networks pour le mappage d'utilisateur. Pour un système multi-utilisateur qui ne s'exécute pas sous Windows, vous pouvez récupérer des mappages utilisateur à partir d'un serveur Terminal Server à l'aide de l'API XML PAN-OS.
- Pour obtenir des mappages d'utilisateurs de services réseau existants qui authentifient les utilisateurs, tels que les contrôleurs sans fil, les périphériques 802.1x, les serveurs Apple Open Directory, les serveurs proxy et d'autres mécanismes de Network Access Control (contrôle d'accès au réseau ; NAC), reportez-vous à la section Configurer l'ID utilisateur pour surveiller les expéditeurs Syslog pour le mappage d'utilisateur.

  ***Vous pouvez configurer l'agent Windows ou l'agent User-ID intégré à PAN-OS sur le pare-feu pour écouter les messages syslog d'authentification provenant des services réseau, c'est la configuration préférée car seul l'agent intégré PAN-OS prend en charge l'écoute syslog via TLS.***
- Pour inclure le nom d'utilisateur et le domaine dans les en-têtes du trafic sortant pour permettre aux autres périphériques de votre réseau d'identifier l'utilisateur et d'appliquer la politique basée sur les utilisateurs, vous pouvez Insertion du nom d'utilisateur dans les en-têtes HTTP.
- Pour Partage des mappages User-ID sur l'ensemble des systèmes virtuels, vous pouvez configurer un système virtuel en tant que pôle User-ID.
- Pour les autres clients que vous ne pouvez pas faire correspondre en utilisant les autres méthodes, vous pouvez Envoyer des mappages d'utilisateur au User-ID à l'aide de l'API XML.

- Un réseau à grande échelle peut posséder des centaines de sources d'informations que les pare-feu interrogent pour le mappage d'utilisateur et le mappage de groupe et disposer de nombreux pare-feu qui appliquent les politiques en fonction des informations de mappage. Vous pouvez simplifier l'administration User-ID d'un tel réseau en groupant les informations de mappage avant que les agents User-ID ne les recueillent. Vous pouvez également réduire la quantité de ressources que les pare-feu et les sources d'informations utilisent dans cadre du processus de requête en configurant certains pare-feu pour qu'ils redistribuent les informations de mappage. Pour plus de détails, voir Déploiement de User-ID dans un réseau à grande échelle.

## Création d'un compte de service dédié pour l'agent User-ID

Pour utiliser l'agent User-ID Windows ou l'agent User-ID intégré à PAN-OS pour mapper les utilisateurs lors de leur connexion à vos serveurs Exchange, contrôleurs de domaine, serveurs eDirectory ou clients Windows, créez, sur chaque domaine que l'agent surveillera, un compte de service dédié pour l'agent User-ID sur un contrôleur de domaine.

L'agent User-ID cartographie les utilisateurs sur la base des journaux d'événements de sécurité. Pour que l'agent User-ID puisse cartographier les utilisateurs avec succès, vérifiez que la source de vos mappages génère des journaux pour les événements Audit Logon, Audit Kerberos Authentication Service et Audit Kerberos Service Ticket Operations. Au minimum, la source doit générer des journaux pour les événements suivants :

- Logon Success (4624)
- Authentication Ticket Granted (4768)
- Service Ticket Granted (4769)
- Ticket Granted Renewed (4770)

Les permissions requises pour le compte de service dépendent des méthodes de mappage d'utilisateur et des paramètres que vous envisagez d'utiliser. Par exemple, si vous utilisez l'User-ID intégré à PAN-OS, le compte de service exige les privilèges d'opérateurs de serveur pour surveiller les sessions d'utilisateur. Si vous utilisez l'agent User-ID Windows, le compte de service exige les privilèges d'opérateurs de serveur pour surveiller les sessions d'utilisateur. Pour réduire le risque d'infecter le compte de service User-ID, vous devez toujours configurer le compte en indiquant le nombre minimal de permissions nécessaires pour l'agent.

- Si vous installez l'agent User-ID Windows sur un serveur pris en charge par Windows, Configurez un compte de service pour l'agent User-ID basé sur Windows.
- Si vous utilisez l'agent User-ID intégré à PAN-OS sur le pare-feu, Configurez un compte de service pour l'agent User-ID intégré à PAN-OS.

***User-ID offre de nombreuses méthodes pour assurer une collecte sécuritaire des informations de mappage d'utilisateur. Certaines des anciennes fonctionnalités, qui étaient conçues pour des environnements qui exigeaient uniquement le mappage des utilisateurs des postes de travail Windows associés au réseau local, dépendent de comptes de service privilégiés. L'infection de votre compte de service privilégié ouvrirait votre réseau à des attaques. Il est recommandé d'éviter d'utiliser les anciennes fonctionnalités qui exigent des privilèges qui pourraient constituer une menace en cas de compromission, comme le sondage du client et la surveillance des sessions.***

## Configurer un compte de service pour l'agent User-ID basé sur Windows

Créez un compte de service Active Directory (AD) spécial pour que l'agent User-ID basé sur Windows puisse accéder aux services et aux hôtes qu'il surveillera pour recueillir les informations de mappage d'utilisateur. Vous devez créer un compte de service dans chaque domaine que l'agent surveillera. Après avoir activé les permissions requises pour le compte de service, procédez à la Configuration du mappage d'utilisateur à l'aide de l'agent User-ID Windows.

*Le flux de travail suivant précise tous les privilèges requis et fournit une orientation quant aux fonctionnalités de User-ID qui exigent des privilèges qui pourraient présenter une menace. Vous pourrez ainsi décider de la meilleure manière d'identifier les utilisateurs sans compromettre votre niveau de sécurité global.*

**STEP 1 |** Créez un compte de service AD pour l'agent User-ID.

Vous devez créer un compte de service dans chaque domaine que l'agent surveillera.

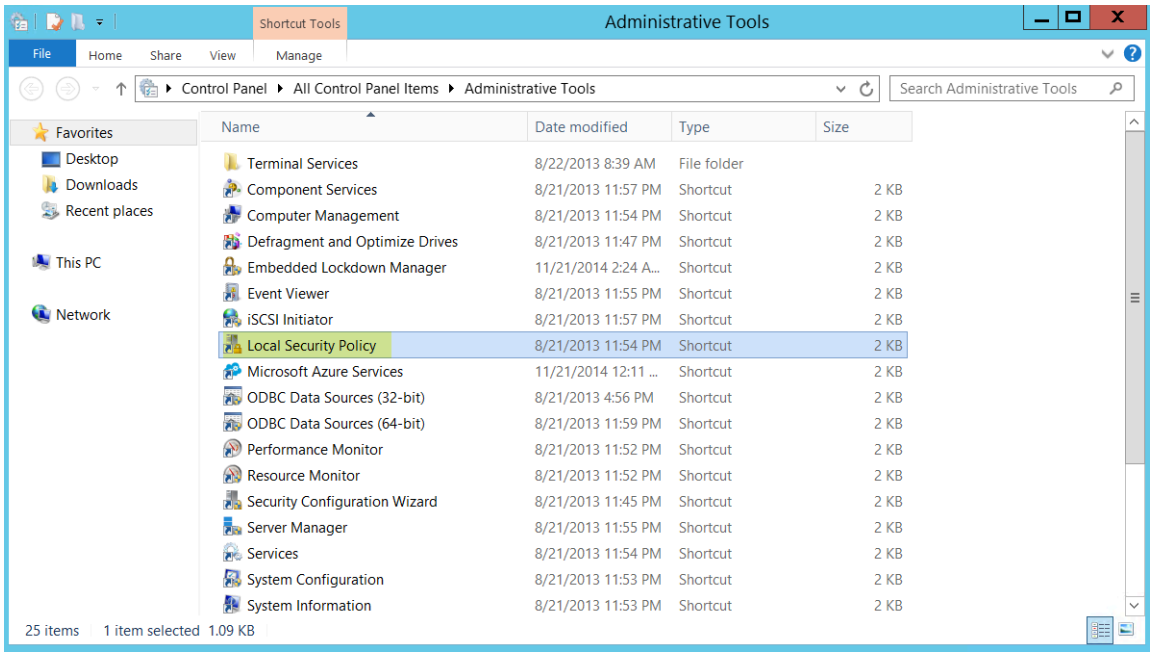
1. Connectez-vous au contrôleur de domaine.
2. Faites un clic droit sur l'icône Windows (), **Search (Cherchez)** des **`Active Directory Users and Computers`**, puis lancez l'application.
3. Ouvrez l'arborescence du domaine dans le volet de navigation, faites un clic droit sur **Managed Service Accounts (Comptes de service gérés)**, puis sélectionnez **New (Nouveau)** > **User (Utilisateur)**.
4. Saisissez le **First Name (Prénom)**, le **Last Name (Nom)** et le **User logon name (Nom de connexion)** de l'utilisateur, puis cliquez sur **Suivant**.
5. Saisissez le **Password (Mot de passe)** et **Confirm Password (Confirmez le mot de passe)**, puis cliquez sur **Next (Suivant)** et sur **Finish (Terminer)**.

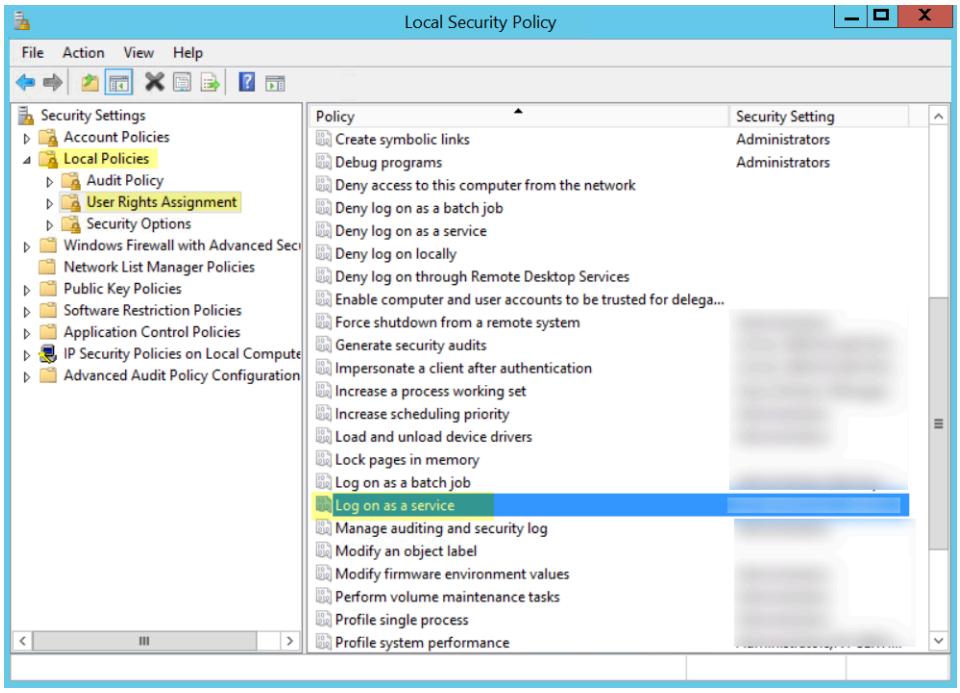
**STEP 2 |** Configurez une politique locale ou de groupe pour que le compte de service puisse ouvrir une session en tant que service.

La permission d'ouvrir une session en tant que service ne s'avère nécessaire que localement sur le serveur Windows qui est l'hôte de l'agent.

- Pour affecter les permissions localement :

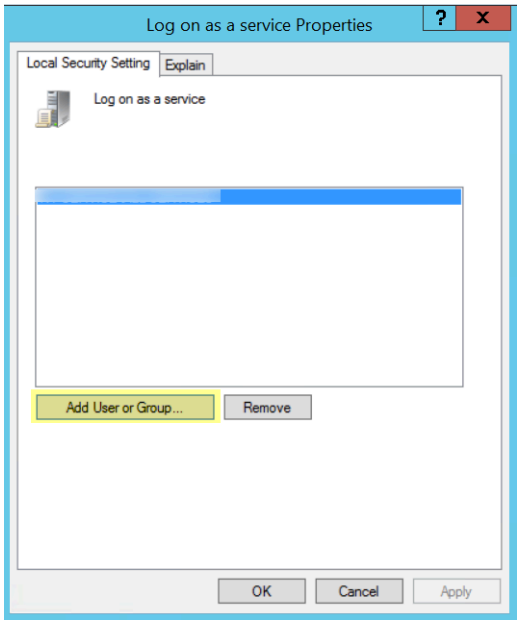
1. sélectionnez **Control Panel (Panneau de commande)** > **Administrative Tools (Outils administratifs)** > **Local Security Policy (Politique de sécurité locale)**.
2. 

3. Sélectionnez **Local Policies (Politiques locales)** > **User Rights Assignment (Affectation des droits d'utilisateurs)** > **Log on as a service (Ouvrir une session en tant que service)**.

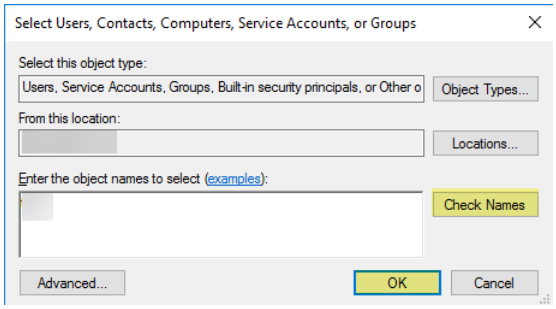


4. **Add User or Group (Ajoutez un utilisateur ou un groupe)** pour ajouter le compte de service.




5. **Enter the object names to select (Entrez les noms d'objet à sélectionner)** (le nom du compte de service) au format **`domain\username`**, puis cliquez sur **OK**.

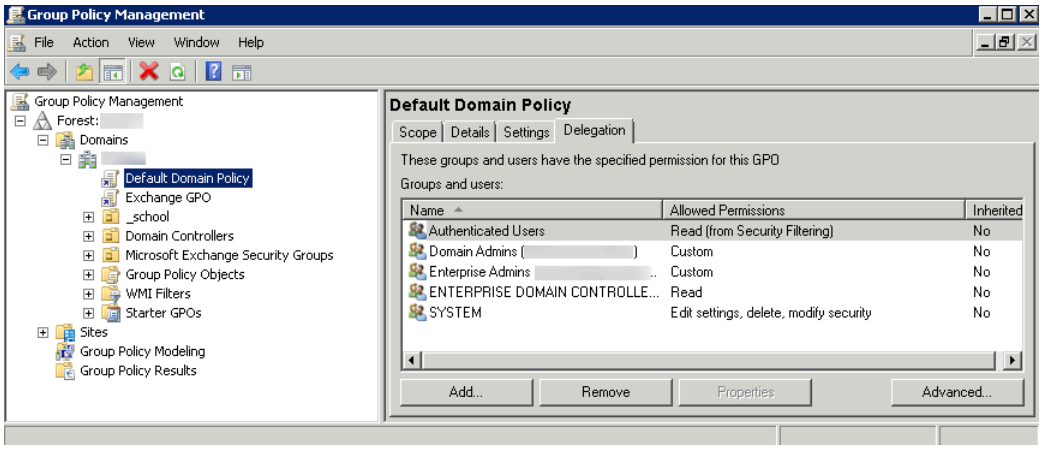



- Pour configurer une politique de groupe si vous installez des agents User-ID Windows sur plusieurs serveurs, utilisez l'éditeur de gestion des politiques de groupe.

  1. Sélectionnez **Start (Démarrer)** > **Group Policy Management (Gestion des politiques de groupe)** > **<your domain> (<votre domaine>)** > **Default Domain Policy (Politique de**

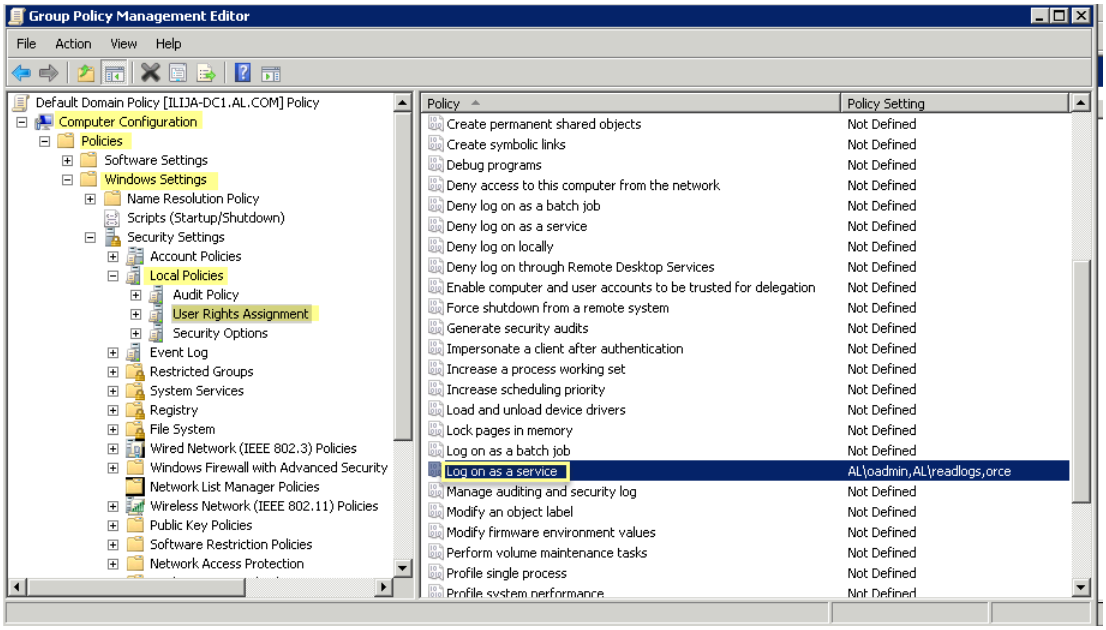
**domaine par défaut)** > **Action** > **Edit (Modifier)** pour le serveur Windows qui est l'hôte de l'agent.




2. Sélectionnez **Computer Configuration (Configuration de l'ordinateur)** > **Policies (Politiques)** > **Windows Settings (Paramètres Windows)** > **Security Settings (Paramètres**

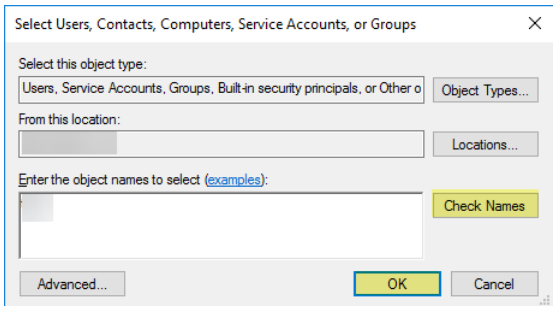
 

**de sécurité)** > **Local Policies (Politiques locales)** > **User Rights Assignment (Affectation des droits d'utilisateurs)**.




3. Faites un clic droit sur **Log on as a service (Ouvrir une session en tant que service)**, puis sélectionnez **Properties (Propriétés)**.
4. **Add User or Group (Ajoutez l'utilisateur ou le groupe)** du compte de service ou le groupe intégré, puis cliquez deux fois sur **OK**.

*Les administrateurs possèdent ce privilège par défaut.*




**STEP 3 |** Si vous souhaitez utiliser WMI pour collecter les données des utilisateurs, affectez des privilèges DCOM au compte de service pour qu'il puisse utiliser les requêtes WMI sur les serveurs surveillés.

1. Sélectionnez **Active Directory Users and Computers (Utilisateurs et ordinateurs Active Directory)** > **<your domain> (Votre domaine)** > **Builtin (Intégré)** > **Distributed COM Users (Utilisateurs COM distribués)**.
2. Faites un clic droit sur **Properties (Propriétés)** > **Members (Membres)** > **Add (Ajouter)**, puis saisissez le nom du compte de service.

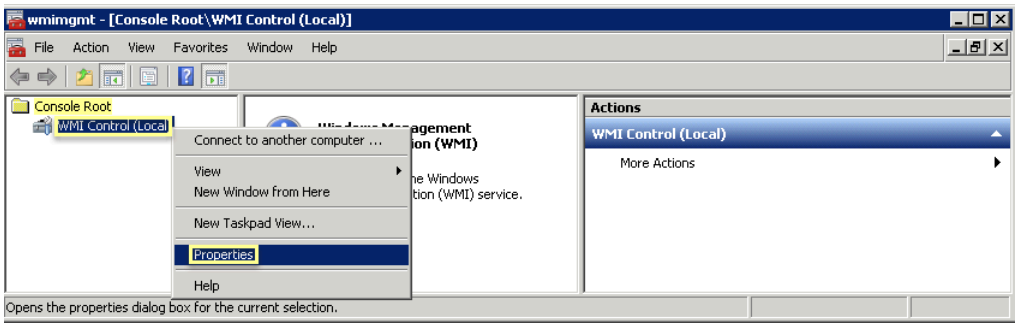
 

**STEP 4 |** Si vous prévoyez d'utiliser le sondage WMI, accordez au compte les droits de lecture sur l'espace de noms CIMV2 et affectez les permissions requises sur les systèmes client devant faire l'objet du sondage.

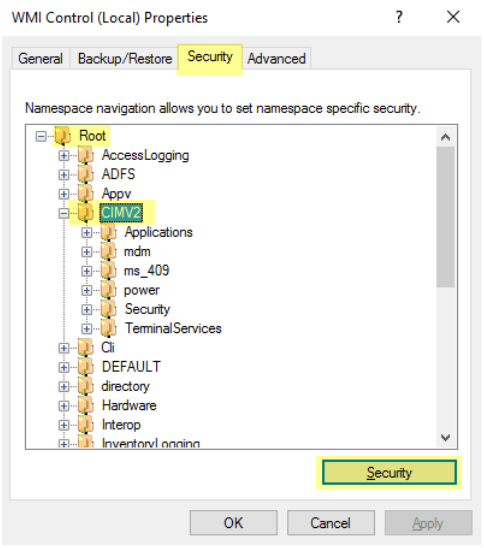
*N'activez pas l'interrogation du client sur les réseaux haute sécurité. L'interrogation du client peut générer une grande quantité de trafic sur le réseau et peut constituer une menace pour la sécurité lorsqu'il est mal configuré. Au lieu de cela, collectez des informations de mappage d'utilisateur à partir de sources plus isolées et fiables telles que les contrôleurs de domaine et par l'intermédiaire des intégrations avec Syslog ou l'API XML, qui ont l'avantage supplémentaire de vous permettre de recueillir en toute sécurité des informations de mappage d'utilisateurs à partir de n'importe quel type de périphérique ou de système d'exploitation, plutôt que de se cantonner aux clients Windows.*

Effectuez cette tâche sur chaque système client que l'agent User-ID sondera pour extraire les informations de mappage d'utilisateur :

1. Faites un clic droit sur l'icône Windows (), **Search (Cherchez)** **`wmimgmt.msc`** et lancez la console de gestion WMI.
2. Dans l'arborescence de la console, faites un clic droit sur **WMI Control (Contrôle WMI)**, puis sélectionnez **Properties (Propriétés)**.




3. Sélectionnez l'onglet **Security (Sécurité)**, puis sélectionnez **Root (Racine)** > **CIMV2**, et cliquez sur le bouton **Security (Sécurité)**.

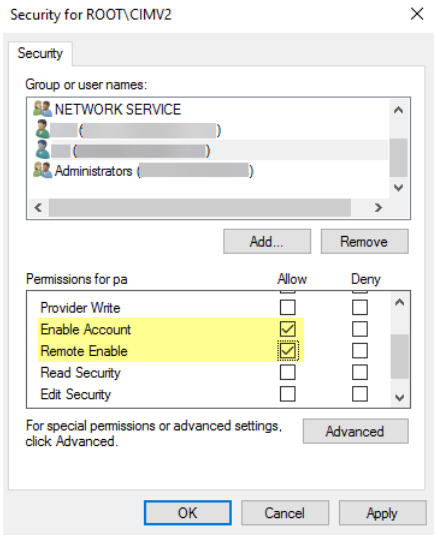


4. **Add (Ajoutez)** le nom du compte de service que vous avez créé, **Check Names (Vérifiez les noms)** pour vérifier votre entrée, puis cliquez sur **OK (OK)**.

   *Vous pourriez devoir changer les **Locations (Emplacements)** ou cliquer sur **Advanced (Avancé)** pour obtenir les noms de compte. Pour plus d'informations, reportez-vous à l'aide de la boîte de dialogue.*

5. Dans la section Permissions (Permissions) de **<nom d'utilisateur>**, **Allow (Autorisez)** les droits **Enable Account (Activation du compte)** et **Remote Enable (Activation à distance)**.



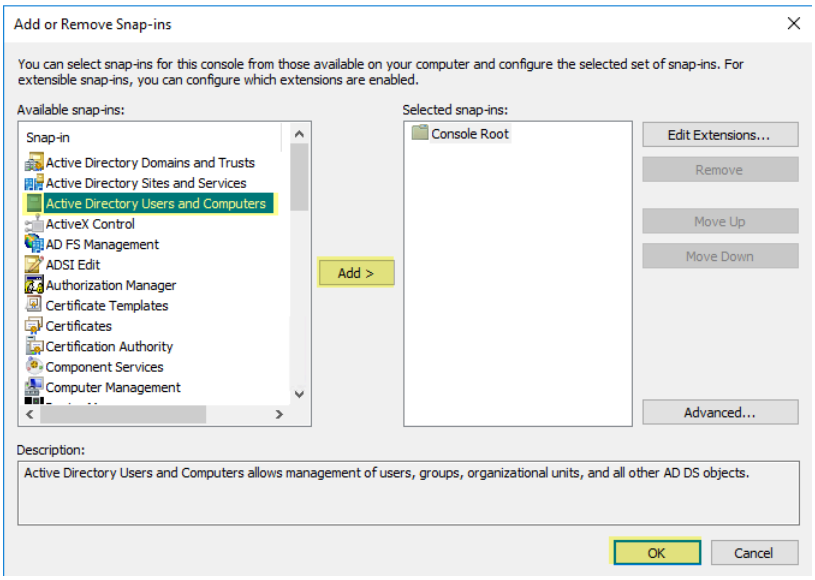

6. Cliquez deux fois sur **OK**.
7. Utilisez le composant Groupes et utilisateurs locaux de la console MMC (lusrmgr.msc) pour ajouter le compte de service aux utilisateurs du Distributed Component Object Model (modèle de composant objet distribué ; DCOM) et aux groupes d'utilisateurs du bureau à distance sur le système à sonder.

**STEP 5 |** Si vous souhaitez utiliser la Surveillance du serveur pour identifier les utilisateurs, ajoutez le compte de service au groupe intégré Event Log Reader (Lecteurs des journaux des événements) afin d'accorder au compte de service les privilèges de lecture des événements des journaux de sécurité.

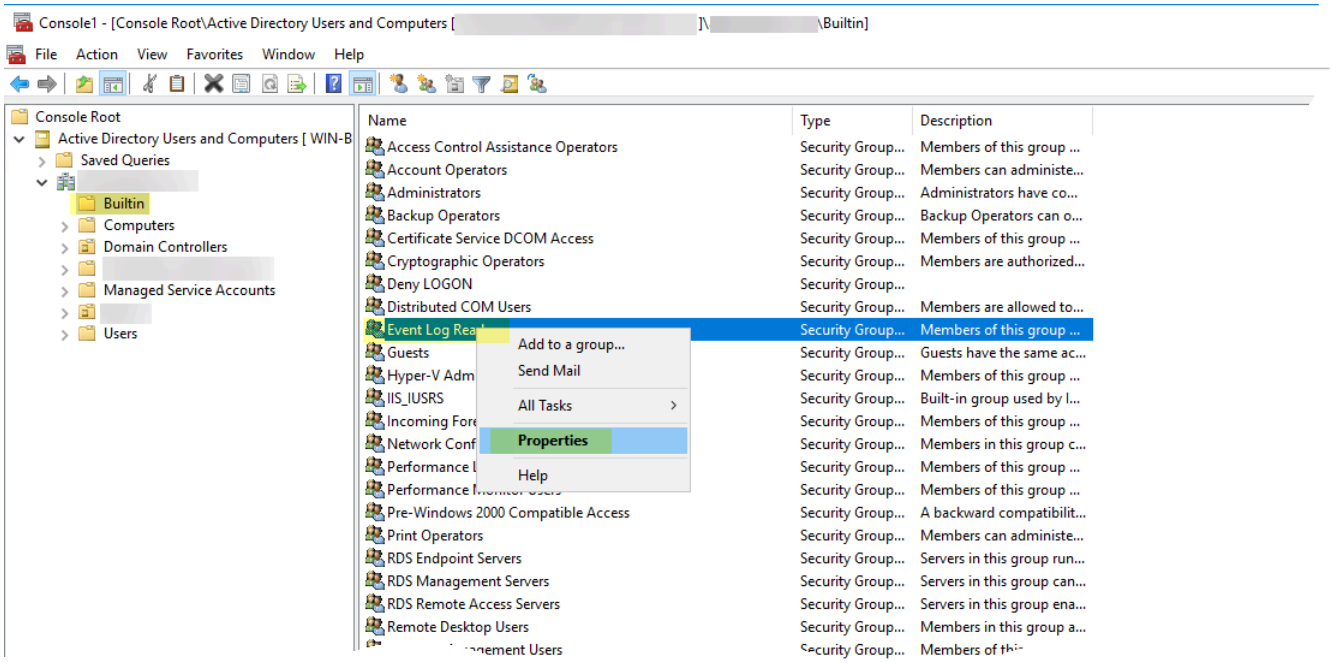
1. Sur le contrôleur du domaine ou le serveur Exchange qui contient les journaux que vous voulez que l'agent User-ID lise, ou sur le serveur membre qui reçoit les événements du transfert des journaux Windows, sélectionnez **Start (Démarrer)** > **Run (Exécuter)**, et saisissez **MMC**.
2. Sélectionnez **File (Fichier)** > **Add/Remove Snap-in (Ajouter/Supprimer un composant logiciel enfichable)** > **Active Directory Users and Computers** > **Add (Aouter)**, puis cliquez

sur **OK** pour exécuter la MMC et le composant logiciel enfichable Active Directory Users and Computers.

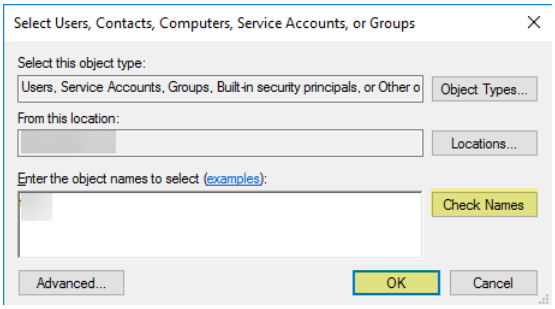



3. Accédez au dossier intégré du domaine, faites un clic droit sur le groupe **Event Log Reader (Lecteurs des journaux des événements)**, puis sélectionnez **Properties (Propriétés)** > **Members (Membres)**.



4. **Add (Ajoutez)** le compte de service, puis cliquez sur **Check Names (Vérifier les noms)** pour vérifier que le nom d'objet est correct.

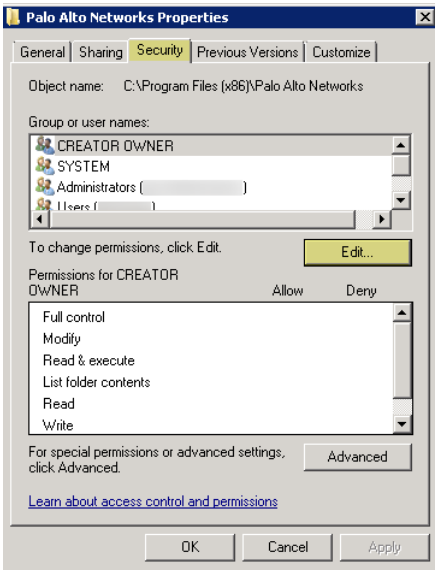



5. Cliquez deux fois sur **OK (OK)** pour enregistrer les paramètres.
6. Confirmez que le groupe Event Log Reader (Lecteurs des journaux des événements) intégré présente le compte de service en tant que membre (**Event Log Readers (Lecteurs des journaux d'événements)** > **Properties (Propriétés)** > **Members (Membres)**).

**STEP 6 |** Affectez des autorisations de compte au dossier d'installation pour autoriser le compte de service à accéder au dossier d'installation de l'agent et y lire les journaux de configuration et de rédaction.

Vous n'avez à effectuer cette étape que si le compte de service que vous avez configuré pour l'agent User-ID n'est pas un administrateur de domaine ni un administrateur local sur l'hôte du serveur de l'agent User-ID.

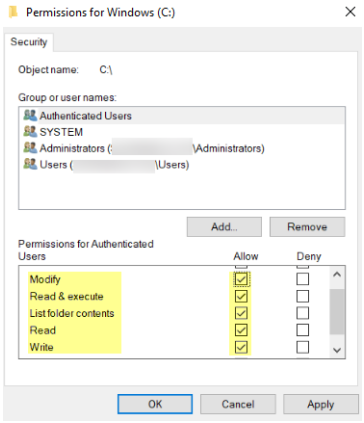
1. À partir de l'Explorateur Windows, accédez à **`C:\Program Files(x86)\Palo Alto Networks`**, puis faites un clic droit sur le dossier et sélectionnez **Properties (Propriétés)**.
2. Dans l'onglet **Security (Sécurité)**, cliquez sur **Edit (Modifier)**.




3. **Add (Ajoutez)** le compte de service de l'agent User-ID et **Allow (Autorisez)** des autorisations **Modify (Modifier)**, **Read & execute (Lire et exécuter)**, **List folder contents**

**(Afficher le contenu du dossier)**, **Read (Lire)** et **Write(Écrire)**, puis cliquez sur **OK** pour enregistrer les paramètres du compte.

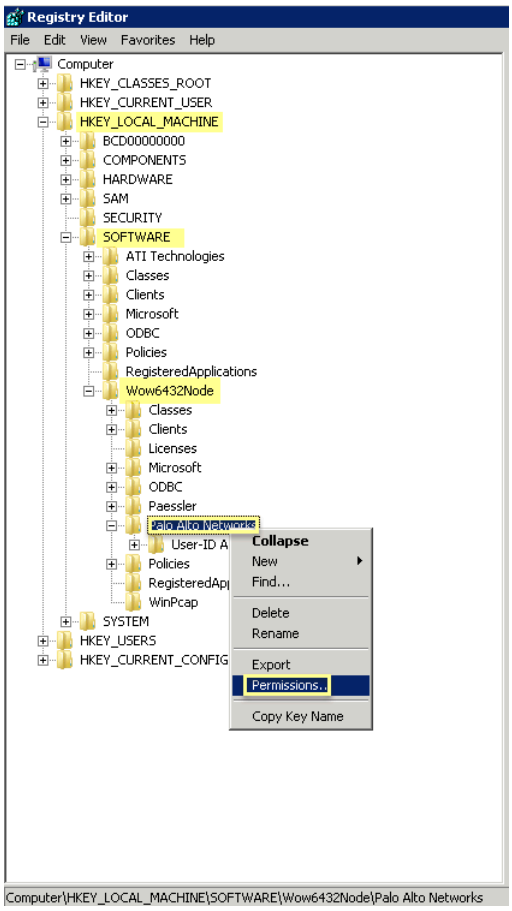



*Si vous ne voulez pas configurer les autorisations individuelles, vous pouvez plutôt* ***Allow (Autoriser)*** *l'autorisation* ***Full Control (Contrôle total)****.*

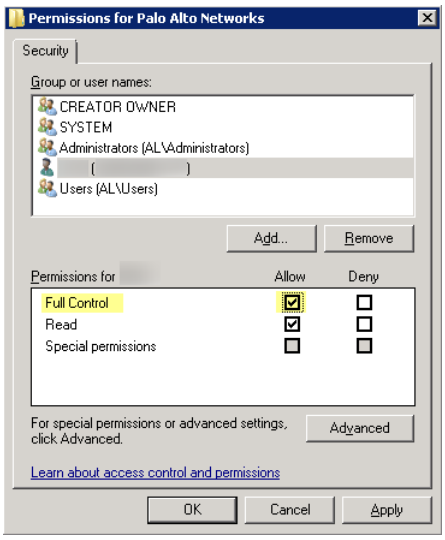
**STEP 7 |** Pour permettre à l'agent d'effectuer des modifications de configuration (par exemple, si vous sélectionnez un autre niveau de journalisation, accordez les autorisations du compte de service à la sous-arborescence de registre de l'agent User-ID.

1. Sélectionnez **Start (Démarrer)** > **Run (Exécuter)**, puis saisissez **`regedt32`** et accédez à la sous-arborescence Palo Alto Networks à l'un des emplacements suivants :
   - **Systèmes 32 bits** : `HKEY_LOCAL_MACHINE\Software\ Palo Alto Networks`
   - **Systèmes 64 bits** : `HKEY_LOCAL_MACHINE\Software\WOW6432Node\PaloAlto Networks`
2. Faites un clic droit sur le nœud **Palo Alto Networks** et sélectionnez **Permissions (Autorisations)**.




3. Accordez le **Full Control (Contrôle total)** au compte de service de l'agent User-ID et cliquez sur **OK (OK)** pour enregistrer le paramètre.




**STEP 8 |** Désactivez les privilèges du compte de service qui ne sont requis.

En veillant à ce que le compte de service User-ID dispose du nombre minimal de privilèges de compte, vous pouvez réduire la surface d'attaque dans l'éventualité où le compte était infecté.

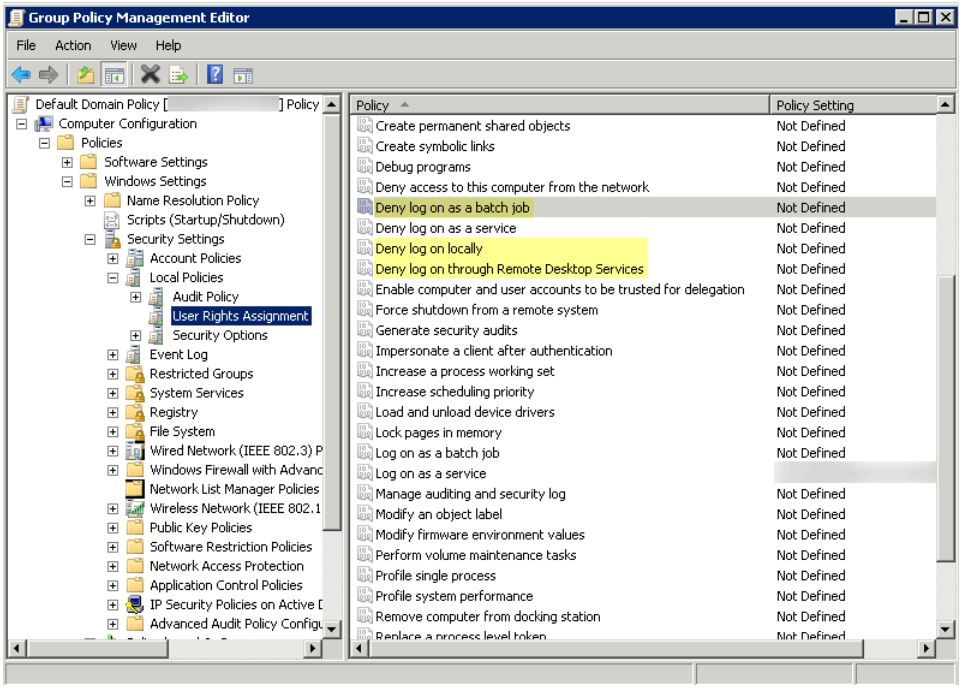
Pour veiller à ce que le compte User-ID possède le minimum de privilèges nécessaires, refusez les privilèges suivants sur le compte.

- **Refuser la connexion interactive du compte de service User-ID** : bien que le compte de service User-ID ait besoin des droits de lecture et d'analyse des journaux des événements Active Directory, il n'a pas besoin de se connecter interactivement aux serveurs ou aux systèmes. Vous pouvez restreindre ce privilège en utilisant des politiques de groupe ou un compte de service géré (reportez-vous à TechNet de Microsoft pour obtenir de plus amples renseignements).

  1. Sélectionnez **Group Policy Management Editor (Éditeur de gestion de la politique de groupe)** > **Default Domain Policy (Politique par défaut du domaine)** > **Computer Configuration (Configuration de l'ordinateur)** > **Policies (Politiques)** > **Windows Settings (Paramètres Windows)** > **Security Settings (Paramètres de sécurité)** > **User Rights Assignment (Affectation des droits d'utilisateur)**.
  2. Pour **Deny log on as a batch job (Refuser la connexion en tant que travail par lots)**, **Deny log on locally (Refuser la connexion localement)** et **Deny log on through Remote Desktop Services (Refuser la connexion par l'intermédiaire des services de bureau à distance)**, faites un clic droit sur **Properties (Propriétés)**.

3. Sélectionnez **Define these policy settings (Définir ces paramètres de politique)** > **Add User or Group (Ajouter l'utilisateur ou le groupe)**, ajoutez le nom du compte de service, puis cliquez sur **OK**.

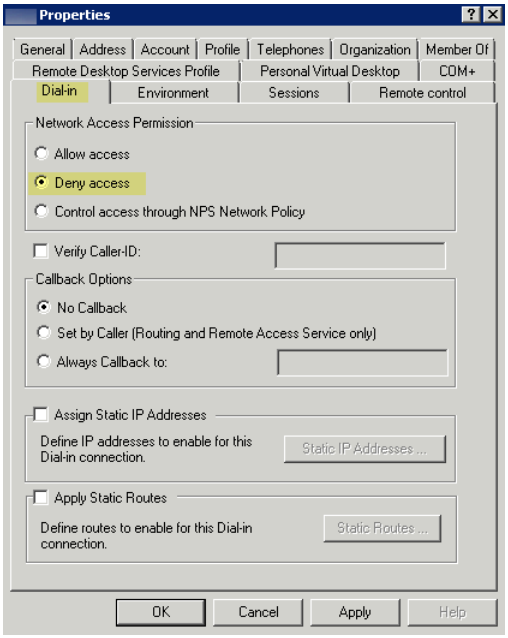



- **Refuser l'accès à distance pour le compte de service User-ID** : cette option empêche un pirate d'utiliser le compte pour accéder à votre réseau à partir de l'extérieur.

  1. Sélectionnez **Start (Démarrer)** > **Run (Exécuter)**, saisissez **MMC**, et sélectionnez **File (Fichier)** > **Add/Remove Snap-in (Ajouter / Supprimer un composant logiciel enfichable)** > **Active Directory Users and Computers (Utilisateurs et Ordinateurs Active Directory)** > **Users (Utilisateurs)**.
  2. Faites un clic droit sur le nom du compte de service, puis sélectionnez **Properties (Propriétés)**.

3. Sélectionnez **Dial-in (Accès entrant)**, puis **Deny (Refusez)** la **Network Access Permission (Autorisation d'accès au réseau)**.




**STEP 9 |** Puis, passez à l'étape suivante : Configuration du mappage d'utilisateur à l'aide de l'agent User-ID Windows.

## Configurer un compte de service pour l'agent User-ID intégré à PAN-OS

Créez un compte de service Active Directory (AD) dédié pour que l'agent User-ID intégré à PAN-OS puisse accéder aux services et aux hôtes qu'il surveillera pour collecter les mappages d'utilisateur. Vous devez créer un compte de service dans chaque domaine que l'agent surveillera. Après avoir activé les permissions requises pour le compte de service, procédez à la Configuration du mappage d'utilisateur à l'aide de l'agent User-ID intégré à PAN-OS.

*Le flux de travail suivant précise tous les privilèges requis et fournit une orientation quant aux fonctionnalités de User-ID qui exigent des privilèges qui pourraient présenter une menace. Vous pourrez ainsi décider de la meilleure manière d'identifier les utilisateurs sans compromettre votre niveau de sécurité global.*

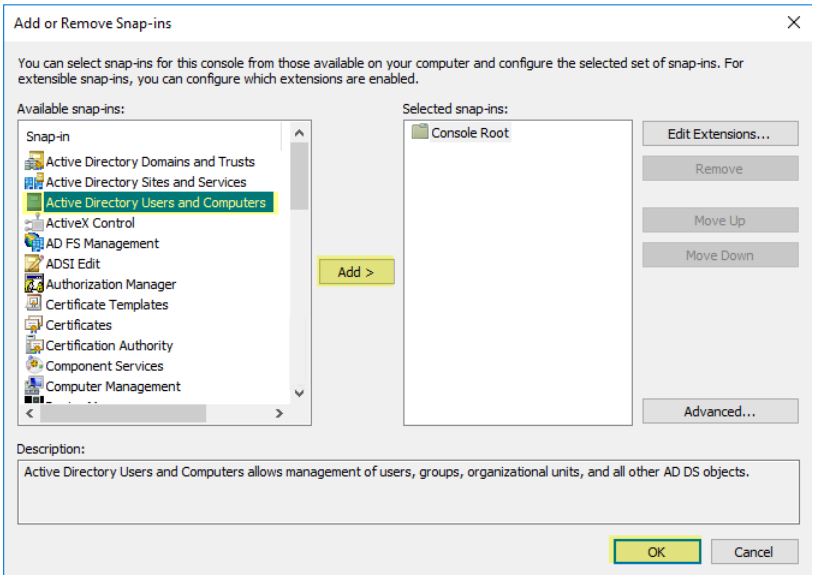
**STEP 1 |** Créez un compte de service AD pour l'agent User-ID.

Vous devez créer un compte de service dans chaque domaine que l'agent surveillera.

1. Connectez-vous au contrôleur de domaine.
2. Faites un clic droit sur l'icône Windows (), **Search (Cherchez)** des **`Active Directory Users and Computers`**, puis lancez l'application.
3. Ouvrez l'arborescence du domaine dans le volet de navigation, faites un clic droit sur **Managed Service Accounts (Comptes de service gérés)**, puis sélectionnez **New (Nouveau)** > **User (Utilisateur)**.
4. Saisissez le **First Name (Prénom)**, le **Last Name (Nom)** et le **User logon name (Nom de connexion)** de l'utilisateur, puis cliquez sur **Suivant**.
5. Saisissez le **Password (Mot de passe)** et **Confirm Password (Confirmez le mot de passe)**, puis cliquez sur **Next (Suivant)** et sur **Finish (Terminer)**.

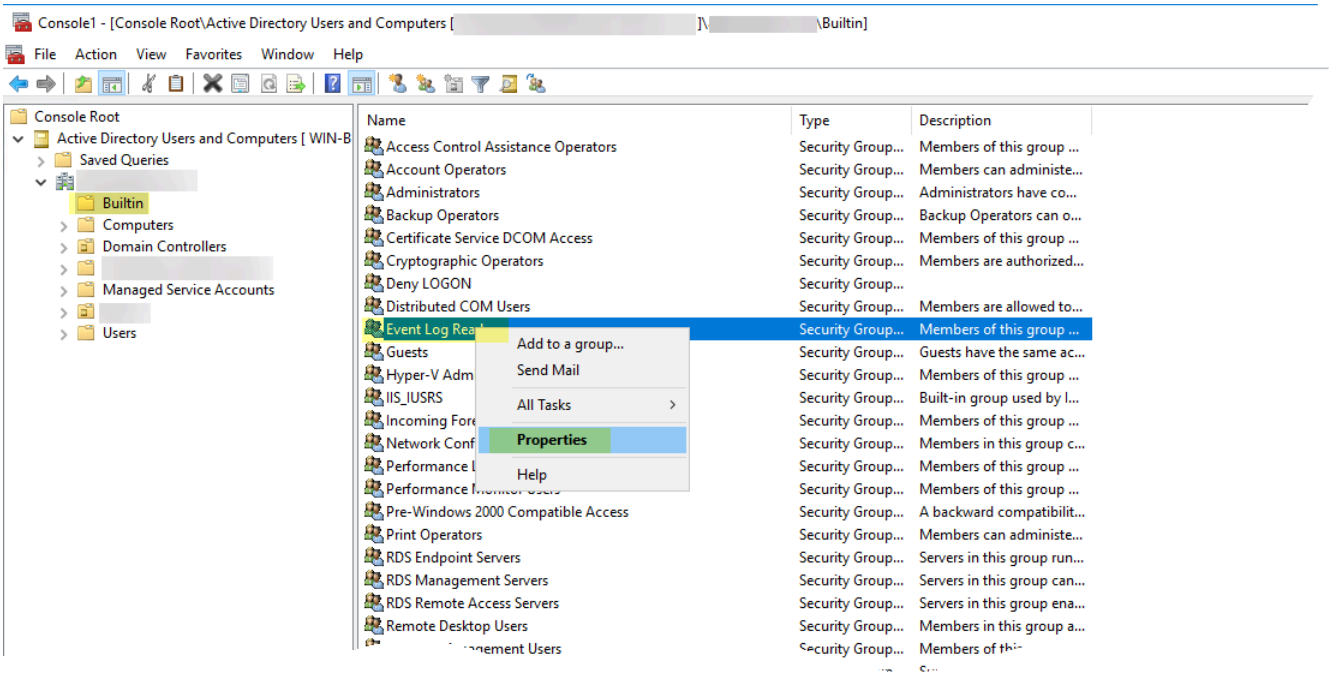
**STEP 2 |** Si vous souhaitez utiliser la Surveillance du serveur pour identifier les utilisateurs, ajoutez le compte de service au groupe intégré Event Log Reader (Lecteurs des journaux des événements) afin d'accorder au compte de service les privilèges de lecture des événements des journaux de sécurité.

1. Sur le contrôleur du domaine ou le serveur Exchange qui contient les journaux que vous voulez que l'agent User-ID lise, ou sur le serveur membre qui reçoit les événements du transfert des journaux Windows, sélectionnez **Start (Démarrer)** > **Run (Exécuter)**, et saisissez **`MMC`**.
2. Sélectionnez **File (Fichier)** > **Add/Remove Snap-in (Ajouter/Supprimer un composant logiciel enfichable)** > **Active Directory Users and Computers** > **Add (Aouter)**, puis cliquez sur **OK** pour exécuter la MMC et le composant logiciel enfichable Active Directory Users and Computers.

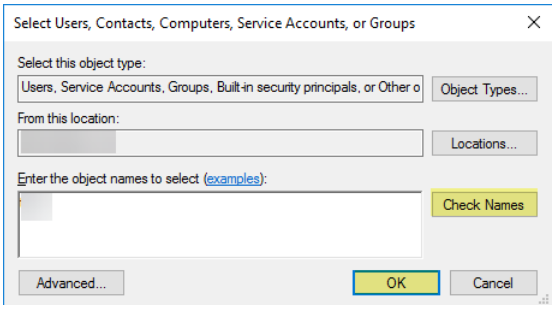


3. Accédez au dossier intégré du domaine, faites un clic droit sur le groupe **Event Log Reader (Lecteurs des journaux des événements)**, puis sélectionnez **Properties (Propriétés)** > **Members (Membres)**.




4. **Add (Ajoutez)** le compte de service, puis cliquez sur **Check Names (Vérifier les noms)** pour vérifier que le nom d'objet est correct.




5. Cliquez deux fois sur **OK (OK)** pour enregistrer les paramètres.
6. Confirmez que le groupe Event Log Reader (Lecteurs des journaux des événements) intégré présente le compte de service en tant que membre (**Event Log Readers (Lecteurs des journaux d'événements)** > **Properties (Propriétés)** > **Members (Membres)**).

**STEP 3 |** Si vous souhaitez utiliser WMI pour collecter les données des utilisateurs, affectez des privilèges DCOM au compte de service pour qu'il puisse utiliser les requêtes WMI sur les serveurs surveillés.

1. Sélectionnez **Active Directory Users and Computers (Utilisateurs et ordinateurs Active Directory)** > **<your domain> (Votre domaine)** > **Builtin (Intégré)** > **Distributed COM Users (Utilisateurs COM distribués)**.
2. Faites un clic droit sur **Properties (Propriétés)** > **Members (Membres)** > **Add (Ajouter)**, puis saisissez le nom du compte de service.

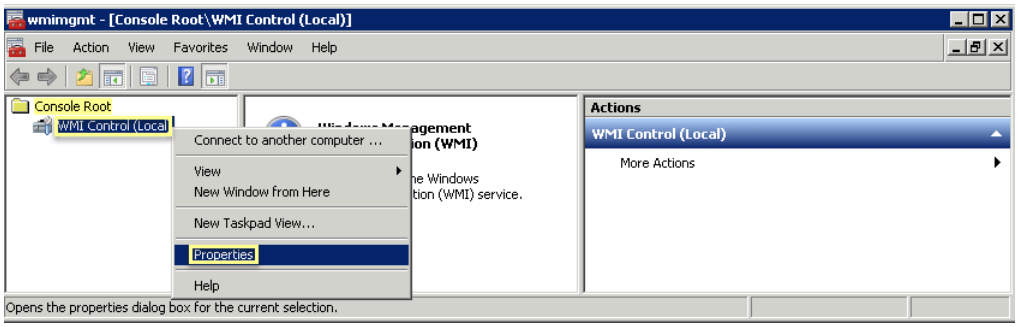
 

**STEP 4 |** Si vous prévoyez d'utiliser le sondage WMI, accordez au compte de service les droits de lecture sur l'espace de noms CIMV2 sur les contrôleurs de domaine que vous souhaitez surveiller et affectez les permissions requises sur les systèmes client devant faire l'objet du sondage.

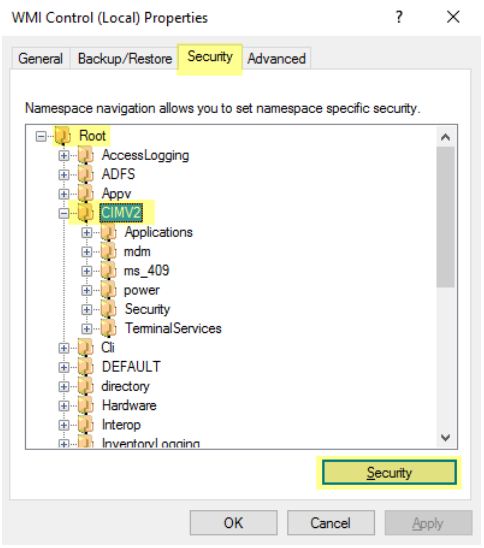
*N'activez pas l'interrogation du client sur les réseaux haute sécurité. L'interrogation du client peut générer une grande quantité de trafic sur le réseau et peut constituer une menace pour la sécurité lorsqu'il est mal configuré. Au lieu de cela, collectez des informations de mappage d'utilisateur à partir de sources plus isolées et fiables telles que les contrôleurs de domaine et par l'intermédiaire des intégrations avec Syslog ou l'API XML, qui ont l'avantage supplémentaire de vous permettre de recueillir en toute sécurité des informations de mappage d'utilisateurs à partir de n'importe quel type de périphérique ou de système d'exploitation, plutôt que de se cantonner aux clients Windows.*

Effectuez cette tâche sur chaque système client que l'agent User-ID sondera pour extraire les informations de mappage d'utilisateur :

1. Faites un clic droit sur l'icône Windows (), **Search (Cherchez)** **`wmimgmt.msc`** et lancez la console de gestion WMI.
2. Dans l'arborescence de la console, faites un clic droit sur **WMI Control (Contrôle WMI)**, puis sélectionnez **Properties (Propriétés)**.




3. Sélectionnez l'onglet **Security (Sécurité)**, puis sélectionnez **Root (Racine)** > **CIMV2**, et cliquez sur le bouton **Security (Sécurité)**.

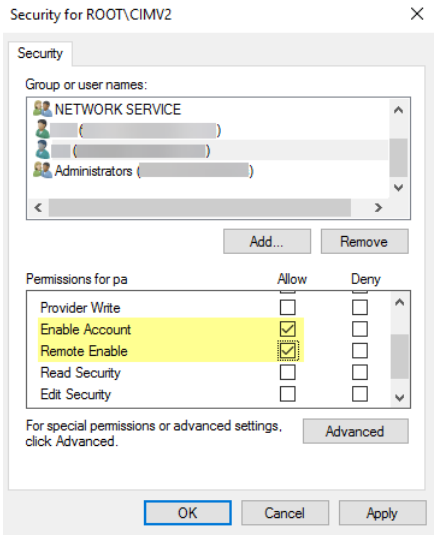


4. **Add (Ajoutez)** le nom du compte de service que vous avez créé, **Check Names (Vérifiez les noms)** pour vérifier votre entrée, puis cliquez sur **OK (OK)**.

   *Vous pourriez devoir changer les **Locations (Emplacements)** ou cliquer sur **Advanced (Avancé)** pour obtenir les noms de compte. Pour plus d'informations, reportez-vous à l'aide de la boîte de dialogue.*

5. Dans la section Permissions (Permissions) de **<nom d'utilisateur>**, **Allow (Autorisez)** les droits **Enable Account (Activation du compte)** et **Remote Enable (Activation à distance)**.




6. Cliquez deux fois sur **OK**.
7. Utilisez le composant Groupes et utilisateurs locaux de la console MMC (lusrmgr.msc) pour ajouter le compte de service aux utilisateurs du Distributed Component Object Model (modèle de composant objet distribué ; DCOM) et aux groupes d'utilisateurs du bureau à distance sur le système à sonder.

**STEP 5 |** (Non recommandé) Pour permettre à l'agent de surveiller les sessions des utilisateurs pour sonder les serveurs Windows afin d'obtenir les informations de mappage des utilisateurs, affectez les privilèges d'opérateur du serveur au compte de service.

*Puisque ce groupe dispose également des privilèges nécessaires pour éteindre et redémarrer les serveurs, n'affectez le compte à ce groupe que si la surveillance des sessions des utilisateurs est très importante.*

1. Sélectionnez **Active Directory Users and Computers (Utilisateurs et ordinateurs Active Directory)** > **<your domain> (Votre domaine)** > **Builtin (Intégré)** > **Server Operators Group (Groupe d'opérateurs de serveur)**.
2. Faites un clic droit sur **Properties (Propriétés)** > **Members (Membres)** > **Add (Ajouter)**, puis ajoutez le nom du compte de service.

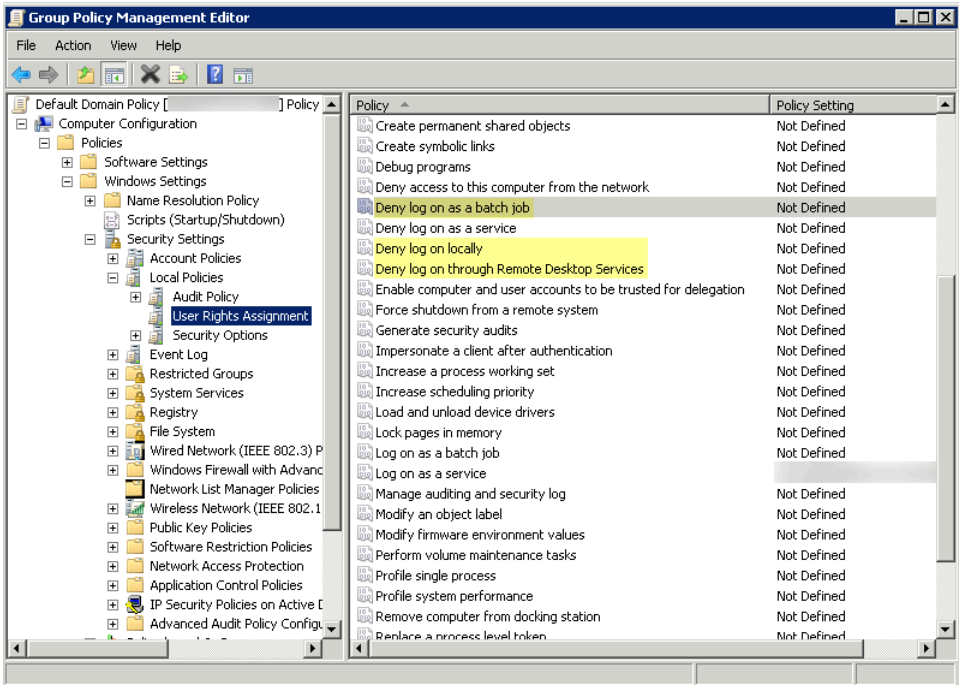
**STEP 6 |** Désactivez les privilèges du compte de service qui ne sont requis.

En veillant à ce que le compte de service User-ID dispose du nombre minimal de privilèges de compte, vous pouvez réduire la surface d'attaque dans l'éventualité où le compte était infecté.

Pour veiller à ce que le compte User-ID possède le minimum de privilèges nécessaires, refusez les privilèges suivants sur le compte :

- **Refuser la connexion interactive du compte de service User-ID** : bien que le compte de service User-ID ait besoin des droits de lecture et d'analyse des journaux des événements Active Directory, il n'a pas besoin de se connecter interactivement aux serveurs ou aux systèmes. Vous pouvez restreindre ce privilège en utilisant des politiques de groupe ou un compte de service géré (reportez-vous à TechNet de Microsoft pour obtenir de plus amples renseignements).

  1. Sélectionnez **Group Policy Management Editor (Éditeur de gestion de la politique de groupe)** > **Default Domain Policy (Politique par défaut du domaine)** > **Computer Configuration (Configuration de l'ordinateur)** > **Policies (Politiques)** > **Windows Settings (Paramètres Windows)** > **Security Settings (Paramètres de sécurité)** > **User Rights Assignment (Affectation des droits d'utilisateur)**.
  2. Sous **Deny log on as a batch job (Refuser la connexion en tant que travail par lots)**, **Deny log on locally (Refuser la connexion localement)** et **Deny log on through Remote Desktop Services (Refuser la connexion par l'intermédiaire des services de bureau à distance)**, faites un clic droit sur **Properties (Propriétés)**, puis sélectionnez **Define these policy settings (Définir ces paramètres de politique)** > **Add User or Group (Ajouter l'utilisateur ou le groupe)**, ajoutez le nom du compte de service, puis cliquez sur **OK**.



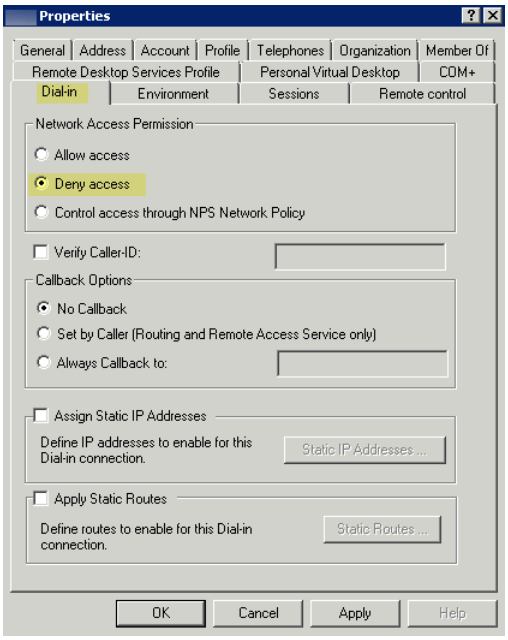

- **Refuser l'accès à distance pour le compte de service User-ID** : cette option empêche un pirate d'utiliser le compte pour accéder à votre réseau à partir de l'extérieur.

  1. **Start (Démarrer)** > **Run (Exécuter)**, saisissez **MMC**, et sélectionnez **File (Fichier)** > **Add/Remove Snap-in (Ajouter / Supprimer un composant logiciel enfichable)** > **Active**

**Directory Users and Computers (Utilisateurs et Ordinateurs Active Directory)** > **Users (Utilisateurs)**.

2. Faites un clic droit sur le nom du compte de service, puis sélectionnez **Properties (Propriétés)**.
3. Sélectionnez **Dial-in (Accès entrant)**, puis **Deny (Refusez)** la **Network Access Permission (Autorisation d'accès au réseau)**.




**STEP 7 |** Puis, passez à l'étape suivante : Configuration du mappage d'utilisateur à l'aide de l'agent User-ID intégré à PAN-OS.

# Configuration du mappage d'utilisateur à l'aide de l'agent User-ID Windows

Dans la plupart des cas, la majorité des utilisateurs de votre réseau peut se connecter à vos services de domaines surveillés. Pour ces utilisateurs, l'agent User-ID de Palo Alto Networks surveille les événements de connexion sur les serveurs et effectue le mappage d'adresse IP/nom d'utilisateur. La méthode selon laquelle vous configurez l'agent User-ID dépend de la taille de votre environnement et de l'emplacement de vos serveurs de domaines. Il est recommandé de placer vos agents User-ID près des serveurs qu'ils surveilleront (autrement dit, les serveurs surveillés et l'agent User-ID Windows ne doivent pas être connectés via une liaison réseau étendue), car la plupart du trafic de mappage d'utilisateur se situe entre l'agent et le serveur surveillé et qu'une très faible proportion du trafic (le delta des mappages d'utilisateurs depuis la dernière mise à jour) se situe entre l'agent et le pare-feu.

Les rubriques suivantes décrivent l'installation et la configuration de l'agent User-ID, ainsi que la configuration du pare-feu pour récupérer les informations de mappage de l'agent :

- Installation de l'agent User-ID basé sur Windows
- Configuration de l'agent User-ID Windows pour le mappage d'utilisateur

## Installation de l'agent User-ID basé sur Windows

La procédure suivante décrit l'installation de l'agent User-ID sur un serveur membre du domaine et la configuration du compte de service avec les autorisations requises. Si vous effectuez une mise à niveau, le programme d'installation supprimera automatiquement l'ancienne version ; il est toutefois recommandé de sauvegarder le fichier config.xml avant d'exécuter le programme d'installation.

*Pour plus d'informations sur la configuration système requise pour l'installation de l'agent User-ID Windows et sur les versions de système d'exploitation serveur prises en charge, reportez-vous à la section* Notes de version de l'agent User-ID *et la* Matrice de compatibilité Palo Alto Networks.

**STEP 1 |** Créez un compte de service Active Directory spécial pour que l'agent User-ID puisse accéder aux services et aux hôtes qu'il surveillera pour recueillir les informations de mappage d'utilisateur.

Créez un compte de service dédié pour l'agent User-ID et accordez les autorisations nécessaires pour l'agent User-ID Windows.

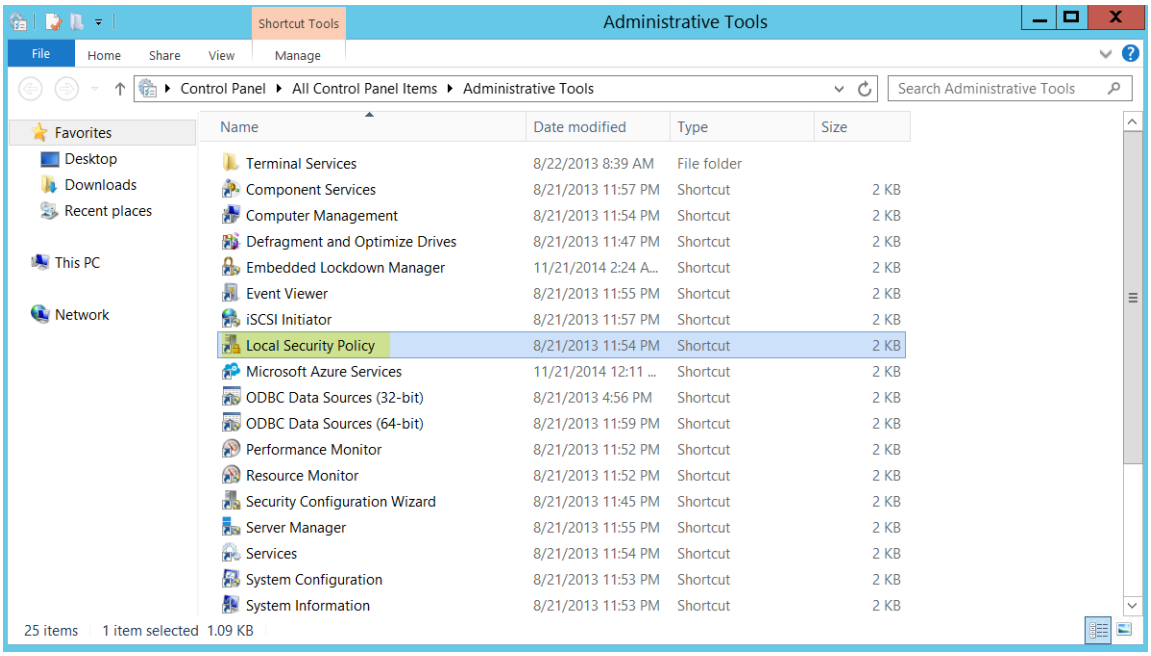
1. Activez le compte de service pour qu'il ouvre une session en tant que service en configurant la politique locale ou de groupe.
   1. Pour configurer la politique de groupe si vous installez les agents User-ID Windows sur plusieurs serveurs, sélectionnez **Group Policy Management (Gestion de la politique de groupes)** > **Default Domain Policy (Politique de domaine par défaut)** > **Computer Configuration (Configuration de l'ordinateur)** > **Policies (Politiques)** > **Windows Settings (Paramètres Windows)** > **Security Settings (Paramètres de sécurité)** > **Local Policies (Politiques locales)** > **User Rights Assignment (Affectation des droits d'utilisateurs)** pour le serveur Windows qui est l'hôte de l'agent.
   2. Faites un clic droit sur **Log on as a service (Ouvrir une session en tant que service)**, puis sélectionnez **Properties (Propriétés)**.

3. Ajoutez le nom d'utilisateur du compte de service ou le groupe intégré (les administrateurs possèdent ce privilège par défaut).

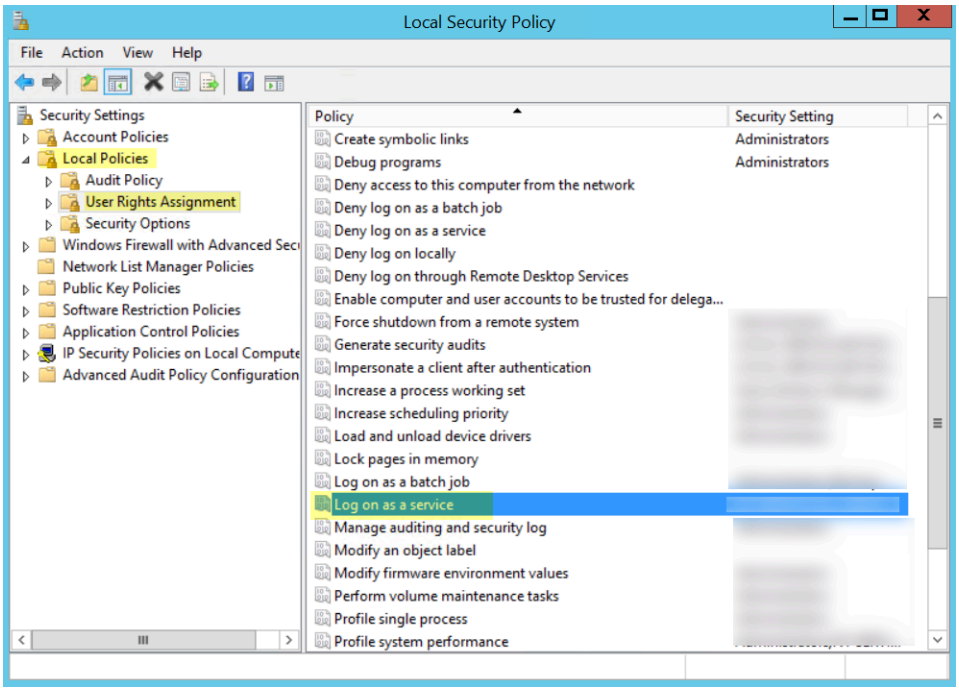
*La permission d'ouvrir une session en tant que service ne s'avère nécessaire que localement sur le serveur Windows qui est l'hôte de l'agent. Si vous utilisez un seul agent User-ID, vous pouvez accorder les permissions localement sur l'hôte de l'agent en utilisant les instructions suivantes.*

1. Pour affecter les permissions localement, sélectionnez **Control Panel (Panneau de commande)** > **Administrative Tools (Outils administratifs)** > **Local Security Policy (Politique de sécurité locale)**.

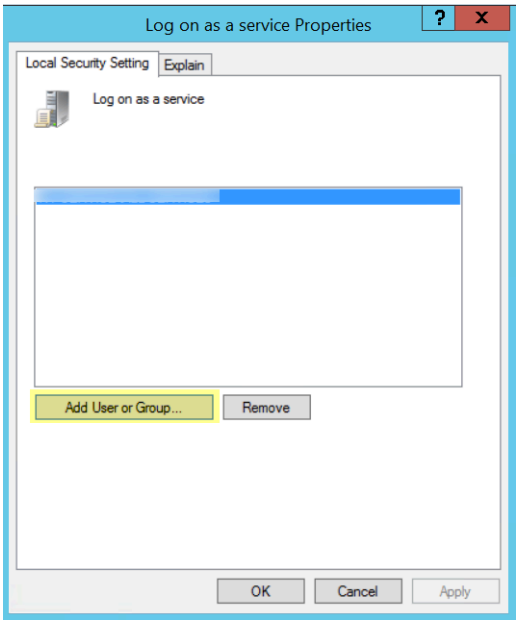


2. Sélectionnez **Local Policies (Politiques locales)** > **User Rights Assignment (Affectation des droits d'utilisateurs)** > **Log on as a service (Ouvrir une session en tant que service)**.

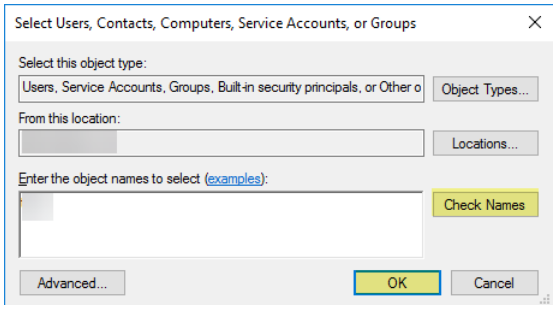



3. **Add User or Group (Ajoutez un utilisateur ou un groupe)** pour ajouter le compte de service.



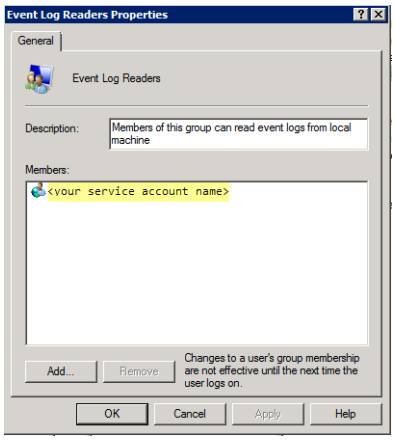
4. Saisissez le nom du compte de service au format **`domain\username`** dans le champ **Enter the object names to select (Saisissez les noms d'objet à sélectionner)**, puis cliquez sur **OK**.




Pour confirmer la validité du nom du compte de service, **Check Names (Vérifiez les noms)**.

2. Si vous souhaitez utiliser la surveillance du serveur pour identifier les utilisateurs, ajoutez le compte de service au groupe intégré Event Log Reader (Lecteurs des journaux des événements) pour lui accorder les privilèges de lecture des événements des journaux de sécurité.

   1. Sur le contrôleur du domaine ou le serveur Exchange qui contient les journaux que vous voulez que l'agent User-ID lise, ou sur le serveur membre qui reçoit les événements du transfert des journaux Windows, exécutez la console MMC et lancez le composant logiciel enfichable Utilisateurs et ordinateurs Active Directory.
   2. Accédez au dossier intégré du domaine, faites un clic droit sur le groupe **Event Log Reader (Lecteurs des journaux des événements)**, puis sélectionnez **Add to Group (Ajouter au groupe)** pour ouvrir la boite de dialogue des propriétés.
   3. Cliquez sur **Add (Ajouter)**, puis saisissez le nom du compte de service que le service User-ID utilisera et cliquez sur **Check Names (Vérifier les noms)** pour vérifier que le nom d'objet est correct.
   4. Cliquez deux fois sur **OK (OK)** pour enregistrer les paramètres.
   5. Confirmez que le groupe Event Log Reader (Lecteurs des journaux des événements) intégré présente le compte de service en tant que membre.

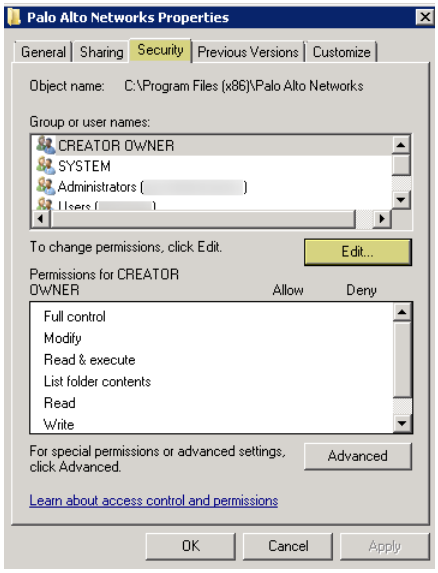


3. Affectez des autorisations de compte au dossier d'installation pour autoriser le compte de service à accéder au dossier d'installation de l'agent et y lire les journaux de configuration et de rédaction.

   Vous n'avez à effectuer cette étape que si le compte de service que vous avez configuré pour l'agent User-ID n'est pas un administrateur de domaine ni un administrateur local sur l'hôte du serveur de l'agent User-ID.

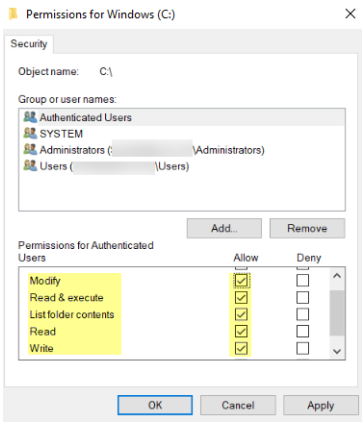
   1. À partir de l'Explorateur Windows, accédez à **`C:\Program Files(x86)\Palo Alto Networks`** pour les systèmes 32 bits, puis faites un clic droit sur le dossier et sélectionnez **Properties (Propriétés)**.
   2. Dans l'onglet **Security (Sécurité)**, cliquez sur **Edit (Modifier)**.




   3. **Add (Ajoutez)** le compte de service de l'agent User-ID et affectez-lui des autorisations **Modify (Modifier)**, **Read & execute (Lire et exécuter)**, **List folder contents (Afficher le**

**contenu du dossier) Read (Lire)** et **Write (Écrire)**, puis cliquez sur **OK** pour enregistrer les paramètres du compte.




*Si vous voulez autoriser le compte de service à accéder aux clés de registre de l'agent User-ID, **Allow (Autorisez)** la permission **Full Control (Contrôle total)**.*

4. Accordez les autorisations du compte de service à la sous-arborescence de registre de l'agent User-ID :
   1. Exécutez **`regedt32`** et accédez à la sous-arborescence Palo Alto Networks à l'un des emplacements suivants : `HKEY_LOCAL_MACHINE\Software\Palo Alto Networks`.
   2. Faites un clic droit sur le nœud Palo Alto Networks et sélectionnez **Permissions (Autorisations)**.
   3. Accordez le **Full Control (Contrôle total)** au compte de service de l'agent User-ID et cliquez sur **OK (OK)** pour enregistrer le paramètre.

**STEP 2 |** Sélectionnez l'emplacement d'installation de l'agent User-ID.

L'agent User-ID interroge les journaux du contrôleur de domaine et du serveur Exchange à l'aide de Microsoft Remote Procedure Calls (Appels de procédure distants Microsoft ; MSRPC). Lors de la connexion initiale, l'agent transfère la plupart des 50 000 événements récents du journal pour mapper les utilisateurs. Lors de chaque connexion subséquente, l'agent transfère les événements qui sont assortis d'un horodatage ultérieur à la dernière communication avec le contrôleur de domaine. Par conséquent, installez toujours un ou plusieurs agents User-ID sur chaque site dont les serveurs doivent être surveillés.

- Vous devez installer l'agent User-ID sur un système qui exécute l'une des versions de système d'exploitation prises en charge suivantes : reportez-vous à la section « Compatibilité de l'agent User-ID avec le système d'exploitation » dans la matrice de comptabilité. Le système doit également répondre aux exigences minimales (voir les Notes de version de l'agent User-ID).
- Assurez-vous que le système qui hébergera l'agent User-ID est membre du même domaine que les serveurs qu'il surveillera.
- Il est recommandé d'installer l'agent User-ID près des serveurs qu'il surveillera : il y a plus de trafic entre l'agent User ID et les serveurs surveillés qu'entre l'agent User-ID et le pare-feu, par conséquent, le placement de l'agent près des serveurs surveillés optimise l'utilisation de la bande passante.

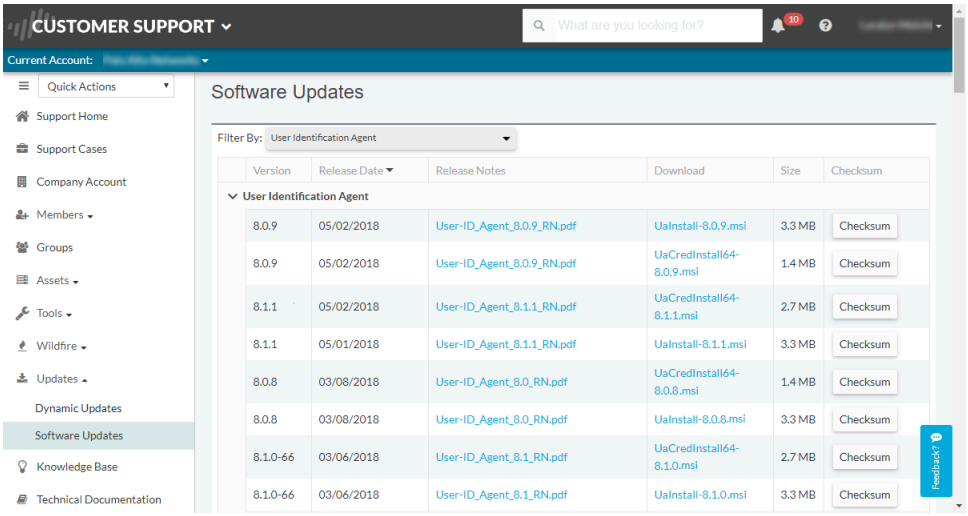
- Pour veiller au mappage le plus complet des utilisateurs, vous devez surveiller tous les contrôleurs de domaine qui traitent l'authentification des utilisateurs que vous voulez mapper. Vous pouvez installer plusieurs agents User-ID pour surveiller toutes vos ressources de manière efficace.
- Si vous utilisez l'agent User-ID pour la détection des informations d'identification, vous devez l'installer sur le read-only domain controller (contrôleur de domaine en lecture seule ; RODC). Il est recommandé de déployer un agent distinct à cette fin. N'utilisez pas l'agent User-ID qui est installé sur le RODC pour mapper les adresses IP à des utilisateurs. Le programme d'installation de l'agent User-ID pour la détection des informations d'identification se nomme UaCredInstall64-x.x.x.msi.

**STEP 3 |** Téléchargez le programme d'installation de l'agent User-ID.

*Installez la version d'agent User-ID identique à la version PAN-OS exécutée sur les pare-feu. Si aucune version d'agent User-ID ne correspond à la version PAN-OS, installez la dernière version qui est la plus proche de la version PAN-OS.*

1. Connectez-vous au portail de support client de Palo Alto Networks.
2. Sélectionnez **Updates (Mises à jour)** > **Software Updates (Mises à jour logicielles)**.
3. Définissez **Filter By (Filtrer par)** sur **User Identification Agent (Agent d'identification utilisateur)**, puis sélectionnez la version de l'agent User-ID que vous souhaitez installer dans la colonne Download (Téléchargement) correspondante. Le nom de fichier utilise le format suivant : `UaInstall-x.x.x.msi` (où `x` représente le numéro de version). Par exemple, pour télécharger la version 10.0 de l'agent User-ID, sélectionnez **UaInstall-10.0.0-0.msi**.

   Si vous utilisez l'agent User-ID pour la credential detection (détection des informations d'identification), téléchargez plutôt le fichier `UaCredInstall64-xxx.msi`. Téléchargez et installez `UaCredInstall64-xxx.msi` uniquement si vous utilisez l'ID utilisateur pour la détection des informations d'identification.
4. Enregistrez le fichier sur les systèmes sur lesquels vous prévoyez d'installer l'agent.



**STEP 4 |** Exécutez le programme d'installation en tant qu'administrateur.

1. Ouvrez le menu **Start (Démarrer)** de Windows, faites un clic droit sur le programme **Command Prompt (Invite de commandes)**, puis sélectionnez **Run as administrator (Exécuter en tant qu'administrateur)**.
2. À partir de la ligne de commande, exécutez le fichier .msi que vous avez téléchargé. Par exemple, si vous enregistrez le fichier .msi sur le Bureau, saisissez ce qui suit :

```
C:\Users\administrator.acme>cd Desktop
C:\Users\administrator.acme\Desktop>UaInstall-6.0.0-1.msi
```

3. Suivez les invites du programme d'installation pour installer l'agent à l'aide des paramètres par défaut. Par défaut, l'agent est installé sous **`C:\Program Files(x86)\Palo Alto Networks`**, mais vous pouvez **Browse (Parcourir)** un emplacement différent.
4. Lorsque l'installation est terminée, **Close (Fermez)** la fenêtre du programme d'installation.

**STEP 5 |** Lancez l'application Agent User-ID en tant qu'administrateur.

Ouvrez le menu **Start (Démarrer)** de Windows, faites un clic droit sur le programme **User-ID Agent (Agent User-ID)**, puis sélectionnez **Run as administrator (Exécuter en tant qu'administrateur)**.

*Vous devez exécuter l'application de l'agent User-ID en tant qu'administrateur pour installer l'application, valider les changements de configuration ou désinstaller l'application.*

**STEP 6 |** (Facultatif) Modifiez le compte de service que l'agent User-ID utilise pour se connecter.

Par défaut, l'agent utilise le compte administrateur utilisé pour installer le fichier .msi. Pour modifier le compte pour qu'il devienne restreint :

1. Sélectionnez **User Identification(Identification utilisateur)** > **Setup (Configuration)** et cliquez sur **Edit (Modifier)**.
2. Sélectionnez l'onglet **Authentication (Authentification)** et saisissez le nom du compte de service que l'agent User-ID utilisera dans le champ **User name for Active Directory (Nom d'utilisateur pour Active Directory)**.
3. Saisissez le **Password (Mot de passe)** du compte spécifié.
4. **Commit (Validez)** les modifications apportées à la configuration de l'agent User-ID pour redémarrer le service au moyen des informations d'identification du compte de service.

**STEP 7 |** (Facultatif) Affectez vos propres certificats pour l'authentification mutuelle entre l'agent User-ID Windows et le pare-feu.

1. Obtenez votre certificat pour l'agent User-ID Windows au moyen de l'une des méthodes suivantes. Chargez le certificat du serveur au format Privacy Enhanced Mail (courrier à confidentialité améliorée ; PEM) et la clé chiffrée du certificat du serveur.
   - Générez un certificat et exportez-le aux fins de chargement sur l'agent User-ID Windows.
   - Exportez un certificat de votre Certificate Authority (autorité de certification ; CA), puis chargez-le sur l'agent User-ID Windows.
2. Ajoutez un certificat de serveur à l'agent User-ID Windows.
   1. Sur l'agent User-ID Windows, sélectionnez **Server Certificate (Certificat du serveur)**, puis cliquez sur **Add (Ajouter)**.
   2. Saisissez le chemin et le nom du fichier du certificat envoyé par la CA ou accédez au fichier du certificat.
   3. Entrez la phrase secrète de la clé privée.
   4. Cliquez sur **OK (OK)**, puis sur **Commit (Valider)**.
3. Chargez un certificat sur le pare-feu pour valider l'identité de l'agent User-ID Windows.
4. Configurez le profil du certificat du périphérique client (pare-feu ou Panorama).
   1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificats)**.
   2. Configuration d'un profil de certificat.

      *Vous ne pouvez affecter qu'un seul profil de certificat aux agents User-ID Windows et aux agents Terminal Server (TS). Par conséquent, votre profil de certificat doit comprendre toutes les autorités de certification ayant délivré des certificats chargés sur les agents User-ID et TS connectés.*
5. Affectez le profil de certificat sur le pare-feu.
   1. Sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Connection Security (Sécurité de la connexion)** et cliquez sur le bouton de modification.
   2. Sélectionnez le **User-ID Certificate Profile (Profil de certifcat User-ID)** que vous avez configuré à l'étape précédente.
   3. Cliquez sur **OK**.
6. **Commit (Validez)** vos modifications.

**STEP 8 |** Configurer la détection des informations d'identification avec l'agent User-ID de Windows.

Pour utiliser l'agent User-ID Windows pour détecter l'envoi des informations d'identification et Empêcher le hameçonnage des informations d'identification, vous devez installer le service d'informations d'identification User-ID sur l'agent User-ID Windows. Vous ne pouvez installer ce module d'extension que sur un Read-Only Domain Controller (contrôleur de domaine en lecture seule ; RODC).

## Configuration de l'agent User-ID Windows pour le mappage d'utilisateur

L'agent Windows User-ID Palo Alto Networks est un service Windows qui se connecte aux serveurs de votre réseau (par exemple, aux serveurs Active Directory, Microsoft Exchange et Novell eDirectory) et surveille les événements de connexion dans les journaux. L'agent utilise ces informations pour mapper des adresses IP à des noms d'utilisateurs. Les pare-feu Palo Alto Networks se connectent à l'agent User-ID pour récupérer ces informations de mappage d'utilisateur, qui permettent la visibilité des activités des utilisateurs par nom d'utilisateur plutôt que par adresse IP et la mise en œuvre de la sécurité en fonction de l'utilisateur et du groupe.

*Pour plus d'informations sur les versions de système d'exploitation serveur prises en charge par l'agent User-ID, reportez-vous à la section « Compatibilité de l'agent User-ID avec le système d'exploitation » des* Notes de version de l'agent User-ID*.*

**STEP 1 |** Définissez les serveurs que l'agent User-ID surveillera pour collecter les informations de mappage d'adresse IP/nom d'utilisateur.

L'agent User-ID peut surveiller jusqu'à 100 serveurs, dont un maximum de 50 expéditeurs Syslog.

*Pour pouvoir collecter tous les mappages nécessaires, l'agent User-ID doit se connecter à tous les serveurs auxquels vos utilisateurs se connectent afin de surveiller les fichiers journaux de sécurité de tous les serveurs contenant des événements de connexion.*

1. Ouvrez le menu **Start (Démarrer)** de Windows, puis sélectionnez **User-ID Agent (Agent User-ID)**.
2. Sélectionnez **User Identification (Identification utilisateur)** > **Discovery (Détection)**.
3. Dans la section **Servers (Serveurs)** de l'écran, cliquez sur **Add (Ajouter)**.
4. Saisissez le **Name (Nom)** et la **Server Address (Adresse serveur)** du serveur à surveiller. L'adresse réseau peut être un FQDN ou une adresse IP.
5. Sélectionnez le **Server Type (Type de serveur)** (**Microsoft Active Directory (Microsoft Active Directory)**, **Microsoft Exchange (Microsoft Exchange)**, **Novell eDirectory (Novell eDirectory)** ou **Syslog Sender (Expéditeur Syslog)**), puis cliquez sur **OK (OK)** pour enregistrer la saisie du serveur. Répétez cette étape pour chaque serveur à surveiller.
6. (Optional (Facultatif)) Pour permettre à l'agent Windows User-ID de détecter automatiquement les contrôleurs de domaine de votre réseau à l'aide de recherches DNS, cliquez sur **Auto Discover (Détection automatique)**. Si vous avez de nouveaux contrôleurs de domaine que l'agent d'ID utilisateur Windows doit découvrir, cliquez sur **Auto Discover (Découverte automatique)** chaque fois que vous souhaitez découvrir les nouveaux contrôleurs de domaine.

   *La détection automatique localise uniquement les contrôleurs de domaines ; vous devez ajouter manuellement les serveurs Exchange et eDirectoy, ainsi que les expéditeurs Syslog.*
7. (Facultatif) Pour ajuster la fréquence à laquelle le pare-feu interroge les serveurs configurés pour obtenir les informations de mappage, sélectionnez **User Identification (Identification utilisateur)** > **Setup ( Configuration)**, puis **Edit (Modifiez)** la section Setup (Configuration). Dans l'onglet **Server Monitor (Surveillance du serveur)**, modifiez la valeur dans le champ **Server Log Monitor Frequency (seconds) (Fréquence de surveillance du journal du serveur (secondes))**. Augmentez la valeur de ce champ à 5 secondes dans les

environnements contenant d'anciens contrôleurs de domaines ou des liaisons à latence élevée.

*Assurez-vous que le paramètre **Enable Server Session Read (Activer la lecture de la session serveur)** n'est pas sélectionné. Ce paramètre nécessite que l'agent User-ID possède un compte Active Directory avec des privilèges d'Opérateur de serveur afin de pouvoir lire toutes les sessions utilisateur. Au lieu de cela, utilisez une intégration Syslog ou API XML pour surveiller les sources qui recueillent les événements de connexion et de déconnexion pour tous les types de périphériques et de systèmes d'exploitation (plutôt qu'uniquement Windows), tels que les contrôleurs sans fil et les Network Access Controllers (contrôleurs d'accès au réseau ; NAC).*

8. Cliquez sur **OK** pour enregistrer les paramètres.

**STEP 2 |** Spécifiez les sous-réseaux que l'agent User-ID Windows doit inclure ou exclure de User-ID.

Par défaut, User-ID mappe tous les utilisateurs qui accèdent aux serveurs que vous surveillez.

*Il est recommandé de toujours spécifier les réseaux à inclure et à exclure de User-ID pour garantir que l'agent ne communique qu'avec les ressources internes et pour empêcher le mappage des utilisateurs non autorisés. Vous de devriez activer User-ID que sur les sous-réseaux auxquels les utilisateurs internes de votre organisation se connectent.*

1. Sélectionnez **User Identification (Identification utilisateur)** > **Discovery (Détection)**.
2. **Add (Ajoutez)** une entrée à la liste Inclure/Exclure des réseaux configurés, puis donnez un **Name (Nom)** à l'entrée et saisissez la plage d'adresses IP du sous-réseau sous **Network Address (Adresse réseau)**.
3. Indiquez si le réseau doit être inclus ou exclu :
   - **Include specified network (Inclure le réseau spécifié)** : sélectionnez cette option si vous souhaitez restreindre le mappage des utilisateurs uniquement aux utilisateurs qui sont connectés au sous-réseau spécifié. Par exemple, si vous incluez 10.0.0.0/8, l'agent mappe les utilisateurs qui sont connectés à ce sous-réseau et exclut les autres. Si vous souhaitez que l'agent mappe les utilisateurs des autres sous-réseaux, vous devez répéter ces étapes pour ajouter d'autres réseaux à la liste.
   - **Exclude specified network (Exclure le réseau spécifié)** : Sélectionnez cette option uniquement si vous souhaitez que l'agent exclut un sous-ensemble des sous-réseaux que vous avez ajoutés à la liste Inclure. Par exemple, si vous incluez 10.0.0.0/8 et que vous excluez 10.2.50.0/22, l'agent mappera les utilisateurs de tous les sous-réseaux de 10.0.0.0/8, sauf 10.2.50.0/22, et exclura tous les sous-réseaux n'appartenant pas à 10.0.0.0/8.

     *Si vous ajoutez des profils Exclude (Exclure) sans ajouter de profils Include (Inclure), l'agent User-ID exclura tous les sous-réseaux et pas uniquement ceux que vous avez ajoutés.*
4. Cliquez sur **OK**.

**STEP 3 |** (Facultatif) Si vous avez configuré l'agent pour se connecter à un serveur Novell eDirectory, vous devez spécifier la manière dont l'agent doit rechercher des informations dans l'annuaire.

1. Sélectionnez **User Identification (Identification utilisateur)** > **Setup (Configuration)**, puis cliquez sur **Edit (Modifier)** dans la section Setup (Configuration) de la fenêtre.
2. Sélectionnez l'onglet **eDirectory (eDirectory)**, puis renseignez les champs suivants :
   - **Search Base (Base de recherche)** : le point de départ ou contexte racine des requêtes de l'agent, par exemple : `dc=domain1,dc=example, dc=com`.
   - **Bind Distinguished Name (Nom unique de liaison)** : le compte à utiliser pour la liaison à l'annuaire, par exemple : `cn=admin,ou=IT, dc=domain1, dc=example, dc=com`.
   - **Bind Password (Mot de passe de liaison)** : le mot de passe du compte de liaison. L'agent enregistre le mot de passe crypté dans le fichier de configuration.
   - **Search Filter (Filtre de recherche)** : la requête de recherche des entrées utilisateur (le paramètre par défaut est `objectClass=Person`).
   - **Server Domain Prefix (Préfixe du domaine de serveur)** : un préfixe permettant d'identifier l'utilisateur de manière unique. Celui-ci est requis uniquement en cas de chevauchement d'espaces de noms, notamment des utilisateurs différents portant le même nom et provenant de deux annuaires différents.
   - **Use SSL (Utiliser SSL)** : cochez cette case pour utiliser SSL pour la liaisoneDirectory.
   - **Verify Server Certificate (Vérifier le certificat du serveur)** : cochez cette case pour vérifier le certificat du serveur eDirectory lorsque vous utilisez SSL.

**STEP 4 |** (Strongly recommended (Fortement recommandé)) Désactiver le sondage client.

*Palo Alto Networks recommande vivement de désactiver le sondage client sur les réseaux à haute sécurité. Le sondage client peut constituer une menace pour la sécurité s'il n'est pas correctement configuré. Pour plus d'informations, reportez-vous à la section* client probing (Sondage client)*.*

1. Sous l'onglet **Client probing (Sondage client)**, décochez la case **Enable WMI Probing (Activer la sonde WMI)** si elle est activée.
2. Décochez la case **Enable NetBIOS Probing (Activer le sondage NetBIOS)** si elle est activée.

   *Palo Alto Network vous recommande vivement de collecter des informations de mappage utilisateur à partir de sources isolées et fiables, telles que des contrôleurs de domaine ou des intégrations avec* Syslog *ou* XML API (API XML)*,afin de capturer en toute sécurité des informations de mappage utilisateur à partir de n'importe quel type de périphérique ou système d'exploitation.*

   *Si vous devez activer le sondage client, activez la case à cocher* ***Enable WMI Probing (Activer le sondage WMI)*** *et sous l'onglet* ***Client probing (Sondage client)****. En raison des risques de sécurité potentiels de cette méthode, activez uniquement la case à cocher* ***Enable NetBIOS Probing (Activer le sondage NetBIOS)*** *si le pare-feu ne peut pas obtenir de mappages utilisateur à l'aide d'une autre méthode. Puis ajoutez une exception d'administration à distance au pare-feu Windows pour chaque client sondé afin de vous assurer que le pare-feu Windows autorisera le sondage client. Le port 139 dans le pare-feu Windows doit être autorisé et les services de partage d'imprimantes et de fichiers doivent être activés sur chaque ordinateur client sondé.*

**STEP 5 |** Enregistrer la configuration.

Cliquez sur **OK (OK)** pour enregistrer les paramètres de configuration de l'agent User-ID, puis sur **Commit (Valider)** pour redémarrer l'agent User-ID et charger les nouveaux paramètres.

**STEP 6 |** (Facultatif) Définissez l'ensemble d'utilisateurs pour lesquels vous n'avez pas à procéder au mappage d'adresse IP/nom d'utilisateur, les comptes de kiosques par exemple.

Enregistrez la liste `ignore-user` en tant que document texte sur l'hôte de l'agent en utilisant le titre de `ignore_user_list` et utilisez l'extension de fichier .txt pour l'enregistrer dans le dossier de l'agent User-ID sur le serveur du domaine où l'agent est installé.

Dressez la liste des comptes d'utilisateurs à ignorer ; le nombre de comptes que vous pouvez ajouter à la liste est illimité. Chaque nom de compte d'utilisateur doit se trouver sur une nouvelle ligne. Par exemple :

```
SPAdmin
SPInstall
```

```
TFSReport
```

Vous pouvez utiliser un astérisque comme caractère générique permettant la correspondance de plusieurs noms d'utilisateur. Il ne peut toutefois être placé qu'à la toute fin de l'entrée. Par exemple, `corpdomain\it-admin*` correspondrait à tous les administrateurs du domaine `corpdomain` dont le nom d'utilisateur commence par la chaîne `it-admin`. Vous pouvez également utiliser la liste `ignore-user (utilisateurs ignorés)` pour identifier les utilisateurs qui devront s'authentifier à l'aide du portail d'authentification.

*Après avoir ajouté des entrées à la liste des utilisateurs ignorés, vous devez arrêter et redémarrer la connexion au service.*

**STEP 7 |** Configurez le pare-feu qui se connectera à l'agent User-ID.

*Le pare-feu ne peut se connecter qu'à un seul agent User-ID Windows qui utilise le service d'informations d'identification User-ID pour détecter l'envoi des informations d'identification d'entreprise. Reportez-vous à la section* Configuration de la détection des informations d'identification à l'aide de l'agent User-ID Windows *pour obtenir de plus amples précisions sur l'utilisation de ce service pour empêcher l'hameçonnage des informations d'identification.*

Suivez les étapes ci-dessous pour chaque pare-feu qui se connectera à l'agent User-ID pour recevoir des mappages d'utilisateur :

1. Sélectionnez **Device (Périphérique)** > **Data Redistribution (Redistribution des données)** > **Agents** et cliquez sur **Add (Ajouter)**.
2. Donnez un **Name (Nom)** à l'agent.
3. **Add an Agent Using (Ajoutez un agent à l'aide)** de l'**Host and Port (Hôte et port)**.
4. Saisissez l'adresse IP du **Host (Hôte)** Windows sur lequel l'agent User-ID est installé.
5. Saisissez le numéro de **Port (Port)** (de 1 à 65535) sur lequel l'agent écoutera les requêtes de mappage d'utilisateur. Cette valeur doit correspondre à la valeur configurée sur l'agent User-ID. Par défaut, le port est défini sur 5007 sur le pare-feu et sur les versions plus récentes de l'agent User-ID. Néanmoins, certaines versions plus anciennes de l'agent User-ID utilisent le port 2010 par défaut.
6. Sélectionnez les **IP User Mappings (Mappage d'utilisateur IP)** comme **Data type (Type de données)**.
7. Assurez-vous que la configuration est **Enabled (Activée)**, puis cliquez sur **OK (OK)**.
8. **Commit (Validez)** les modifications.
9. Vérifiez que le **Connected status (État Connecté)** est affiché (voyant vert).

**STEP 8 |** Vérifiez que l'agent User-ID parvient à mapper les adresses IP aux noms d'utilisateurs et que les pare-feu peuvent se connecter à l'agent.

1. Lancez l'agent User-ID et sélectionnez **User Identification (Identification utilisateur)**.
2. Vérifiez que l'état de l'agent affiché est **Agent is running (L'agent est en cours d'exécution)**. Si l'agent n'est pas en cours d'exécution, cliquez sur **Start (Démarrer)**.
3. Pour vérifier que l'agent User-ID peut se connecter aux serveurs surveillés, assurez-vous que l'état de chaque serveur est **Connected (Connecté)**.
4. Pour vérifier que les pare-feu peuvent se connecter à l'agent User-ID, assurez-vous que l'état de chaque périphérique connecté est **Connected (Connecté)**.
5. Pour vérifier que l'agent User-ID mappe les adresses IP aux noms d'utilisateurs, sélectionnez **Monitoring (Surveillance)** et assurez-vous que la table de mappage est renseignée. Vous pouvez également **Search (Rechercher)** des utilisateurs spécifiques ou **Delete (Supprimer)** des mappages d'utilisateur de la liste.

## Configuration du mappage d'utilisateur à l'aide de l'agent User-ID intégré à PAN-OS

La procédure suivante décrit comment configurer l'agent User-ID intégré à PAN-OS sur le pare-feu pour le mappage d'adresse IP/nom d'utilisateur. L'agent User-ID intégré à PAN-OS effectue les mêmes tâches que l'agent Windows, excepté le sondage du client NetBIOS (le sondage WMI est pris en charge).

**STEP 1 |** Créez un compte de service Active Directory pour que l'agent User-ID puisse accéder aux services et aux hôtes qu'il surveillera pour extraire les informations de mappage d'utilisateur.

Création d'un compte de service dédié pour l'agent User-ID.

**STEP 2 |** Définissez les serveurs que le pare-feu surveillera pour collecter des informations de mappage d'utilisateur.

Parmi les 100 serveurs surveillés par pare-feu, vous pouvez définir un maximum de 50 expéditeurs Syslog pour tout système virtuel unique.

*Pour pouvoir collecter tous les mappages nécessaires, le pare-feu doit se connecter à tous les serveurs auxquels vos utilisateurs se connectent afin qu'il puisse surveiller les fichiers journaux de sécurité de tous les serveurs contenant des événements de connexion.*

1. Sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **User Mapping (Mappage d'utilisateur)**.
2. Cliquez sur **Add (Ajouter)** dans la section Server Monitoring (Surveillance des serveurs).
3. Saisissez un **Name (Nom)** pour identifier le serveur.
4. Sélectionnez le **Type (Type)** de serveur.
   - **Microsoft Active Directory**
   - **Microsoft Exchange**
   - **Novell eDirectory**
   - **Expéditeur Syslog**
5. (Microsoft Active Directory ou Microsoft Exchange uniquement) Sélectionnez le **Transport Protocol (Protocole de transport)** que vous souhaitez utiliser pour surveiller les journaux de sécurité et les informations de session sur le serveur.
   - **WMI** : Le pare-feu et les serveurs surveillés utilisent Windows Management Instrumentation (Instrumentation de gestion Windows ; WMI) pour communiquer.
   - **WinRM-HTTP** : Le pare-feu et les serveurs surveillés utilisent Kerberos pour l'authentification mutuelle, et le serveur surveillé chiffre la communication avec le pare-feu au moyen d'une clé de session Kerberos négociée.
   - **WinRM-HTTPS** : Le pare-feu et les serveurs surveillés utilisent HTTPS pour communiquer et utilisent l'authentification de base ou Kerberos pour l'authentification mutuelle.

   Si vous sélectionnez une option Windows Remote Management (WinRM), vous devez Configuration de la surveillance du serveur à l'aide de WinRM.
6. (Microsoft Active Directory, Microsoft Exchange ou Novell eDirectory uniquement) Saisissez la **Network Address (Adresse réseau)** du serveur.

*Si vous utilisez WinRM avec Kerberos, vous devez saisir un fully qualified domain name (nom de domaine complet ; FDQN). Si vous voulez utiliser WinRM avec l'authentification de base ou **WMI** pour surveiller le serveur, vous pouvez saisir une adresse IP ou un FQDN.*

*Pour surveiller les serveurs au moyen de WMI, spécifiez une adresse IP, le nom du compte de service (si toute la surveillance des serveurs se trouve dans le même domaine) ou un fully qualified domain name (nom de domaine qualifié ; FQDN). Si vous spécifiez un FQDN, utilisez le nom d'ouverture de bas niveau (RAD)\sAMAccountName (DLN)\sAMAccountName plutôt que le format FQDN \sAMAccountName. Par exemple, utilisez **`example\user.services`**, et non pas **`example.com\user.services`**. Si vous spécifiez un FQDN, le pare-feu tentera de s'authentifier à l'aide de Kerberos, qui ne prend pas en charge WMI.*

7. (Expéditeur Syslog uniquement) Si vous sélectionnez **Syslog Sender (Expéditeur Syslog)** en tant que **Type** de serveur, Configuration de l'agent User-ID intégré à PAN-OS en tant qu'écouteur Syslog.
8. (Novell eDirectory uniquement) Assurez-vous que le **Server Profile (Profil de serveur)** que vous sélectionnez est **Enabled (Activé)**, puis cliquez sur **OK**.
9. (Facultatif) Cliquez sur **Discover (Détecter)** si vous voulez que le pare-feu détecte automatiquement les contrôleurs de domaine de votre réseau à l'aide de recherches DNS.

   *La fonction de détection automatique s'applique aux contrôleurs de domaines uniquement ; vous devez ajouter manuellement les serveurs Exchange et eDirectory que vous souhaitez surveiller.*

**STEP 3 |** (Facultatif) Indiquez la fréquence à laquelle le pare-feu interroge les serveurs Windows à la recherche d'informations de mappage. Il s'agit de l'intervalle entre la fin de la dernière requête et le début de la suivante.

*Si le contrôleur de domaine traiter de nombreuses demandes, les délais entre les requêtes peuvent dépasser la valeur spécifiée.*

1. **Edit (Modifiez)** la **Palo Alto Networks User-ID Agent Setup (Configuration de l'agent User-ID Palo Alto Networks)**.
2. Sélectionnez l'onglet **Server Monitor (Surveillance du serveur)** et spécifiez la **Server Log Monitor Frequency (Fréquence de surveillance du journal du serveur)** en secondes (1 secondes par défaut, plage de 3 à 3 600 secondes). Augmentez la valeur de ce champ à

5 secondes dans les environnements contenant d'anciens contrôleurs de domaines ou des liaisons à latence élevée.

*Assurez-vous que l'option **Enable Session (Activer la session)** n'est pas sélectionnée. Cette option nécessite que l'agent User-ID possède un compte Active Directory avec des privilèges d'Opérateur de serveur afin de pouvoir lire toutes les sessions utilisateur. Au lieu de cela, utilisez une intégration Syslog ou API XML pour surveiller les sources qui recueillent les événements de connexion et de déconnexion pour tous les types de périphériques et de systèmes d'exploitation (plutôt qu'uniquement Windows), tels que les contrôleurs sans fil et les Network Access Controllers (contrôleurs d'accès au réseau ; NAC).*

3. Cliquez sur **OK** pour enregistrer vos modifications.

**STEP 4 |** Spécifiez les sous-réseaux que l'agent User-ID intégré à PAN-OS doit inclure ou exclure du mappage d'utilisateur.

Par défaut, User-ID mappe tous les utilisateurs qui accèdent aux serveurs que vous surveillez.

*Il est recommandé de toujours spécifier les réseaux à inclure et , éventuellement, à exclure de User-ID pour garantir que l'agent ne communique qu'avec les ressources internes et pour empêcher le mappage des utilisateurs non autorisés. Vous ne devriez activer le mappage d'utilisateur que sur les sous-réseaux auxquels les utilisateurs internes de votre organisation se connectent.*

1. Sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **User Mapping (Mappage d'utilisateur)**.
2. **Add (Ajoutez)** une entrée à **Include/Exclude Networks (Include/Exclude des réseaux)** et saisissez un **Name (Nom)** pour l'entrée Assurez-vous que l'entrée est **Enabled (Activée)**.
3. Saisissez la **Network Address (Adresse réseau)**, puis indiquez si elle doit être incluse ou exclue :
   - **Include (Inclure)** : sélectionnez cette option si vous souhaitez restreindre le mappage des utilisateurs uniquement aux utilisateurs qui sont connectés au sous-réseau spécifié. Par exemple, si vous incluez 10.0.0.0/8, l'agent mappe les utilisateurs qui sont connectés à ce sous-réseau et exclut les autres. Si vous souhaitez que l'agent mappe les utilisateurs des autres sous-réseaux, vous devez répéter ces étapes pour ajouter d'autres réseaux à la liste.
   - **Exclude (Exclure)** : sélectionnez cette option uniquement si vous souhaitez que l'agent exclut un sous-ensemble des sous-réseaux que vous avez ajoutés à la liste Inclure. Par exemple, si vous incluez 10.0.0.0/8 et que vous excluez 10.2.50.0/22, l'agent mappera les utilisateurs de tous les sous-réseaux de 10.0.0.0/8, sauf 10.2.50.0/22, et exclura tous les sous-réseaux n'appartenant pas à 10.0.0.0/8.

     *Si vous ajoutez des profils Exclude (Exclure) sans ajouter de profils Include (Inclure), l'agent User-ID exclura tous les sous-réseaux et pas uniquement ceux que vous avez ajoutés.*
4. Cliquez sur **OK**.

**STEP 5 |** Définissez les informations d'identification de domaine du compte utilisé par le pare-feu pour accéder aux ressources Windows. Celles-ci sont requises pour la surveillance des serveurs Exchange et des contrôleurs de domaines, ainsi que pour le sondage WMI.

1. **Edit (Modifiez)** la **Palo Alto Networks User-ID Agent Setup (Configuration de l'agent User-ID Palo Alto Networks)**.
2. Sélectionnez l'onglet **Server Monitor Account (Compte de surveillance du serveur)**, puis saisissez le **User Name (Nom d'utilisateur)** et le **Password (Mot de passe)** du compte de service que l'agent User-ID utilisera pour sonder les clients et surveiller les serveurs. Saisissez le nom d'utilisateur au format **`domaine\nom d'utilisateur`**.
3. SI vous utilisez WinRM pour surveiller les serveurs, configurez le pare-feu pour qu'il s'authentifie auprès du serveur que vous surveillez.
   - Si vous souhaitez utiliser WinRM avec l'authentification de base, activez WinRM sur le serveur, configurez l'authentification de base, puis spécifiez le **Domain's DNS Name (Nom DNS du domaine)** du compte de service.
   - Si vous voulez utiliser WinRM avec Kerberos, Configurez un profil de serveur Kerberos si vous ne l'avez pas encore fait, puis sélectionnez le **Kerberos Server Profile (Profil du serveur Kerberos)**.

**STEP 6 |** (Facultatif, non recommandé) Configurez le sondage WMI (l'agent User-ID intégré à PAN-OS ne prend pas en charge le sondage NetBIOs).

*N'activez pas le sondage WMI sur les réseaux haute sécurité. L'interrogation du client peut générer une grande quantité de trafic sur le réseau et peut constituer une menace pour la sécurité lorsqu'il est mal configuré.*

1. À l'onglet **Client Probing (Sondage du client)**, **Enable Probing (Activez le sondage)**.
2. (Facultatif) Spécifiez le **Probe Interval (Intervalle de sondage)** pour définir l'intervalle (en minutes) entre la fin de la dernière requête de sondage et le début de la suivante.

   Au besoin, augmentez la valeur pour vous assurer que l'agent User-ID dispose de suffisamment de temps pour sonder toutes les adresses IP apprises (20 par défaut, plage de 1 à 1 440).

   *Si la charge de la requête est élevée, le retard observé entre les requêtes pourrait considérablement dépasser l'intervalle indiqué.*
3. Cliquez sur **OK**.
4. Vérifiez que le pare-feu Windows autorise le sondage du client en ajoutant une exception d'administration à distance au pare-feu Windows pour chaque client sondé.

**STEP 7 |** (Facultatif) Définissez l'ensemble de comptes utilisateur qui n'ont pas à faire l'objet de mappages d'adresse IP/nom d'utilisateur, comme les comptes de kiosques par exemple.

> ***Définissez la liste des utilisateurs ignorés sur le pare-feu faisant office d'agent User-ID, et non pas sur le client. Si vous définissez la liste des utilisateurs ignorés sur le pare-feu client, les utilisateurs qui figurent dans la liste font toujours l'objet d'un mappage lors de la redistribution.***

Sélectionnez l'onglet **Ignore User List (Liste des utilisateurs ignorés)** et **Add (Ajoutez)** chaque nom d'utilisateur à exclure du mappage d'utilisateur. Vous pouvez également utiliser la liste des utilisateurs ignorés pour identifier les utilisateurs qui devront s'authentifier à l'aide du portail d'authentification. Vous pouvez utiliser un astérisque comme caractère générique permettant la correspondance de plusieurs noms d'utilisateur. Il ne peut toutefois être placé qu'à la toute fin de l'entrée. Par exemple, `corpdomain\it-admin*` correspondrait à tous les administrateurs du domaine `corpdomain` dont le nom d'utilisateur commence par la chaîne `it-admin`. Vous pouvez ajouter un maximum de 5 000 entrées à exclure du mappage d'utilisateur.

**STEP 8 |** Activez vos modifications de configuration.

Cliquez sur **OK**, puis sur **Commit (Valider)**.

**STEP 9 |** Vérifiez la configuration.

1. Accédez à la CLI du pare-feu.
2. Saisissez la commande opérationnelle suivante :

```
> show user server-monitor state all
```

3. Dans l'onglet **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **User Mapping (Mappage d'utilisateur)** de l'interface Web, vérifiez que l'état de chaque serveur configuré pour la surveillance est `Connected (Connecté)`.

## Configuration de la surveillance du serveur à l'aide de WinRM

Vous pouvez configurer l'agent User-ID intégré à PAN-OS pour qu'il surveille les serveurs à l'aide de Windows Remote Management (Gestion à distance Windows ; WinRM). L'utilisation du protocole WinRM améliore la vitesse, l'efficacité et la sécurité lors de la surveillance des événements serveurs pour mapper les événements utilisateur aux adresses IP. L'agent User-ID intégré à PAN-OS prend en charge le protocole WinRM sur Windows Server 2012 Active Directory ou Microsoft Exchange Server 2012 ou toute version ultérieure des deux.

On peut configurer la surveillance du serveur à l'aide de WinRM de trois façons :

- Configuration de WinRM sur HTTPS à l'aide de l'authentification de base—Le pare-feu s'authentifie auprès du serveur surveillé à l'aide du nom d'utilisateur et du mot de passe du compte de service de l'agent d'User-ID, et le pare-feu authentifie le serveur surveillé à l'aide du profil de certificat User-ID.
- Configuration de WinRM sur HTTP à l'aide de Kerberos—Le pare-feu et les serveurs surveillés utilisent Kerberos pour l'authentification mutuelle, et le serveur surveillé chiffre la communication avec le pare-feu au moyen d'une clé de session Kerberos négociée.

- Configuration de WinRM sur HTTPS à l'aide de Kerberos—Le pare-feu et le serveur surveillé utilisent HTTPS pour communiquer et utilisent Kerberos pour l'authentification mutuelle.

## Configuration de WinRM sur HTTPS à l'aide de l'authentification de base

Lorsque vous configurez WinRM pour utiliser le protocole HTTPS avec l'authentification de base, le pare-feu transmet les informations d'identification du compte de service dans un tunnel sécurisé au moyen de SSL.

**STEP 1 |** Configurez le compte de service avec l'utilisateur de gestion à distance et les privilèges CIMV2 du serveur que vous souhaitez surveiller.

**STEP 2 |** Sur le serveur Windows que vous surveillez, obtenez l'empreinte de certificat que le serveur Windows utilisera avec WinRM et activez WinRM.

*Le compte que vous utilisez pour configurer WinRM sur le serveur que vous souhaitez surveiller doit disposer de privilèges d'administrateur.*

1. Vérifiez que le certificat est installé dans le magasin de certificats de l'ordinateur local (**Certificates (Local Computer) [Certificats (Ordinateur local)]** > **Personal (Personnel)** > **Certificates (Certificats)**).

   Si vous ne voyez pas le magasin de certificats de l'ordinateur local, lancez la console de gestion de Microsoft (**Start (Démarrer)** > **Run (Exécuter)** > **MMC**) et ajoutez l'instantané des certificats (**File (Fichier)** > **Add/Remove Snap-in (Ajouter/Retirer l'instantané)** > **Certificates (Certificats)** > **Add (Ajouter)** > **Computer account (Compte de l'ordinateur)** > **Next (Suivant)** > **Finish (Finir)**).
2. Ouvrez le certificat et sélectionnez **General (Général)** > **Details (Détails)** > **Show: <All> (Montrer : <Tout>)**.
3. Sélectionnez la **Thumbprint (Empreinte de pouce)** et copiez-la.
4. Pour activer la connexion du pare-feu au serveur Windows à l'aide de WinRM, saisissez la commande suivante : **`winrm quickconfig`**.
5. Saisissez ensuite **`y`** pour confirmer les changements et confirmer que le résultat affiche `WinRM service started`.

   Si WinRM est activé, le résultat `WinRM service is already running on this machine.` s'affiche. Vous serez invité à confirmer les changements de configuration requis supplémentaires.
6. Pour vérifier que WinRM communique à l'aide de HTTPS, saisissez la commande suivante : **`winrm enumerate winrm/config/listener`** et confirmez que le résultat affiche `Transport = HTTPS`.

   WinRM/HTTPS utilise le port 5986 par défaut.
7. À partir de l'invite de commande du serveur Windows, saisissez la commande suivante : **`winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="<nom d'hôte>";CertificateThumbprint="empreinte de`**

***pouce du certificat"}***, où *nom d'hôte* est le nom d'hôte du serveur Windows et *empreinte de pouce du certificat* est la valeur que vous avez copiée du certificat.

*Utilisez l'invite de commande (pas Powershell) et supprimez les espaces dans l'empreinte du certificat pour que WinRM puisse valider le certificat.*

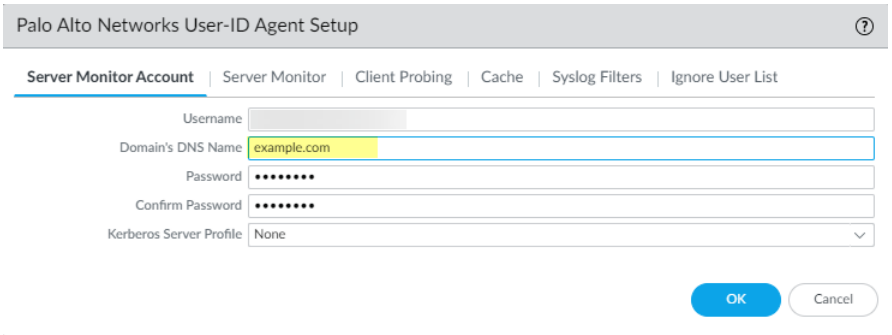
8. À partir de l'invite de commande du serveur Windows, saisissez la commande suivante :

```
c:\> winrm set winrm/config/client/auth @{Basic="true"}
```

9. Saisissez la commande suivante : **`winrm get winrm/config/service/Auth`** et confirmez que `Basic = true`.

**STEP 3 |** Activez l'authentification de base entre l'agent User-ID intégré à PAN-OS et les serveurs faisant l'objet de la surveillance.

1. Sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **User Mapping (Mappage d'utilisateur)** > **Palo Alto Networks User-ID Agent Setup(Configuration de l'agent User-ID Palo Alto Networks)** > **Server Monitor Account (Compte de surveillance du serveur)**.
2. Au format **`domain\username`**, saisissez le **User Name (Nom d'utilisateur)** du compte de service que l'agent User-ID utilisera pour surveiller les serveurs.
3. Saisissez le **Domain's DNS Name (Nom DNS du domaine)** du compte de surveillance du serveur.

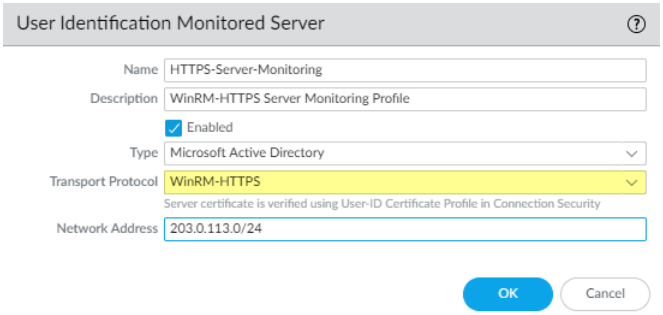



4. Saisissez le **Password (Mot de passe)** et le **Confirm Password (Mot de passe de confirmation)** pour le compte de service.
5. Cliquez sur **OK**.

**STEP 4 |** Configurez la surveillance du serveur pour l'agent User-ID intégré à PAN-OS.

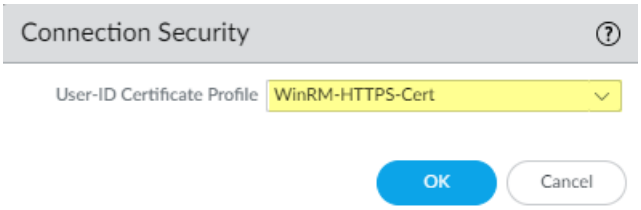
1. Sélectionnez le **Type** de serveur Microsoft (**Microsoft Active Directory** ou **Microsoft Exchange**).
2. Sélectionnez **Win-RM-HTTPS** en tant que **Transport Protocol (Protocole de transport)** pour utiliser Windows Remote Management (WinRM) sur HTTPS pour surveiller les journaux de sécurité du serveur et les informations de session.




3. Saisissez l'adresse IP ou la **Network Address (Adresse réseau)** du FQDN du serveur.

**STEP 5 |** Pour permettre à l'agent User-ID intégré à PAN-OS de communiquer avec les serveurs surveillés à l'aide de WinRM-HTTPS, vérifiez que vous avez importé avec succès le certificat racine pour le service de certificats que le serveur Windows utilise pour WinRM sur le pare-feu et associez-le à un profil de certificat de User-ID.

1. Sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Connection Security (Sécurité de la connexion)**.
2. Cliquez sur **Edit (Modifier)**.
3. Sélectionnez le certificat du serveur Windows pour le **User-ID Certificate Profile (Profil de certificat de User-ID)**.




4. Cliquez sur **OK**.

**STEP 6 |** **Commit (Validez)** vos modifications.

**STEP 7 |** Vérifiez que l'état de chaque serveur surveillé est Connecté (**Device (Périphérique)** > **User Identification (Identification utilisateur)** > **User Mapping (Mappage d'utilisateur)**).

## Configuration de WinRM sur HTTP à l'aide de Kerberos

Lorsque vous configurez WinRM sur HTTP à l'aide de Kerberos, le pare-feu et les serveurs surveillés utilisent Kerberos pour l'authentification mutuelle, et le serveur surveillé chiffre la communication avec le pare-feu au moyen d'une clé de session Kerberos négociée.

*WinRM avec Kerberos prend en charge les suites de chiffrement aes128-cts-hmac-sha1-96 et aes256-cts-hmac-sha1-96. Si le serveur que vous souhaitez surveiller utilise RC4, vous devez télécharger la mise à jour Windows et désactivez RC4 pour Kerberos dans les paramètres du registre du serveur que vous souhaitez surveiller.*

**STEP 1 |** Configurez le compte de service avec l'utilisateur de gestion à distance et les privilèges CIMV2 du serveur que vous souhaitez surveiller.

**STEP 2 |** Confirmez que WinRM est activé sur le serveur Windows que vous surveillez.

*Le compte que vous utilisez pour configurer WinRM sur le serveur que vous souhaitez surveiller doit disposer de privilèges d'administrateur.*

1. Pour activer la connexion du pare-feu au serveur Windows à l'aide de WinRM, saisissez la commande suivante : **`winrm quickconfig`**.
2. Saisissez ensuite **`y`** pour confirmer les changements et confirmer que le résultat affiche `WinRM service started`.

   Si WinRM est activé, le résultat `WinRM service is already running on this machine.` s'affiche. Vous serez invité à confirmer les changements de configuration requis supplémentaires.
3. Pour vérifier que WinRM communique à l'aide de HTTPS, saisissez la commande suivante : **`winrm enumerate winrm/config/listener`** et confirmez que le résultat affiche `Transport = HTTPS`.

   WinRM/HTTP utilise le port 5985 par défaut.
4. Saisissez la commande suivante : **`winrm get winrm/config/service/Auth`** et confirmez que `Kerberos = true`.

**STEP 3 |** Activez l'authentification à l'aide de Kerberos sur l'agent User-ID intégré à PAN-OS et les serveurs surveillés.

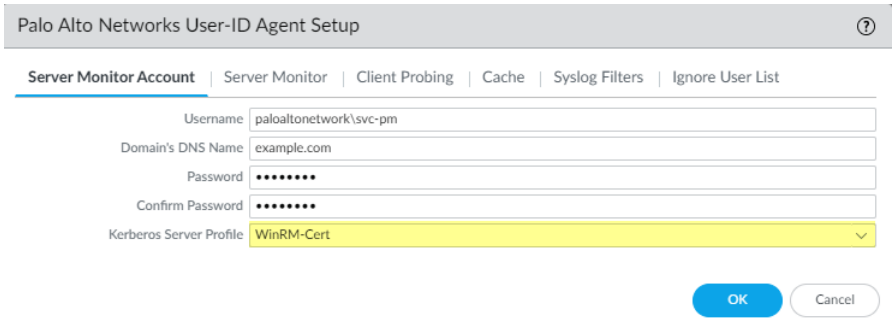
1. Si vous ne l'avez pas fait lors de la configuration initiale, configurez les paramètres de date et d'heure (NTP) pour assurer le succès de la négociation Kerberos.
2. Configurez un profil de serveur Kerberos sur le pare-feu pour qu'il s'authentifie auprès du serveur à surveiller pour surveiller les journaux de sécurité et les informations de session.
3. Sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **User Mapping (Mappage d'utilisateur)** > **Palo Alto Networks User-ID Agent**

**Setup(Configuration de l'agent User-ID Palo Alto Networks)** > **Server Monitor Account (Compte de surveillance du serveur)**.

4. Au format **`domain\username`**, saisissez le **User Name (Nom d'utilisateur)** du compte de service que l'agent User-ID utilisera pour surveiller les serveurs.
5. Saisissez le **Domain's DNS Name (Nom DNS du domaine)** du compte de surveillance du serveur.

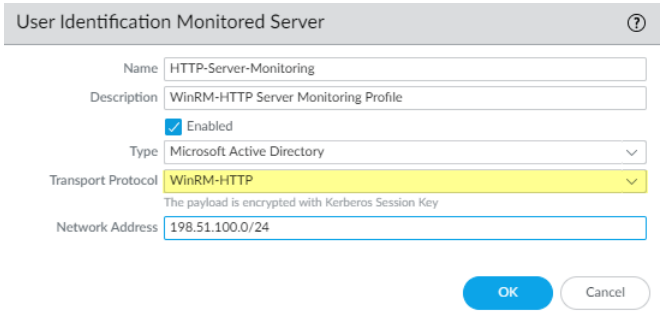
   Kerberos utilise le nom de domaine pour localiser le compte de service.
6. Saisissez le **Password (Mot de passe)** et le **Confirm Password (Mot de passe de confirmation)** pour le compte de service.
7. Sélectionnez le **Kerberos Server Profile (Profil de serveur Kerberos)** que vous avez configuré à l'étape 3.2.




8. Cliquez sur **OK**.

**STEP 4 |** Configurez la surveillance du serveur pour l'agent User-ID intégré à PAN-OS.

1. Configurez le Type de serveur Microsoft (**Microsoft Active Directory** ou **Microsoft Exchange**).
2. Sélectionnez **WinRM-HTTP** en tant que **Transport Protocol (Protocole de transport)** pour utiliser Windows Remote Management (WinRM) sur HTTP pour surveiller les journaux de sécurité du serveur et les informations de session.




3. Saisissez la **Network Address (Adresse réseau)** du FQDN du serveur.

   Si vous utilisez Kerberos, l'adresse réseau doit être un fully qualified domain name (nom de domaine complet ; FDQN).

**STEP 5 |** **Commit (Validez)** vos modifications.

**STEP 6 |** Vérifiez que l'état de chaque serveur surveillé est Connecté (**Device (Périphérique)** > **User Identification (Identification utilisateur)** > **User Mapping (Mappage d'utilisateur)**).

## Configuration de WinRM sur HTTPS à l'aide de Kerberos

Lorsque vous configurez WinRM sur HTTPS à l'aide de Kerberos, le pare-feu et le serveur surveillé utilisent HTTPS pour communiquer et utilisent Kerberos pour l'authentification mutuelle.

*WinRM avec Kerberos prend en charge les suites de chiffrement aes128-cts-hmac-sha1-96 et aes256-cts-hmac-sha1-96. Si le serveur que vous souhaitez surveiller utilise RC4, vous devez télécharger la mise à jour Windows et désactivez RC4 pour Kerberos dans les paramètres du registre du serveur que vous souhaitez surveiller.*

**STEP 1 |** Configurez le compte de service avec l'utilisateur de gestion à distance et les privilèges CIMV2 du serveur que vous souhaitez surveiller.

**STEP 2 |** Sur le serveur Windows que vous surveillez, obtenez l'empreinte de certificat que le serveur Windows utilisera avec WinRM et activez WinRM.

*Le compte que vous utilisez pour configurer WinRM sur le serveur que vous souhaitez surveiller doit disposer de privilèges d'administrateur.*

1. Vérifiez que le certificat est installé dans le magasin de certificats de l'ordinateur local (**Certificates (Local Computer) [Certificats (Ordinateur local)]** > **Personal (Personnel)** > **Certificates (Certificats)**).

   Si vous ne voyez pas le magasin de certificats de l'ordinateur local, lancez la console de gestion de Microsoft (**Start (Démarrer)** > **Run (Exécuter)** > **MMC**) et ajoutez l'instantané des certificats (**File (Fichier)** > **Add/Remove Snap-in (Ajouter/Retirer l'instantané)** > **Certificates (Certificats)** > **Add (Ajouter)** > **Computer account (Compte de l'ordinateur)** > **Next (Suivant)** > **Finish (Finir)**).
2. Ouvrez le certificat et sélectionnez **General (Général)** > **Details (Détails)** > **Show: <All> (Montrer : <Tout>)**.
3. Sélectionnez la **Thumbprint (Empreinte de pouce)** et copiez-la.
4. Pour activer la connexion du pare-feu au serveur Windows à l'aide de WinRM, saisissez la commande suivante : **`winrm quickconfig`**.
5. Saisissez ensuite **`y`** pour confirmer les changements et confirmer que le résultat affiche `WinRM service started`.

   Si WinRM est activé, le résultat `WinRM service is already running on this machine.` s'affiche. Vous serez invité à confirmer les changements de configuration requis supplémentaires.
6. Pour vérifier que WinRM communique à l'aide de HTTPS, saisissez la commande suivante : **`winrm enumerate winrm/config/listener`**. Confirmez ensuite que le résultat affiche `Transport = HTTPS`.

   WinRM/HTTPS utilise le port 5986 par défaut.
7. À partir de l'invite de commande du serveur Windows, saisissez la commande suivante : **`winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="<nom d'hôte>";CertificateThumbprint="empreinte de`**

***pouce du certificat"}***, où *nom d'hôte* est le nom d'hôte du serveur Windows et *empreinte de pouce du certificat* est la valeur que vous avez copiée du certificat.

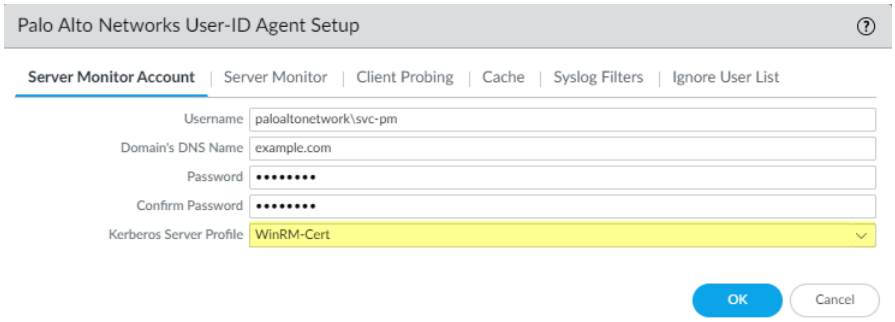
*Utilisez l'invite de commande (pas Powershell) et supprimez les espaces dans l'empreinte du certificat pour que WinRM puisse valider le certificat.*

8. Saisissez la commande suivante : **`winrm get winrm/config/service/Auth`** et confirmez que `Basic = false` et `Kerberos= true`.

**STEP 3 |** Activez l'authentification à l'aide de Kerberos sur l'agent User-ID intégré à PAN-OS et les serveurs surveillés.

1. Si vous ne l'avez pas fait lors de la configuration initiale, configurez les paramètres de date et d'heure (NTP) pour assurer le succès de la négociation Kerberos.
2. Configurez un profil de serveur Kerberos sur le pare-feu pour qu'il s'authentifie auprès du serveur à surveiller pour surveiller les journaux de sécurité et les informations de session.
3. Sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **User Mapping (Mappage d'utilisateur)** > **Palo Alto Networks User-ID Agent Setup(Configuration de l'agent User-ID Palo Alto Networks)** > **Server Monitor Account (Compte de surveillance du serveur)**.
4. Au format **`domain\username`**, saisissez le **User Name (Nom d'utilisateur)** du compte de service que l'agent User-ID utilisera pour surveiller les serveurs.
5. Saisissez le **Domain's DNS Name (Nom DNS du domaine)** du compte de surveillance du serveur.

   Kerberos utilise le nom de domaine pour localiser le compte de service.
6. Saisissez le **Password (Mot de passe)** et le **Confirm Password (Mot de passe de confirmation)** pour le compte de service.
7. Sélectionnez le **Kerberos Server Profile (Profil de serveur Kerberos)** que vous avez créé à l'étape 3.2.

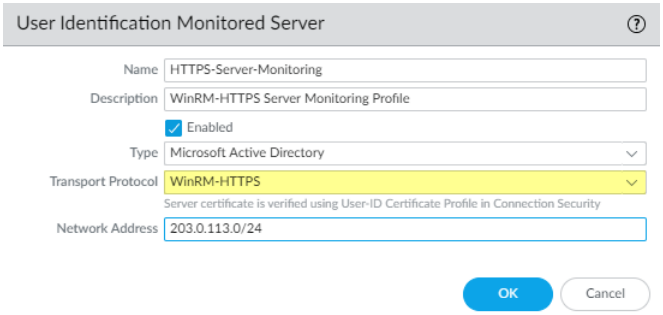



8. Cliquez sur **OK**.

**STEP 4 |** Configurez la surveillance du serveur pour l'agent User-ID intégré à PAN-OS.

1. Configurez le Type de serveur Microsoft (**Microsoft Active Directory** ou **Microsoft Exchange**).
2. Sélectionnez **Win-RM-HTTPS** en tant que **Transport Protocol (Protocole de transport)** pour utiliser Windows Remote Management (WinRM) sur HTTPS pour surveiller les journaux de sécurité du serveur et les informations de session.



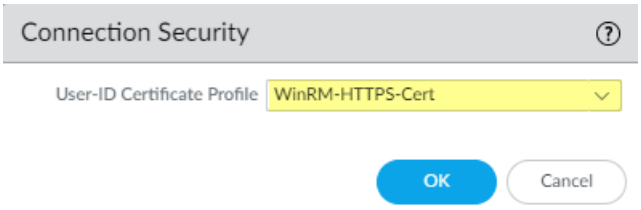

3. Saisissez la **Network Address (Adresse réseau)** du FQDN du serveur.

   Si vous utilisez Kerberos, l'adresse réseau doit être un fully qualified domain name (nom de domaine complet ; FDQN).

**STEP 5 |** Pour permettre à l'agent User-ID intégré à PAN-OS de communiquer avec les serveurs surveillés à l'aide de WinRM-HTTPS, vérifiez que vous avez importé avec succès le certificat racine pour le service de certificats que le serveur Windows utilise pour WinRM sur le pare-feu et associez-le à un profil de certificat de User-ID.

Le pare-feu utilise le même certificat pour s'authentifier auprès de tous les serveurs surveillés.

1. Sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Connection Security (Sécurité de la connexion)**.
2. Cliquez sur **Edit (Modifier)**.
3. Sélectionnez le certificat du serveur Windows pour le **User-ID Certificate Profile (Profil de certificat de User-ID)**.




4. Cliquez sur **OK**.
5. **Commit (Validez)** vos modifications.

**STEP 6 |** Vérifiez que l'état de chaque serveur surveillé est Connecté (**Device (Périphérique)** > **User Identification (Identification utilisateur)** > **User Mapping (Mappage d'utilisateur)**).

# Configuration de User-ID pour la surveillance des expéditeurs Syslog lors du mappage d'utilisateur

Pour obtenir les mappages adresse IP/nom d'utilisateur des services réseau qui authentifient actuellement les utilisateurs, vous pouvez configurer l'agent User-ID intégré à PAN-OS ou l'agent User-ID Windows pour analyser les messages Syslog provenant de ces services. Pour vous assurer que les mappages sont à jour, vous pouvez également configurer l'agent User-ID pour qu'il analyse les messages Syslog des événements de déconnexion afin que le pare-feu supprime automatiquement les mappages obsolètes.

- Configuration de l'agent User-ID intégré à PAN-OS en tant qu'écouteur Syslog
- Configuration de l'agent User-ID Windows en tant qu'écouteur Syslog

## Configuration de l'agent User-ID intégré à PAN-OS en tant qu'écouteur Syslog

Pour configurer l'agent User-ID intégré à PAN-OS pour créer de nouveaux mappages d'utilisateurs et pour supprimer les mappages obsolètes via la surveillance Syslog, vous devez commencer par définir les profils d'analyse Syslog. L'agent User-ID utilise les profils pour trouver des événements de connexion et de déconnexion dans les messages Syslog. Dans les environnements où les ***expéditeurs Syslog*** (les services réseau qui authentifient les utilisateurs) transmettent des messages Syslog dans des formats divers, configurez un profil pour chaque format de message Syslog. Les messages Syslog doivent respecter certains critères pour qu'un agent User-ID les analyse (reportez-vous à la section Syslog). La présente procédure utilise des exemples présentant les formats suivants :

- **Événements de connexion** : `[Tue Jul 5 13:15:04 2016 CDT] Administratorauthentication success User:johndoe1 Source:192.168.3.212`
- **Événements de déconnexion** : `[Tue Jul 5 13:18:05 2016CDT] User logout successful User:johndoe1 Source:192.168.3.212`

Une fois les profils d'analyse Syslog configurés, vous devez spécifier les expéditeurs Syslog que l'agent User-ID doit surveiller.

**STEP 1 |** Déterminez si un profil d'analyse Syslog prédéfini existe pour vos expéditeurs Syslog.

Palo Alto Networks fournit plusieurs profils prédéfinis par l'intermédiaire des mises à jour de contenu des applications. Les profils prédéfinis s'appliquent au pare-feu, tandis que les profils personnalisés sont spécifiques à un seul système virtuel.

*Tout nouveau profil d'analyse Syslog dans une version de contenu donnée est documenté dans la note de version correspondante avec la Regex spécifique utilisée pour définir le filtre.*

1. Installez les dernières mises à jour des applications et des menaces ou des applications.
   1. Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)** et cliquez sur **Check Now (Vérifier maintenant)**.
   2. **Download (Téléchargez)** et **Install (Installez)** les nouvelles mises à jour.
2. Déterminez quels profils d'analyse Syslog sont disponibles :
   1. Sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **User Mapping (Mappage d'utilisateurs)** et cliquez sur **Add (Ajouter)** dans la section Server Monitoring (Surveillance du serveur).
   2. Définissez le **Type (Type)** sur **Syslog Sender (Expéditeur Syslog)** et cliquez sur **Add (Ajouter)** dans la section Filter (Filtre). Si le profil d'analyse Syslog dont vous avez besoin est disponible, sautez les étapes associées à la définition des profils personnalisés.

**STEP 2 |** Définissez les profils d'analyse Syslog pour créer et supprimer des mappages d'utilisateurs.

Chaque profil filtre les messages Syslog pour identifier les événements de connexion (pour créer des mappages d'utilisateurs) ou les événements de déconnexion (pour supprimer les mappages) ; aucun profil ne peut faire les deux.

1. Passez en revue les messages Syslog que l'expéditeur Syslog génère pour identifier la syntaxe des événements de connexion et de déconnexion. Vous pourrez ainsi définir les modèles de correspondance lors de la création des profils d'analyse Syslog.

   *Lors de votre examen des messages Syslog, déterminez également s'ils incluent le nom de domaine. Si ce n'est pas le cas, et que vos mappages d'utilisateurs exigent les noms de domaine, saisissez le **Default Domain Name (Nom de domaine par défaut)** lorsque vous définissiez les expéditeurs Syslog que l'agent User-ID surveille (plus loin au cours de cette procédure).*
2. Sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **User Mapping (Mappage d'utilisateur)** et modifiez la section Palo Alto Networks User-ID Agent Setup Agent Setup (Configuration de l'agent User-ID Palo Alto Networks).
3. Sélectionnez **Syslog Filters (Filtres Syslog)**, puis cliquez sur **Add (Ajouter)** pour ajouter un nouveau profil d'analyse syntaxique Syslog.
4. Donnez un nom pour identifier le **Syslog Parse Profile (Profil d'analyse Syslog)**.
5. Sélectionnez le **Type (Type)** d'analyse à effectuer pour trouver des événements de connexion ou de déconnexion dans les messages Syslog :
   - **Regex Identifier (Identificateur de Regex)** : expressions régulières.
   - **Field Identifier (Identificateur de champ)** : chaînes de texte.

   Les étapes suivantes décrivent la configuration de ces types d'analyse.

**STEP 3 |** (**Analyse de l'identificateur Regex uniquement**) Définissez les modèles de correspondance de Regex.

*Si le message Syslog contient un espace autonome ou une tabulation comme délimiteur, utilisez un caractère* ***\ s*** *pour un espace et un caractère* ***\ t*** *pour une tabulation.*

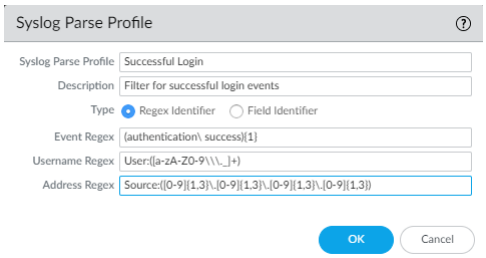
1. Saisissez la **Event Regex (Regex d'événement)** applicable au type d'événements que vous souhaitez trouver :
   - **Événements de connexion** : pour le message d'exemple, l'expression régulière **`(authentication\ success){1}`** extrait la première **`\{1\`** instance de la chaîne `authenticationsuccess`.
   - **Événements de déconnexion** : pour le message d'exemple, l'expression régulière **`(logout\ successful){1}`** extrait la première **`{1}`** instance de la chaîne `logoutsuccessful`.

   La barre oblique inversée (\) avant l'espace est un caractère d'échappement Regex standard qui indique au moteur Regex de ne pas traiter l'espace comme caractère spécial.
2. Saisissez la **Username Regex (Regex de nom utilisateur)** pour identifier le début du nom d'utilisateur.

   Dans le message d'exemple, la Regex **`User:([a-zA-Z0-9\\\._]+)`** correspond à la chaîne `User:johndoe1` et identifie `johndoe1` comme nom d'utilisateur.
3. Renseignez la **Address Regex (Regex d'adresse)** qui permet d'identifier la partie de l'adresse IP dans les messages Syslog.

   Dans le message d'exemple, l'expression régulière **`Source:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})`** correspond à l'adresse IPv4 `Source:192.168.3.212`.

   Voici un exemple d'un profil d'analyse Syslog qui se sert de regex pour identifier des événements de connexion :




4. Cliquez deux fois sur **OK (OK)** pour enregistrer le profil.

**STEP 4 |** (**Analyse de l'identificateur de champ uniquement**) Définissez les modèles de correspondance de chaîne.

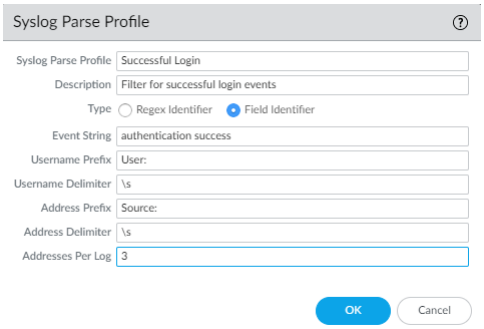
1. Saisissez une **Event String (Chaîne d'événement)** pour identifier le type d'événements que vous souhaitez trouver.
   - **Événements de connexion** : pour le message d'exemple, la chaîne `authentication success` identifie les événements de connexion.
   - **Événements de déconnexion** : pour le message d'exemple, la chaîne `logoutsuccessful` identifie les événements de déconnexion.
2. Saisissez un **Username Prefix (Préfixe de nom utilisateur)** pour identifier le début du champ Nom d'utilisateur dans les messages Syslog. Le champ ne prend pas en charge les expressions régulières telles que \s (pour un espace) ou \t (pour un onglet).

   Dans le message d'exemple, `User :` identifie le début du champ de nom d'utilisateur.
3. Saisissez le **Username Delimiter (Délimiteur de nom d'utilisateur)** qui indique la fin du champ Nom d'utilisateur dans les messages Syslog. Utilisez **`\s`** pour indiquer un espace autonome (comme dans le message d'exemple) et **`\t`** pour indiquer un onglet.
4. Saisissez un **Address Prefix (Préfixe d'adresse)** pour identifier le début du champ Adresse IP dans les messages Syslog. Le champ ne prend pas en charge les expressions régulières telles que \s (pour un espace) ou \t (pour un onglet).

   Dans le message d'exemple, `Source :` identifie le début du champ Adresse.
5. Saisissez le **Address Delimiter (Délimiteur d'adresse)** qui indique la fin du champ Adresse IP dans les messages Syslog.

   Par exemple, saisissez **`\n`** pour indiquer que le délimiteur est un saut de ligne.

   Voici un exemple d'un profil d'analyse Syslog qui se sert de la correspondance de chaîne pour identifier des événements de connexion :




6. Cliquez deux fois sur **OK (OK)** pour enregistrer le profil.

**STEP 5 |** Précisez les expéditeurs Syslog que le pare-feu surveille.

Parmi les 100 serveurs surveillés par pare-feu, vous pouvez définir un maximum de 50 expéditeurs Syslog pour tout système virtuel unique.

Le pare-feu ignore tout message Syslog reçu d'expéditeurs qui ne sont pas dans la liste.

1. Sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **User Mapping (Mappage d'utilisateurs)** et **Add (Ajoutez)** une entrée dans la liste Server Monitoring (Surveillance du serveur).
2. Saisissez un **Name (Nom)** pour identifier l'expéditeur.
3. Assurez-vous que le profil de l'expéditeur est **Enabled (Activé)** (par défaut).
4. Définissez le **Type (Type)** sur **Syslog Sender (Expéditeur Syslog)**.
5. Saisissez la **Network Address (Adresse réseau)** de l'expéditeur Syslog (adresse IP ou FQDN).
6. Sélectionnez **SSL (SSL)** (par défaut) ou **UDP (UDP)** en tant que **Connection Type (Type de connexion)**.

   *Pour sélectionner le certificat TLS que le pare-feu utilise pour recevoir les messages syslog, sélectionnez **Device (Périphérique) > User Identification (Identification utilisateur) > User Mapping (Mappage d'utilisateur) > Palo Alto Networks User-ID Agent Setup (Configuration de l'agent User-ID Palo Alto Networks). Edit (Modifiez)** les paramètres et sélectionnez **Server Monitor (Moniteur de serveur)**, puis sélectionnez le **Syslog Service Profile (Profil de service syslog)** qui contient le certificat TLS que vous souhaitez que le pare-feu utilise pour recevoir les messages syslog.*

   *L'agent User-ID intégré à PAN-OS accepte les messages Syslog uniquement via SSL et UDP. Toutefois, vous devez être vigilant lorsque vous utilisez UDP pour recevoir des messages Syslog, car il s'agit d'un protocole non fiable et il est impossible de vérifier qu'un message provient d'un expéditeur Syslog de confiance. Bien que vous puissiez limiter les messages Syslog à des adresses IP source spécifiques, un pirate peut toujours usurper l'adresse IP, permettant ainsi l'éventuelle injection de messages Syslog non autorisés dans le pare-feu.*

   *Utilisez toujours SSL pour écouter les messages Syslog, car le trafic est chiffré (UDP envoie le trafic en texte clair). Si vous devez utiliser UDP, assurez-vous que l'expéditeur Syslog et le client se trouvent tous les deux sur un réseau sécurisé dédié pour empêcher les hôtes non de confiance d'envoyer du trafic UDP au pare-feu.*

   Le Status (État) affiché d'un expéditeur Syslog qui utilise SSL pour se connecter sera Connected (Connecté) uniquement lorsqu'une connexion SSL est active. Les expéditeurs Syslog utilisant UDP n'affichera aucune valeur d'état
7. Pour chaque format Syslog pris en charge par l'expéditeur, **Add (Ajoutez)** un profil d'analyse Syslog à la liste Filter (Filtre). Sélectionnez le **Event Type (Type d'événement)** que, selon

sa configuration, chaque profil doit identifier : **login (connexion)** (par défaut) ou **logout (déconnexion)**.

8. (Facultatif) Si les messages Syslog ne contiennent aucune information de domaine et que vos mappages d'utilisateurs exigent des noms de domaine, saisissez un **Default Domain Name (Nom de domaine par défaut)** à ajouter aux mappages.
9. Cliquez sur **OK** pour enregistrer les paramètres.

**STEP 6 |** Activez les services d'écoute Syslog sur l'interface que le pare-feu utilise pour recueillir des mappages d'utilisateur.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **Interface Mgmt (Gestion de l'interface)**, puis modifiez un profil de gestion d'interface existant ou cliquez sur **Add (Ajouter)** pour ajouter un nouveau profil.
2. Sélectionnez **User-ID Syslog Listener-SSL (Écouteur SSL Syslog User-ID)** ou **User-ID Syslog Listener-UDP (Écouteur UDP Syslog User-ID)**, ou les deux, selon les protocoles que vous avez définis pour vos expéditeurs Syslog dans la liste Server Monitoring (Surveillance du serveur).

   *Les ports d'écoute (514 pour UDP et 6514 pour SSL) ne sont pas configurables ; ils sont activés par l'intermédiaire du service de gestion uniquement.*
3. Cliquez sur **OK (OK)** pour enregistrer le profil de gestion d'interface.

   *Même après l'activation du service Écouteur Syslog User-ID sur l'interface, celle-ci accepte des connexions Syslog uniquement des expéditeurs qui disposent d'une entrée correspondante dans la configuration des serveurs surveillés User-ID. Le pare-feu ignore les connexions ou les messages reçus d'expéditeurs qui ne figurent pas dans la liste.*
4. Affectez le profil de gestion d'interface que le pare-feu utilise pour recueillir des mappages d'utilisateur :
   1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** et modifiez l'interface.
   2. Sélectionnez **Advanced (Avancé)** > **Other info (Autres informations)**, sélectionnez le **Management Profile (Profil de gestion)** d'interface que vous venez d'ajouter, puis cliquez sur **OK (OK)**.
5. **Commit (Validez)** vos modifications.

**STEP 7 |** Vérifiez que le pare-feu ajoute et supprime les mappages d'utilisateur lorsque les utilisateurs se connectent et se déconnectent.

*Vous pouvez utiliser les commandes de la CLI pour voir des renseignements supplémentaires sur les expéditeurs Syslog, sur les messages Syslogs et sur les mappages d'utilisateur.*

1. Connectez-vous à un autre système client pour lequel un expéditeur Syslog faisant l'objet d'une surveillance génère des messages d'événements de connexion et de déconnexion.
2. Connectez-vous à l'ILC du pare-feu.
3. Vérifiez que le pare-feu mappe le nom d'utilisateur de connexion à l'adresse IP du client :

```
> show user ip-user-mapping ip <ip-address>
IP address:    192.0.2.1 (vsys1)
User:          localdomain\username
From:          SYSLOG
```

4. Déconnectez-vous du système client.
5. Vérifiez que le pare-feu a supprimé le mappage d'utilisateur :

```
> show user ip-user-mapping ip <ip-address>
No matched record
```

## Configuration de l'agent User-ID Windows en tant qu'écouteur Syslog

Pour configurer l'agent User-ID Windows pour créer de nouveaux mappages d'utilisateurs et pour supprimer les mappages obsolètes via la surveillance Syslog, vous devez commencer par définir les profils d'analyse Syslog. L'agent User-ID utilise les profils pour trouver des événements de connexion et de déconnexion dans les messages Syslog. Dans les environnements où les ***expéditeurs Syslog*** (les services réseau qui authentifient les utilisateurs) transmettent des messages Syslog dans des formats divers, configurez un profil pour chaque format de message Syslog. Les messages Syslog doivent respecter certains critères pour qu'un agent User-ID les analyse (reportez-vous à la section Syslog). La présente procédure utilise des exemples présentant les formats suivants :

- Événements de connexion : `[Tue Jul 5 13:15:04 2016 CDT] Administrator authentication success User:johndoe1 Source:192.168.3.212`
- Événements de déconnexion : `[Tue Jul 5 13:18:05 2016 CDT] User logout successful User:johndoe1 Source:192.168.3.212`

Une fois les profils d'analyse Syslog configurés, vous devez spécifier les expéditeurs Syslog que l'agent User-ID doit surveiller.

*L'agent User-ID Windows accepte les messages Syslog uniquement via TCP et UDP. Toutefois, vous devez être vigilant lorsque vous utilisez UDP pour recevoir des messages Syslog, car il s'agit d'un protocole non fiable et il est impossible de vérifier qu'un message provient d'un expéditeur Syslog de confiance. Bien que vous puissiez limiter les messages Syslog à des adresses IP source spécifiques, un pirate peut toujours usurper l'adresse IP, permettant ainsi l'éventuelle injection de messages Syslog non autorisés dans le pare-feu. Il est recommandé d'utiliser TCP au lieu d'UDP. Dans les deux cas, assurez-vous que l'expéditeur Syslog et le client se trouvent tous les deux sur un VLAN sécurisé dédié pour empêcher les hôtes non de confiance d'envoyer des messages Syslog à l'agent User-ID.*

**STEP 1 |** Déployez les agents User-ID Windows si vous ne l'avez pas déjà fait.

1. Installation de l'agent User-ID basé sur Windows.
2. Configurez le pare-feu qui se connectera à l'agent User-ID.

**STEP 2 |** Définissez les profils d'analyse Syslog pour créer et supprimer des mappages d'utilisateurs.

Chaque profil filtre les messages Syslog pour identifier les événements de connexion (pour créer des mappages d'utilisateurs) ou les événements de déconnexion (pour supprimer les mappages) ; aucun profil ne peut faire les deux.

1. Passez en revue les messages Syslog que l'expéditeur Syslog génère pour identifier la syntaxe des événements de connexion et de déconnexion. Vous pourrez ainsi définir les modèles de correspondance lors de la création des profils d'analyse Syslog.

   *Lors de votre examen des messages Syslog, déterminez également s'ils incluent le nom de domaine. Si ce n'est pas le cas, et que vos mappages d'utilisateurs exigent les noms de domaine, saisissez le **Default Domain Name (Nom de domaine par défaut)** lorsque vous définissiez les expéditeurs Syslog que l'agent User-ID surveille (plus loin au cours de cette procédure).*
2. Ouvrez le menu **Start (Démarrer)** de Windows, puis sélectionnez **User-ID Agent (Agent User-ID)**.
3. Sélectionnez **User Identification (Identification utilisateur)** > **Setup (Configuration)** et **Edit (Modifiez)** la configuration.
4. Sélectionnez **Syslog (Syslog)**, **Enable Syslog Service (Activez le service Syslog)**, puis **Add (Ajoutez)** un profil d'analyse Syslog.
5. Saisissez un **Profile Name (Nom de profil)** et une **Description (Description)**.
6. Sélectionnez le **Type (Type)** d'analyse à effectuer pour trouver des événements de connexion et de déconnexion dans les messages Syslog :

   - **Regex (Regex)** : expressions régulières.
   - **Field (Champ)** : chaînes de texte.

   Les étapes suivantes décrivent la configuration de ces types d'analyse.

**STEP 3 |** (**Analyse Regex uniquement**) Définissez les modèles de correspondance de Regex.

Si le message Syslog contient un espace autonome ou une tabulation comme délimiteur, utilisez un caractère **\s** pour un espace et un caractère **\t** pour une tabulation.

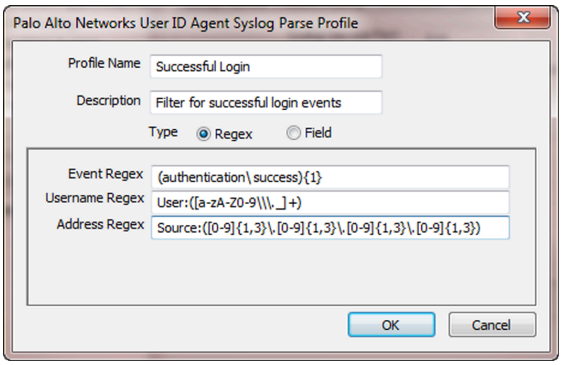
1. Saisissez la **Event Regex (Regex d'événement)** applicable au type d'événements que vous souhaitez trouver :
   - **Événements de connexion** : pour le message d'exemple, l'expression régulière **(authentication\ success){1}** extrait la première **{1}** instance de la chaîne `authentication success`.
   - **Événements de déconnexion** : pour le message d'exemple, l'expression régulière **(logout\ successful){1}** extrait la première **{1}** instance de la chaîne `logout successful`.

   La barre oblique inversée avant l'espace est un caractère d'échappement Regex standard qui indique au moteur Regex de ne pas traiter l'espace comme caractère spécial.
2. Saisissez la **Username Regex (Regex de nom utilisateur)** pour identifier le début du nom d'utilisateur.

   Dans le message d'exemple, la Regex **User:([a-zA-Z0-9\\\._]+)** correspond à la chaîne `User:johndoe1` et identifie `johndoe1` comme nom d'utilisateur.
3. Renseignez la **Address Regex (Regex d'adresse)** qui permet d'identifier la partie de l'adresse IP dans les messages Syslog.

   Dans le message d'exemple, l'expression régulière **Source:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})** correspond à l'adresse IPv4 `Source:192.168.3.212`.

   Voici un exemple d'un profil d'analyse Syslog qui se sert de regex pour identifier des événements de connexion :




4. Cliquez deux fois sur **OK (OK)** pour enregistrer le profil.

**STEP 4 |** (**Analyse de l'identificateur de champ uniquement**) Définissez les modèles de correspondance de chaîne.

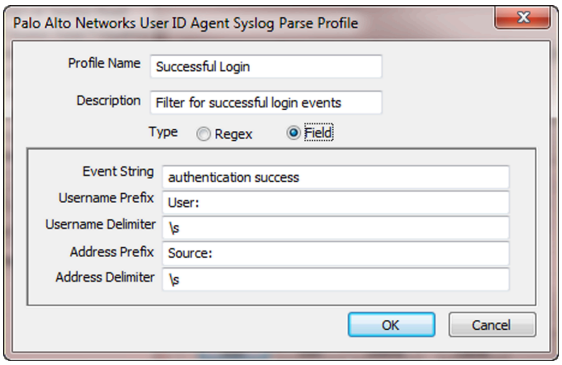
1. Saisissez une **Event String (Chaîne d'événement)** pour identifier le type d'événements que vous souhaitez trouver.
   - **Événements de connexion** : pour le message d'exemple, la chaîne `authentication success` identifie les événements de connexion.
   - **Événements de déconnexion** : pour le message d'exemple, la chaîne `logout successful` identifie les événements de déconnexion.
2. Saisissez un **Username Prefix (Préfixe de nom utilisateur)** pour identifier le début du champ Nom d'utilisateur dans les messages Syslog. Le champ ne prend pas en charge les expressions régulières telles que \s (pour un espace) ou \t (pour un onglet).

   Dans le message d'exemple, `User :` identifie le début du champ de nom d'utilisateur.
3. Saisissez le **Username Delimiter (Délimiteur de nom d'utilisateur)** qui indique la fin du champ Nom d'utilisateur dans les messages Syslog. Utilisez **`\s`** pour indiquer un espace autonome (comme dans le message d'exemple) et **`\t`** pour indiquer un onglet.
4. Saisissez un **Address Prefix (Préfixe d'adresse)** pour identifier le début du champ Adresse IP dans les messages Syslog. Le champ ne prend pas en charge les expressions régulières telles que \s (pour un espace) ou \t (pour un onglet).

   Dans le message d'exemple, `Source :` identifie le début du champ Adresse.
5. Saisissez le **Address Delimiter (Délimiteur d'adresse)** qui indique la fin du champ Adresse IP dans les messages Syslog.

   Par exemple, saisissez **`\n`** pour indiquer que le délimiteur est un saut de ligne.

   Voici un exemple d'un profil d'analyse Syslog qui se sert de la correspondance de chaîne pour identifier des événements de connexion :




6. Cliquez deux fois sur **OK (OK)** pour enregistrer le profil.

**STEP 5 |** Précisez les expéditeurs Syslog que l'agent User-ID surveille.

Parmi les 100 serveurs de tout type que l'agent User-ID peut surveiller, un maximum de 50 peut être des expéditeurs Syslog.

L'agent User-ID ignore tout message Syslog reçu de serveurs qui ne sont pas dans la liste.

1. Sélectionnez **User Identification (Identification utilisateur)** > **Discovery (Découverte)**, puis **Add (Ajoutez)** une entrée à la liste des serveurs.
2. Saisissez un **Name (Nom)** pour identifier l'expéditeur.
3. Saisissez la **Server Address (Adresse serveur)** de l'expéditeur Syslog (adresse IP ou FQDN).
4. Définissez le **Server Type (Type de serveur)** sur **Syslog Sender (Expéditeur Syslog)**.
5. (**Facultatif**) Si vous voulez remplacer le nom de domaine actuel qui se trouve dans le nom d'utilisateur de votre message syslog ou ajouter le domaine au nom d'utilisateur si votre message syslog ne contient pas de domaine, saisissez un **Default Domain Name (Nom de domaine par défaut)**.
6. Pour chaque format Syslog pris en charge par l'expéditeur, **Add (Ajoutez)** un profil d'analyse Syslog à la liste Filter (Filtre). Sélectionnez le **Event Type (Type d'événement)** que chaque profil a été configuré pour identifier : **login (connexion)** (par défaut) ou **logout (déconnexion)**, puis cliquez sur **OK (OK)**.
7. Cliquez sur **OK** pour enregistrer les paramètres.
8. **Commit (Validez)** les changements apportés à la configuration de l'agent User-ID.

**STEP 6 |** Vérifiez que l'agent User-ID ajoute et supprime les mappages d'utilisateur lorsque les utilisateurs se connectent et se déconnectent.

*Vous pouvez utiliser les commandes de la CLI pour voir des renseignements supplémentaires sur les expéditeurs Syslog, sur les messages Syslogs et sur les mappages d'utilisateur.*

1. Connectez-vous à un autre système client pour lequel un expéditeur Syslog faisant l'objet d'une surveillance génère des messages d'événements de connexion et de déconnexion.
2. Vérifiez que l'agent User-ID mappe le nom d'utilisateur de connexion à l'adresse IP du client :
   1. Dans l'agent User-ID, sélectionnez **Monitoring (Surveillance)**.
   2. Entrez le nom d'utilisateur ou l'adresse IP dans le champ de filtrage, **Search (Recherchez)** et vérifiez que le mappage apparaît dans la liste.
3. Vérifiez que le pare-feu a reçu le mappage d'utilisateur de l'agent User-ID :
   1. Connectez-vous à l'ILC du pare-feu.
   2. Exécutez la commande suivante :

```
> show user ip-user-mapping ip <ip-address>
```

Si le pare-feu a reçu le mappage d'utilisateur, le résultat sera semblable à ce qui suit :

```
IP address:    192.0.2.1 (vsys1)
```

```
User:          localdomain\username
From:          SYSLOG
```

4. Déconnectez-vous du système client.
5. Vérifiez que l'agent User-ID a supprimé le mappage d'utilisateur :
   1. Dans l'agent User-ID, sélectionnez **Monitoring (Surveillance)**.
   2. Entrez le nom d'utilisateur ou l'adresse IP dans le champ de filtrage, **Search (Recherchez)** et vérifiez que le mappage n'apparaît pas dans la liste.
6. Vérifiez que le pare-feu a supprimé le mappage d'utilisateur :
   1. Accédez à la CLI du pare-feu.
   2. Exécutez la commande suivante :

```
> show user ip-user-mapping ip <ip-address>
```

Si le pare-feu a supprimé le mappage d'utilisateur, le résultat est comme suit :

```
No matched record
```

# Mappage d'adresses IP à des noms d'utilisateurs à l'aide du portail d'authentification

Lorsqu'un utilisateur initie le trafic Web (HTTP ou HTTPS) correspondant à une Politique d'authentification règle, le pare-feu invite l'utilisateur à s'authentifier via Captive Portal. Cela garantit que vous savez exactement qui accède à vos applications et données les plus sensibles. Sur la base des informations utilisateur collectées lors de l'authentification, le pare-feu crée un nouveau mappage adresse IP-nom d'utilisateur ou met à jour le mappage existant pour cet utilisateur. Cette méthode de mappage utilisateur est utile dans les environnements dans lesquels le pare-feu ne peut pas apprendre les mappages via d'autres méthodes telles que les serveurs de surveillance. Par exemple, vous pouvez avoir des utilisateurs qui ne sont pas connectés à vos serveurs de domaine surveillés, tels que des utilisateurs sur des clients Linux.

- Méthodes d'authentification du portail d'authentification
- Modes du portail d'authentification
- Configuration du portail d'authentification

## Méthodes d'authentification du portail d'authentification

Le portail d'authentification utilise les méthodes suivantes pour authentifier les utilisateurs dont les requêtes Web correspondent aux règles de la politique d'authentification :

| Méthode d'authentification | Description |
|---|---|
| SSO Kerberos | Le pare-feu utilise la Single Sign-On (ouverture de session unique ; SSO) Kerberos pour obtenir de manière transparente les informations d'identification de l'utilisateur du navigateur. Pour utiliser cette méthode, votre réseau requiert une infrastructure |

| Méthode d'authentification | Description |
|---|---|
| | Kerberos, notamment un Key Distribution Center (centre de distribution de clé - KDC) avec un serveur d'authentification et un Ticket Granting Service (service d'émission de tickets - TGS). Le pare-feu doit disposer d'un compte Kerberos.<br><br>En cas d'échec de l'authentification SSO Kerberos, le pare-feu revient au formulaire Web ou à l'authentification du certificat client, selon la configuration de votre politique d'authentification et de votre portail d'authentification. |
| Formulaire Web | Le pare-feu redirige les requêtes Web vers un formulaire Web pour authentification. Pour cette méthode, vous pouvez configurer la politique d'authentification pour utiliser l'authentification à plusieurs facteurs, SAML, Kerberos, TACACS+, RADIUS ou LDAP. Même si les utilisateurs doivent saisir manuellement leurs informations d'identification, cette méthode est compatible avec tous les navigateurs et systèmes d'exploitation. |
| Authentification du certificat client | Le pare-feu demande au navigateur de présenter un certificat client valide pour authentifier l'utilisateur. Pour utiliser cette méthode, vous devez fournir les certificats clients à chaque système utilisateur et installer le certificat d'autorité de certification (CA) de confiance utilisé pour générer ces certificats sur le pare-feu. |

## Modes du portail d'authentification

Le mode du portail d'authentification définit comment le pare-feu capture les requêtes Web pour authentification :

| Mode | Description |
|---|---|
| Transparent | Le pare-feu intercepte le trafic du navigateur en fonction de la règle de la politique d'authentification et remplace l'URL de destination d'origine en générant une requête HTTP 401 de demande d'authentification. Toutefois, étant donné que le pare-feu ne dispose pas du certificat de l'URL de destination, le navigateur affiche une erreur de certificat aux utilisateurs qui tentent d'accéder à un site sécurisé. N'utilisez donc ce mode qu'en cas de nécessité, dans des déploiements de couche 2 ou virtuels par exemple. |
| redirect | Le pare-feu intercepte les sessions HTTP ou HTTPS inconnues et les redirigent vers une interface de Couche 3 du pare-feu à l'aide d'une redirection HTTP 302 pour procéder à l'authentification. Il s'agit du mode préféré car il offre une meilleure expérience à l'utilisateur final (pas d'erreur de certificat). Il requiert cependant |

| Mode | Description |
| --- | --- |
| | une configuration de couche 3 supplémentaire. Un autre avantage du mode Rediriger est qu'il permet l'utilisation de cookies de session, l'utilisateur peut ainsi continuer à consulter des sites authentifiés sans qu'un nouveau mappage ne soit exigé à chaque expiration du délai. Ceci est particulièrement utile pour les utilisateurs passant d'une adresse IP à une autre (du LAN d'entreprise au réseau sans fil par exemple) car ils ne doivent pas nécessairement se réauthentifier lorsque l'adresse IP change tant que la session est ouverte.<br><br>Si vous utilisez SSO Kerberos, vous devez utiliser le mode Rediriger car le navigateur ne fournit les informations d'identification qu'aux sites de confiance. Le mode Rediriger est également requis si vous utilisez Authentification multifacteur pour authentifier les utilisateurs du portail d'authentification. |

## Configuration du portail d'authentification

La procédure suivante décrit comment paramétrer l'authentification du portail d'authentification en configurant l'agent User-ID intégré à PAN-OS afin de rediriger les requêtes Web correspondant à une règle de la politique d'authentification vers une interface du pare-feu (hôte de redirection).

Inspection SSL entrante ***ne prend pas en charge la redirection du portail d'authentification. Pour utiliser la redirection et le décryptage du portail d'authentification, vous devez utiliser le*** proxy de transfert SSL**.**

Selon leur niveau de sensibilité, les applications auxquelles les utilisateurs accèdent via le portail d'authentification reposent sur des paramètres et des méthodes d'authentification différents. Pour respecter toutes les exigences en matière d'authentification, vous pouvez utiliser des objets de mise en œuvre de l'authentification par défaut et personnalisés. Chaque objet associe une règle d'authentification à un profil d'authentification et à une méthode d'authentification du portail d'authentification.

- **Objets de mise en œuvre de l'authentification par défaut** : utilisez les objets par défaut si vous voulez associer plusieurs règles d'authentification au même profil d'authentification général. Vous devez configurer ce profil d'authentification avant de configurer le portail d'authentification, puis l'affecter dans les paramètres du portail d'authentification. Dans le cas de règles d'authentification qui exigent une Multi-Factor Authentication (authentification à plusieurs facteurs ; MFA), vous ne pouvez utiliser les objets de mise en œuvre de l'authentification par défaut.
- **Objets de mise en œuvre de l'authentification personnalisés** : utilisez un objet personnalisé pour chaque règle d'authentification qui exige un profil d'authentification qui diffère du profil général. Les objets personnalisés sont obligatoires pour les règles d'authentification qui reposent sur la MFA. Pour utiliser des objets personnalisés, créez des profils d'authentification et affectez-les aux objets après avoir configuré le portail d'authentification lors de la configuration de la politique d'authentification.

N'oubliez pas que les profils d'authentification ne s'avèrent nécessaires que lorsque les utilisateurs s'authentifient via un formulaire Web du portail d'authentification, ou la SSO Kerberos. En plus de

ces méthodes, vous pouvez éventuellement vous référer aux procédures suivantes, qui décrivent également la mise en œuvre de l'authentification du certificat client.

*Si vous utilisez le portail d'authentification sans les autres fonctions User-ID (mappage d'utilisateur et mappage de groupe), vous n'avez pas besoin de configurer un agent User-ID.*

**STEP 1 |** Configurez les interfaces que le pare-feu utilisera pour les requêtes Web entrantes, en authentifiant les utilisateurs, et en communiquant avec les serveurs d'annuaires pour mapper des noms d'utilisateurs à des adresses IP.

Lorsque le pare-feu se connecte aux serveurs d'authentification ou aux agents User-ID, il utilise l'interface de gestion par défaut. Il est recommandé que vous isoliez votre réseau de gestion en configurant les itinéraires de service pour vous connecter aux serveurs d'authentification ou aux agents User-ID.

1. (Interface MGT uniquement) Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Interfaces (Interfaces)**, modifiez l'interface de **Management (Gestion)**, sélectionnez **User-ID**, puis cliquez sur **OK**.
2. (Interface non MGT uniquement) Affectez un profil de gestion de l'interface à l'interface de Couche 3 que le pare-feu utilisera pour les requêtes Web entrants et pour la communication avec les serveurs d'annuaires. Dans le profil de gestion de l'interface, vous devez activer les **Response Pages (Pages de réponse)** et **User-ID (User-ID)**.
3. (Interface non MGT uniquement) Configurez un itinéraire de service pour l'interface qui sera utilisé par le pare-feu pour authentifier les utilisateurs. Si le pare-feu comporte plusieurs systèmes virtuels (vsys), l'itinéraire de service peut être global ou spécifique au vsys. Les services doivent inclure **LDAP (LDAP)** et éventuellement les suivants :
   - **Kerberos (Kerberos)**, **RADIUS (RADIUS)**, **TACACS+ (TACACS+)** ou **Multi-Factor Authentication (Authentification à facteurs multiples)** : configurez un itinéraire de service pour les services d'authentification que vous utilisez.
   - **UID Agent (Agent UID)** : configurez ce service uniquement en cas d'Activation d'une politique basée sur l'utilisateur et le groupe.
4. (Mode Rediriger uniquement) Créez un enregistrement d'adresse DNS (A) qui mappe l'adresse IP de l'interface de Couche 3 vers l'hôte de redirection. Si vous utiliserez l'authentification SSO Kerberos, vous devez ajouter un enregistrement de pointeur DNS (PTR) exécutant le même mappage.

Si votre réseau ne prend pas en charge l'accès de support aux serveurs d'annuaires à partir d'une interface de pare-feu, une Configuration du mappage d'utilisateur à l'aide de l'agent User-ID Windows est nécessaire.

**STEP 2 |** Vérifiez que le Domain Name System (système de noms de domaine - DNS) est configuré pour résoudre vos adresses de contrôleur de domaine.

Pour vérifier que la résolution fonctionne, envoyez une requête ping au FQDN du serveur. Par exemple :

```
admin@PA-220> ping host dc1.acme.com
```

**STEP 3 |** Configurez les clients pour approuver les certificats du portail d'authentification.

Requis pour le mode Rediriger ; pour rediriger de manière transparente les utilisateurs sans afficher d'erreur de certificat. Vous pouvez générer un certificat auto-signé ou importer un certificat signé par une autorité de certification (CA) externe.

Pour utiliser un certificat auto-signé, créez un certificat CA racine et utilisez-le pour signer le certificat que vous utiliserez pour le portail d'authentification :

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**.
2. Procédez à la création d'un certificat CA racine auto-signé ou à l'importation d'un certificat CA (reportez-vous à la section Importation d'un certificat et d'une clé privée).
3. Procédez à la génération d'un certificat à utiliser pour le portail d'authentification. Veillez à configurer les champs suivants :
   - **Common Name (Nom commun)** : saisissez le nom DNS de l'hôte intranet de l'interface de Couche 3.
   - **Signed By (Signé par)** : sélectionnez le certificat CA que vous venez de créer ou d'importer.
   - Attributs de certificat : cliquez sur **Add (Ajouter)**, pour le **Type (Type)**, sélectionnez **IP (IP)** puis, pour **Value (Valeur)**, saisissez l'adresse IP de l'interface de Couche 3 vers laquelle le pare-feu redirige les requêtes.
4. Configurez un profil de service SSL/TLS. Affectez au profil le certificat du portail d'authentification que vous venez de créer.

   *Si vous n'affectez pas de profil de service SSL/TLS, le pare-feu utilise TLS 1.2 par défaut. Pour utiliser une version TLS différente, configurez un profil de service SSL/TLS pour la version TLS que vous souhaitez utiliser.*
5. Configurez les clients pour approuver le certificat :
   1. Exportez le certificat CA que vous venez de créer ou d'importer.
   2. Importez le certificat en tant que CA racine de confiance dans tous les navigateurs clients, en configurant manuellement le navigateur ou en ajoutant le certificat aux racines de confiance d'un Group Policy Object (objet de politique de groupe - GPO) d'Active Directory (AD).

**STEP 4 |** (Facultatif) Configurez l'authentification du certificat client.

> ***Vous n'avez pas besoin d'un profil ou d'une séquence d'authentification pour authentifier un certificat client. Si vous configurez un profil/une séquence d'authentification et l'authentification du certificat, les utilisateurs doivent s'authentifier avec les deux.***

1. Utilisez le certificat CA racine pour générer un certificat client pour chaque utilisateur qui s'authentifiera via le portail d'authentification. Dans ce cas, la CA est généralement votre CA d'entreprise, et non le pare-feu.
2. Exportez le certificat CA au format PEM sur un système auquel le pare-feu a accès.
3. Importez le certificat CA sur le pare-feu : reportez-vous à la section Importation d'un certificat et d'une clé privée. Une fois l'importation terminée, cliquez sur le certificat importé, sélectionnez **Trusted Root CA (CA racine de confiance)**, puis cliquez sur **OK (OK)**.
4. Configuration d'un profil de certificat.
   - Dans la liste déroulante **Username Field (Champ Nom d'utilisateur)**, sélectionnez le champ du certificat contenant l'identité de l'utilisateur.
   - Dans la liste **CA Certificates (Certificats CA)**, cliquez sur **Add (Ajouter)**, puis sélectionnez le certificat CA que vous venez d'importer.

**STEP 5 |** (Facultatif) Configurez le portail d'authentification pour le Captive Network Assistant d'Apple.

Cette étape n'est obligatoire que si vous utilisez le portail d'authentification avec le Captive Network Assistant (CNA) d'Apple. Pour utiliser le portail d'authentification avec CNA, effectuez les étapes suivantes.

1. Vérifiez que vous avez précisé un FQDN pour la redirection de l'hôte (pas juste une adresse IP).
2. Sélectionnez un profil de service SSL/TLS qui utilise un certificat signé publiquement pour le FQDN spécifié.
3. Saisissez la commande suivante pour ajuster le nombre de demandes prises en charge pour le portail d'authentification : **`set deviceconfig setting ctd cap-portal-ask-requests <valeur de seuil>`**

   Par défaut, le pare-feu a un taux seuil pour le portail d'authentification qui restreint le nombre de demandes à une requête aux deux secondes. Le CNA envoie plusieurs requêtes qui peuvent dépasser ce seuil, ce qui peut entraîner une réinitialisation TCP et une erreur de la part du CNA. La valeur de seuil recommandée est 5 (la valeur par défaut est 1). Cette valeur permet un maximum de cinq demandes aux deux secondes. Selon votre environnement, il se peut que vous deviez configurer une valeur différente. Si la valeur actuelle n'est pas suffisante pour traiter le nombre de demandes, augmentez la valeur.

**STEP 6 |** Configuration des paramètres du portail d'authentification.

1. Sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Authentication Portal Settings (Paramètres du portail d'authentification)** et modifiez les paramètres.
2. **Activer le Portail d'authentification** (il est activé par défaut).
3. Précisez le **Timer (Minuteur)**, qui correspond à la durée de temps maximale (en minutes) pendant laquelle le pare-feu conserve le mappage adresse IP/nom d'utilisateur d'utilisateur après que celui-ci se soit authentifié via le portail d'authentification (valeur par défaut : 60 ; plage comprise entre 1 et 1 440). À l'expiration du **Timer (Minuteur)**, le pare-feu supprime le mappage et tout horodatage d'authentification connexe qui a servi à évaluer le **Timeout (Délai d'expiration)** des règles de la politique d'authentification.

   *Lors de l'évaluation du **Timer (Minuteur)** du portail d'authentification et de la valeur **Timeout (Délai d'expiration)** de chaque règle de politique d'authentification, le pare-feu invite l'utilisateur à s'authentifier de nouveau pour le paramètre qui expire en premier. Une fois que l'utilisateur s'est authentifié de nouveau, le pare-feu remet le compteur du **Timer (Minuteur)** du portail d'authentification à zéro et enregistre les nouveaux horodatages d'authentification de l'utilisateur. Ainsi, pour permettre l'établissement de divers **Timeout (Délais d'expiration)** applicables à différentes règles d'authentification, définissez le **Timer (Minuteur)** du portail d'authentification sur une valeur qui est égale ou supérieure à celle fixée pour tout **Timeout (Délai d'expiration)** d'une règle.*
4. Sélectionnez le **SSL/TLS Service Profile** (Profil de service SSL/TLS) que vous avez créé pour rediriger les requêtes sur TLS. Reportez-vous à la section Configuration d'un profil de service SSL/TLS.
5. Sélectionnez le **Mode (Mode)** (dans cet exemple, **Redirect (Rediriger)**).
6. (Mode Rediriger uniquement) Indiquez le **Redirect Host (Hôte de redirection)**, soit le nom d'hôte intranet (un nom d'hôte sans point) qui résout en adresse IP l'interface de Couche 3 sur le pare-feu vers laquelle les requêtes Web sont redirigées.

   Si les utilisateurs s'authentifient via la Single Sign-On (ouverture de session unique ; SSO) Kerberos, le **Redirect Host (Hôte de redirection)** doit être identique au nom d'hôte indiqué dans le keytab Kerberos.
7. Sélectionnez la méthode d'authentification de repli à utiliser :
   - Si vous utilisez l'authentification du certificat client, sélectionnez le **Certificate Profile (Profil de certificat)** que vous avez créé.
   - Pour utiliser les paramètres globaux pour l'authentification interactive ou SSO, sélectionnez le **Authentication Profile (Profil d'authentification)** que vous avez configuré.
   - Pour utiliser les paramètres propres aux règles de la politique d'authentification pour l'authentification interactive ou SSO, affectez les profils d'authentification aux objets de mise en œuvre de l'authentification lors de la configuration de la politique d'authentification.
8. Cliquez sur **OK (OK)**, puis **Commit (Validez)** la configuration du portail d'authentification.

**STEP 7 |** Étapes suivantes...

Le pare-feu ne présentera pas le formulaire Web du portail d'authentification aux utilisateurs tant que vous n'aurez pas effectué la configuration des règles de la politique d'authentification qui déclenchent l'authentification lorsque des utilisateurs demandent des services ou des applications.

# Configuration du mappage d'utilisateur pour les utilisateurs de serveurs de terminaux

Chaque utilisateur de serveurs de terminaux semble avoir la même adresse IP ; par conséquent, un mappage adresse IP/nom d'utilisateur n'est pas suffisant pour identifier un utilisateur spécifique. Pour identifier des utilisateurs spécifiques sur des serveurs de terminaux Windows, l'agent Terminal Server (agent TS) Palo Alto Networks alloue une plage de ports à chaque utilisateur. Il informe ensuite chaque pare-feu connecté de la plage de ports allouée, ce qui permet au pare-feu de créer une table de mappage adresse IP/nom d'utilisateur et la mise en œuvre de politiques de sécurité en fonction du groupe et de l'utilisateur. Pour les serveurs de terminaux non Windows, configurez l'API XML PAN-OS pour extraire les informations de mappage d'utilisateur. Les valeurs suivantes s'appliquent aux deux méthodes :

- Plage de ports par défaut : 1025 à 65534
- Taille de bloc par utilisateur : 200
- Nombre maximum de systèmes multi-utilisateurs : 2 500

Pour plus d'informations sur les serveurs de terminaux pris en charge par l'agent TS et sur le nombre d'agents TS pris en charge sur chaque modèle de pare-feu, reportez-vous à la section Matrice de compatibilité Palo Alto Networks et l'outil de comparaison de produits.

Les sections suivantes décrivent la configuration du mappage d'utilisateur pour les utilisateurs de serveurs de terminaux :

- Configuration de l'agent Terminal Server (TS) Palo Alto Networks pour le mappage d'utilisateur
- Récupération de mappages d'utilisateurs d'un serveur de terminaux à l'aide de l'API XML PAN-OS

## Configuration de l'agent Terminal Server (TS) Palo Alto Networks pour le mappage d'utilisateur

La procédure suivante vous permet d'installer et de configurer l'agent TS sur le serveur de terminaux. Afin de mapper tous vos utilisateurs, vous devez installer l'agent TS sur tous les serveurs de terminaux auxquels vos utilisateurs se connectent.

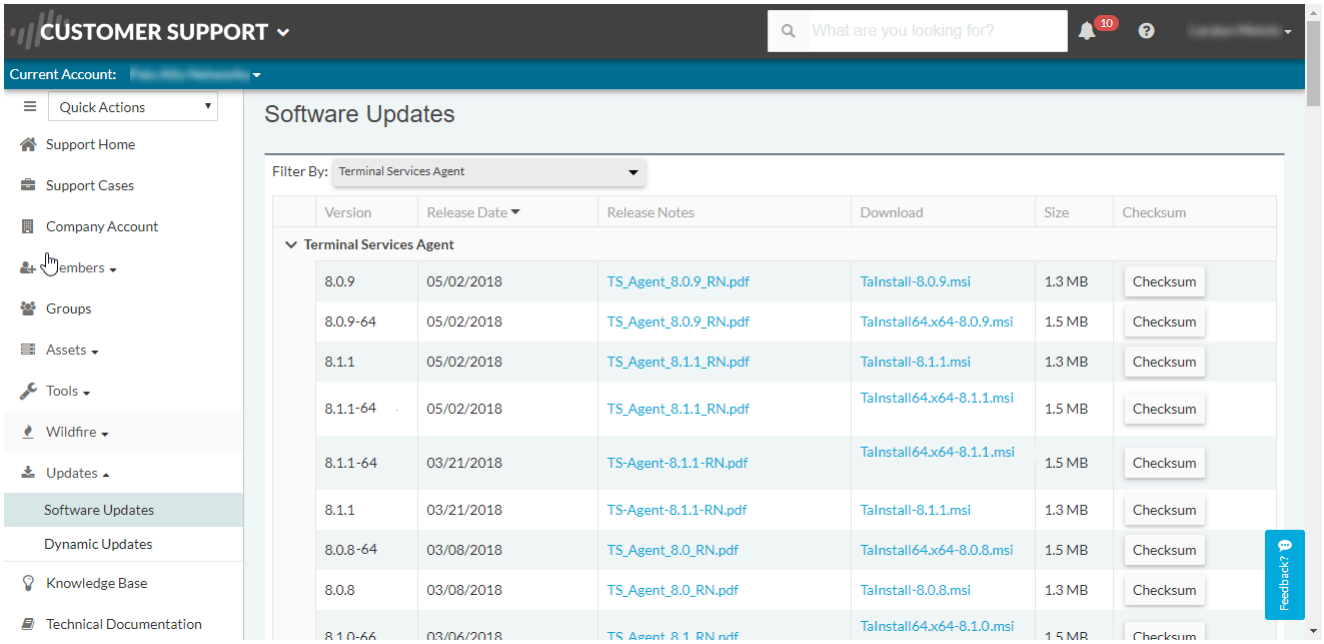
 

*Si vous utilisez l'agent TS 7.0 ou toute version ultérieure, désactivez le logiciel antivirus Sophos sur l'hôte de l'agent TS. Autrement, le logiciel antivirus remplace les ports source que l'agent TS affecte.*

*Pour obtenir de plus amples renseignements sur les valeurs, les plages et les autres spécifications par défaut, reportez-vous à la rubrique* Configuration du mappage d'utilisateur pour les utilisateurs de serveurs de terminaux. *Pour plus d'informations sur les serveurs de terminaux pris en charge par l'agent TS et sur le nombre d'agents TS pris en charge sur chaque modèle de pare-feu, reportez-vous à la section* Matrice de compatibilité Palo Alto Networks.

**STEP 1 |** Téléchargez le programme d'installation de l'agent TS.

1. Connectez-vous au portail de support client de Palo Alto Networks.
2. Sélectionnez **Updates (Mises à jour)** > **Software Updates (Mises à jour logicielles)**.
3. Définissez **Filter By (Filtrer par)** sur **Terminal Services Agent (Agent Terminal Services)**, puis sélectionnez la version de l'agent que vous souhaitez installer dans la colonne Download (Téléchargement) correspondante. Par exemple, pour télécharger l'agent TS 9.0, sélectionnez **TaInstall-9.0.msi**.
4. Enregistrez le fichier `TaInstall.x64-x.x.x-xx.msi` ou `TaInstall-x.x.x-xx.msi` sur les systèmes sur lesquels vous prévoyez installer l'agent : assurez-vous de sélectionner la version appropriée selon la version de système d'exploitation Windows exécutée, 32 ou 64 bits.



**STEP 2 |** Exécutez le programme d'installation en tant qu'administrateur.

1. Ouvrez le menu **Start (Démarrer)** de Windows, faites un clic droit sur le programme **Command Prompt (Invite de commandes)**, puis **Run as administrator (Exécutez en tant qu'administrateur)**.
2. À partir de la ligne de commande, exécutez le fichier .msi que vous avez téléchargé. Par exemple, si vous enregistrez le fichier `TaInstall-9.0.msi` sur le Bureau, saisissez ce qui suit :

```
C:\Users\administrator.acme>cd Desktop
C:\Users\administrator.acme\Desktop>TaInstall-9.0.0-1.msi
```

3. Suivez les invites du programme d'installation pour installer l'agent à l'aide des paramètres par défaut. La configuration installe l'agent sous `C:\ProgramFiles\Palo Alto Networks\Terminal Server Agent`.

   *Pour veiller à la bonne attribution des ports, vous devez utiliser l'emplacement du dossier d'installation de l'agent Terminal Server par défaut.*

4. Lorsque l'installation est terminée, **Close (Fermez)** la boîte de dialogue Configuration.

   *Si vous mettez à niveau une version d'agent TS disposant d'un pilote plus récent que celui de l'installation existante, l'assistant d'installation vous invite à redémarrer le système après la mise à niveau.*

**STEP 3 |** Définissez la plage de ports que l'agent TS doit allouer aux utilisateurs finaux.

*La**System Source Port Allocation Range (Plage d'allocation de ports source du système)** et les **System Reserved Source Ports (Ports source réservés au système)** spécifient la plage de ports qui est allouée aux sessions non utilisateur. Assurez-vous que les valeurs indiquées dans ces champs ne chevauchent pas les ports désignés pour le trafic utilisateur. Ces valeurs peuvent être modifiées uniquement en modifiant les paramètres correspondants du Registre Windows. L'agent TS n'attribue pas les ports du trafic réseau émis par session 0.*

1. Ouvrez le menu **Start** (Démarrer) de Windows, puis sélectionnez **Terminal Server Agent (Agent Terminal Server)** pour lancer l'application de l'agent Terminal Server.
2. **Configure (Configurez)** (menu latéral) l'agent.
3. Définissez la **Source Port Allocation Range (Plage d'allocation de ports source)** (de 20 000 à 39 999 par défaut). Il s'agit de l'ensemble de la plage de numéros de port que l'agent TS allouera pour le mappage d'utilisateur. La plage de ports spécifiée ne doit pas chevaucher la **System Source Port Allocation Range (Plage d'allocation de ports sources du système)**.
4. (Facultatif) Si vous ne souhaitez pas que l'agent TS alloue certains ports ou certaines plages de ports sources aux sessions utilisateur, spécifiez-les dans le champ **Reserved Source**

**Ports (Ports sources réservés)**. Pour inclure plusieurs plages, utilisez des virgules et aucun espace, par exemple : **`2000-3000,3500,4000-5000`**.

5. Spécifiez le nombre de ports à allouer à chaque utilisateur lors de la connexion au serveur de terminaux dans le champ **Port Allocation Start Size Per User (Taille de départ d'allocation de ports par utilisateur)** (200 par défaut).
6. Spécifiez la **Port Allocation Maximum Size Per User (Taille maximale d'allocation de ports par utilisateur)**, qui est le nombre maximum de ports que l'agent Terminal Server peut allouer à chaque utilisateur.
7. Indiquez si vous souhaitez continuer le traitement du trafic de l'utilisateur s'il vient à manquer de ports alloués. L'option **Fail port binding when available ports are used up (Échec de la liaison des ports lorsque les ports disponibles sont utilisés)** est activée par défaut. Celle-ci indique que l'application ne parviendra pas à envoyer le trafic lorsque tous les ports sont utilisés. Pour permettre aux utilisateurs de continuer à utiliser les applications lorsqu'ils sont à court de ports, désactivez (décochez) cette option. Cependant, dans ce cas, le trafic pourrait ne pas être identifié avec User-ID.
8. Si le Terminal Server ne répond plus quand vous essayez de l'arrêter, activer l'option **Detach Agent driver at shutdown**.

**STEP 4 |** (Facultatif) Affectez vos propres certificats pour l'authentification mutuelle entre l'agent TS et le pare-feu.

1. Obtenez votre certificat pour l'agent TS de la PKI de votre entreprise ou générez-en un sur votre pare-feu. La clé privée du certificat Serveur doit être chiffrée et le certificat doit être uploadé au format PEM Effectuez l'une des tâches suivantes sur l'homologue Primaire_A :
   - Générez un certificat sur Panorama.
   - Exportez un certificat de votre Certificate Authority (autorité de certification ; CA), puis chargez-le sur l'agent TS.
2. Ajoutez un certificat de serveur à l'agent TS.
   1. Sur l'agent TS, sélectionnez **Server Certificate (Certificat du serveur)**, puis cliquez sur **Add (Ajouter)**.
   2. Saisissez le chemin et le nom du fichier du certificat envoyé par la CA ou accédez au fichier du certificat.
   3. Entrez le mot de passe de la clé privée.
   4. Cliquez sur **OK**.
   5. **Commit (Validez)** vos modifications.

   *L'agent TS utilise un certificat auto-signé sur le port 5009 avec les informations suivantes :Émetteur : CN=Terminal Server Agent, OU=Engineering, O=Palo Alto Networks, L=Santa Clara, S=California, C=USObjet : CN=Terminal Server Agent, OU=Engineering, O=Palo Alto Networks, L=Santa Clara, S=California, C=US*
3. Configurez et affectez le profil de certificat sur le pare-feu.
   1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates Profile (Profil de certificat)** pour configurer un profil de certificat.

      *Vous ne pouvez affecter qu'un seul profil de certificat aux agents User-ID Windows et aux agents TS. Par conséquent, votre profil de certificat doit comprendre toutes les autorités de certification ayant délivré des certificats chargés sur les agents User-ID Windows et TS connectés.*
   2. Sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Connection Security (Sécurité de la connexion)**.
   3. Modifiez (⚙) et sélectionnez le profil du certificat que vous avez configuré à l'étape précédente comme **User-ID Certificate Profile (Profil du certificat User-ID)**.
   4. Cliquez sur **OK**.
   5. **Commit (Validez)** vos modifications.

**STEP 5 |** Configurez le pare-feu qui se connectera à l'agent Terminal Services.

Suivez les étapes ci-dessous pour chaque pare-feu qui se connectera à l'agent Terminal Services pour recevoir des mappages d'utilisateurs :

1. Sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Terminal Server Agents (Agents Terminal Server)**, puis cliquez sur **Add (Ajouter)**.
2. Donnez un **Name (Nom)** à l'agent Terminal Services.
3. Saisissez le nom d'hôte ou l'adresse IP du **Host (Hôte)** Windows sur lequel l'agent Terminal Services est installé.

   Le nom d'hôte ou adresse IP doit se résoudre en une adresse IP statique. Si vous modifiez le nom d'hôte existant, l'agent TS redémarre lorsque vous validez les modifications pour résoudre le nouveau nom d'hôte. Si le nom d'hôte se résout en plusieurs adresses IP, l'agent TS utilise la première de la liste.
4. (Facultatif) Saisissez le nom d'hôte ou l'adresse IP des **Alternative IP Addresses (Adresses IP alternatives)** qui peuvent apparaître comme adresse IP source du trafic sortant.

   Le nom d'hôte ou adresse IP doit se résoudre en une adresse IP statique. Vous pouvez ajouter jusqu'à 8 adresses IP ou noms d'hôte.
5. Saisissez le numéro de **Port (Port)** sur lequel l'agent écoutera les requêtes de mappage d'utilisateur. Cette valeur doit correspondre à la valeur configurée sur l'agent Terminal Services. Par défaut, le port est défini sur 5009 sur le pare-feu et sur l'agent. Si vous le modifiez ici, vous devez également modifier le champ **Listening Port (Port d'écoute)** dans l'écran **Configure (Configurer)** de l'agent Terminal Services.
6. Assurez-vous que la configuration est **Enabled (Activée)**, puis cliquez sur **OK (OK)**.
7. **Commit (Validez)** vos modifications.
8. Vérifiez que l'état **Connected (Connecté)** est affiché (voyant vert).

**STEP 6 |** Vérifiez que l'agent Terminal Services parvient à mapper les adresses IP aux noms d'utilisateurs et que les pare-feux peuvent se connecter à l'agent.

1. Ouvrez le menu **Start (Démarrer)** de Windows, puis sélectionnez **Terminal Server Agent (Agent Terminal Server)**.
2. Vérifiez que les pare-feu peuvent se connecter en vous assurant que le **Connection Status (État de connexion)** de chaque pare-feu de la liste de connexions est `Connected (Connecté)`.
3. Vérifiez que l'agent Terminal Services parvient à mapper les plages de ports aux noms d'utilisateurs en sélectionnant **Monitor (Surveillance)** dans le menu latéral et en vous assurant que la table de mappage est renseignée.

**STEP 7 |** (Serveurs Windows Server 2012 R2 uniquement) Désactivez le mode protégé amélioré de Microsoft Internet Explorer pour chaque utilisateur qui utilise ce navigateur.

Il n'est pas nécessaire d'effectuer cette tâche pour les autres navigateurs, comme Google Chrome ou Mozilla Firefox.

*Pour désactiver le mode protégé amélioré pour tous les utilisateurs, utilisez la* Politique de sécurité locale.

Effectuez les étapes suivantes sur le serveur Windows :

1. Lancez Internet Explorer.
2. Sélectionnez **Settings (Paramètres)** > **Internet options (Options Internet)** > **Advanced (Avancé)** et faites défiler vers le bas jusqu'à la section Security (Sécurité).
3. Désactivez l'option **Enable Enhanced Protection Mode**.
4. Cliquez sur **OK**.

*Palo Alto Networks recommande de ne pas désactiver le mode protégé d'Internet Explorer, lequel diffère du mode protégé amélioré.*

## Récupération de mappages d'utilisateurs d'un serveur de terminaux à l'aide de l'API XML PAN-OS

L'API XML PAN-OS utilise des requêtes HTTP standard pour envoyer et recevoir des données. Des utilitaires de ligne de commande, comme cURL, peuvent directement émettre des appels API ou en utilisant des structures de scripts ou d'applications prenant en charge les services RESTful.

Pour permettre à un serveur de terminaux non Windows d'envoyer des informations de mappage d'utilisateur directement au pare-feu, créez des scripts qui extraient les événements de connexion et de déconnexion utilisateur, puis utilisez-les pour la saisie au format de requête de l'API XML PAN-OS. Définissez ensuite les méthodes d'envoi de la/des requête(s) de l'API XML au pare-feu à l'aide de cURL ou de wget et en fournissant la clé API du pare-feu pour une communication sécurisée. La création de mappages d'utilisateurs à partir de systèmes multi-utilisateurs, notamment de serveurs de terminaux, nécessite l'utilisation des messages d'API suivants :

- **<multiusersystem>** : définit la configuration d'un système multi-utilisateurs d'API XML sur le pare-feu. Ce message permet la définition de l'adresse IP du serveur de terminaux (qui sera l'adresse source pour tous les utilisateurs sur ce serveur de terminaux). De plus, le message de configuration **<multiusersystem>** spécifie la plage de numéros de ports source à allouer pour le mappage d'utilisateur et le nombre de ports à allouer à chaque utilisateur lors de la connexion (appelé *taille de bloc*). Si vous souhaitez utiliser la plage d'allocation de ports source par défaut (1025-65534) et la taille de bloc (200) par défaut, vous n'avez pas besoin d'envoyer un événement de configuration **<multiusersystem>** au pare-feu. À la place, le pare-feu générera automatiquement la configuration du système multi-utilisateurs d'API XML avec les paramètres par défaut lors de la réception du premier message d'événement de connexion utilisateur.
- **<blockstart>** : utilisé avec les messages **<login>** et **<logout>** pour indiquer le numéro de port source de départ alloué à l'utilisateur. Le pare-feu utilise ensuite la taille de bloc pour déterminer la plage réelle de numéros de ports à mapper à l'adresse IP et au nom d'utilisateur dans le message de connexion. Par exemple, si la valeur **<blockstart>** est de 13200 et que la taille de bloc configurée pour le système multi-utilisateurs est de 300, la plage réelle de ports source allouée à l'utilisateur est comprise entre 13200 et 13499. Chaque connexion initiée

par l'utilisateur doit utiliser un numéro de port source unique dans la plage allouée, permettant au pare-feu d'identifier l'utilisateur en fonction de ses mappages d'adresse IP/port/utilisateur pour la mise en œuvre de règles de sécurité basées sur l'utilisateur et le groupe. Lorsqu'un utilisateur épuise tous les ports alloués, le serveur de terminaux doit envoyer un nouveau message **<login>** allouant une nouvelle plage de ports à l'utilisateur de manière à ce que le pare-feu puisse mettre à jour le mappage d'adresse IP/port/utilisateur. En outre, un seul nom d'utilisateur peut disposer de plusieurs blocs de ports simultanément mappés. Lorsque le pare-feu reçoit un message **<logout>** qui inclut un paramètre **<blockstart>**, il supprime le mappage d'adresse IP/port/utilisateur correspondant de sa table de mappage. Lorsque le pare-feu reçoit un message **<logout>** contenant un nom d'utilisateur et une adresse IP mais aucun paramètre **<blockstart>**, il supprime l'utilisateur de sa table. Enfin, si le pare-feu reçoit un message **<logout>** contenant uniquement une adresse IP, il supprime le système multi-utilisateurs et tous les mappages associés.

*Les fichiers XML que le serveur de terminaux envoie au pare-feu peuvent contenir plusieurs types de messages ; les messages n'ont pas besoin d'être dans un ordre particulier dans le fichier. Cependant, lors de la réception d'un fichier XML contenant plusieurs types de messages, le pare-feu les traitera dans l'ordre suivant : d'abord les requêtes du système multi-utilisateurs, suivies par les connexions, puis les déconnexions.*

Le flux de travail suivant fournit un exemple d'utilisation de l'API XML PAN-OS pour envoyer des mappages d'utilisateurs d'un serveur de terminaux non Windows au pare-feu.

**STEP 1 |** Générez la clé API qui sera utilisée pour authentifier la communication API entre le pare-feu et le serveur de terminaux. Pour générer la clé, vous devez fournir les informations d'identification de connexion d'un compte administrateur ; l'API est disponible pour tous les administrateurs (y compris les administrateurs qui disposent des droits d'API XML).

*Tout caractère spécial contenu dans le mot de passe doit être codé en pourcentage/URL.*

Connectez-vous au pare-feu à partir d'un navigateur. Puis, pour générer la clé API pour le pare-feu, ouvrez une nouvelle fenêtre de navigateur et saisissez l'URL suivante :

```
https://<Firewall-IPaddress>/api/?
type=keygen&user=<username>&password=<password>
```

Où **<Firewall-IPaddress>** est l'adresse IP ou le nom de domaine complet du pare-feu, et **<username>** et **<password>** sont les informations d'identification du compte utilisateur administrateur sur le pare-feu. Par exemple :

```
https://10.1.2.5/api/?type=keygen&user=admin&password=admin
```

Le pare-feu répond par un message contenant la clé, par exemple :

```
<response status="success">
   <result>
      <key>k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg=</key>
   </result>
```

```
</response>
```

**STEP 2 |** (Facultatif) Générez un message de configuration que le serveur de terminaux enverra pour spécifier la plage de ports et la taille de bloc des ports par utilisateur que votre agent Terminal Server utilise.

Si l'agent Terminal Server n'envoie aucun message de configuration, le pare-feu crée automatiquement une configuration d'agent Terminal Server à l'aide des paramètres par défaut suivants lors de la réception du premier message de connexion :

- Plage de ports par défaut : 1025 à 65534
- Taille de bloc par utilisateur : 200
- Nombre maximum de systèmes multi-utilisateurs : 1 000

Vous trouverez ci-dessous un exemple de message de configuration :

```
<uid-message>
  <payload>
<multiusersystem>
<entry ip="10.1.1.23" startport="20000"          endport="39999"
 blocksize="100/">
</multiusersystem>
</payload>
<type>update</type>
<version>1.0</version>
</uid-message>
```

où **entry ip** spécifie l'adresse IP affectée aux utilisateurs de serveurs de terminaux, **startport** et **endport** indiquent la plage de ports à utiliser lors de l'allocation de ports à chaque utilisateur, et **blocksize** précise le nombre de ports à allouer à chaque utilisateur. La taille de bloc maximale est de 4000 et chaque système multi-utilisateurs peut allouer 1000 blocs maximum.

Si vous définissez une taille de bloc ou une plage de ports personnalisée, n'oubliez pas que vous devez configurer les valeurs de manière à ce que chaque port de la plage soit alloué et qu'il n'y ait aucun intervalle ou port inutilisé. Par exemple, si vous définissez la plage de ports sur 1000-1499, vous pouvez définir la taille de bloc sur 100, mais pas sur 200. En effet, si vous la définissiez sur 200, il y aurait des ports inutilisés à la fin.

**STEP 3 |** Créez un script qui extraira les événements de connexion et créera le fichier d'entrée XML à envoyer au pare-feu.

Assurez-vous que le script met en œuvre l'allocation de plages de numéros de ports dans des limites fixes sans aucun chevauchement de port. Par exemple, si la plage de ports est de 1000-1999 et que la taille de bloc est de 200, les valeurs <blockstart> acceptables sont 1000,

1200, 1600 et 1800. Les valeurs <blockstart> 1001, 1300 ou 1850 ne sont pas acceptables, car certains des numéros de ports de la plage sont inutilisés.

*La charge utile d'événement de connexion que le serveur de terminaux envoie au pare-feu peut contenir plusieurs événements de connexion.*

Vous trouverez ci-dessous le format du fichier d'entrée d'un événement de connexion XML PAN-OS :

```
<uid-message>
<payload>
<login>
<entry name="acme\jjaso" ip="10.1.1.23" blockstart="20000">
<entry name="acme\jparker" ip="10.1.1.23" blockstart="20100">
<entry name="acme\ccrisp" ip="10.1.1.23" blockstart="21000">
</login>
</payload>
<type>update</type>
<version>1.0</version>
</uid-message>
```

Le pare-feu utilise ces informations pour renseigner sa table de mappage d'utilisateur. En fonction des mappages extraits à partir de l'exemple ci-dessus, si le pare-feu recevait un paquet contenant une adresse et un port source de 10.1.1.23:20101, il mapperait la requête à l'utilisateur jparker pour la mise en œuvre de politiques.

*Chaque système multi-utilisateurs peut allouer 1 000 blocs de ports maximum.*

**STEP 4 |** Créez un script qui extraira les événements de déconnexion et créera le fichier d'entrée XML à envoyer au pare-feu.

Lors de la réception d'un message d'événement **logout** contenant un paramètre **blockstart**, le pare-feu supprime le mappage d'adresse IP/port/utilisateur correspondant. Si le message **logout** contient un nom d'utilisateur et une adresse IP mais aucun paramètre **blockstart**, le pare-feu supprime tous les mappages d'utilisateurs. Si le message **logout** contient uniquement une adresse IP, le pare-feu supprime le système multi-utilisateurs et tous les mappages associés.

Vous trouverez ci-dessous le format du fichier d'entrée d'un événement de déconnexion XML PAN-OS :

```
<uid-message>
<payload>
<logout>
<entry name="acme\jjaso" ip="10.1.1.23" blockstart="20000">
<entry name="acme\ccrisp" ip="10.1.1.23">
<entry ip="10.2.5.4">
</logout>
</payload>
<type>update</type>
<version>1.0</version>
```

```
</uid-message>
```

*Vous pouvez également effacer l'entrée du système multi-utilisateurs du pare-feu, à l'aide de la commande CLI suivante :* ***clear xml-api multiusersystem***

**STEP 5 |** Assurez-vous que les scripts que vous créez permettent de mettre en œuvre dynamiquement la mise en correspondance de la plage de blocs de ports allouée à l'aide de l'API XML au port source réel affecté à l'utilisateur sur le serveur de terminaux et que le mappage est supprimé lorsque l'utilisateur se déconnecte ou que l'allocation de ports change.

Pour cela, vous pouvez utiliser les règles Netfilter-NAT afin de masquer les sessions utilisateur derrière les plages de ports spécifiques allouées via l'API XML en fonction de l'UID. Par exemple, pour vous assurer qu'un utilisateur dont l'ID utilisateur jjaso est mappé à une valeur Source Network Address Translation (traduction d'adresse réseau source ; SNAT) de 10.1.1.23:20000-20099, le script que vous créez doit inclure ce qui suit :

```
[root@ts1 ~]# iptables -t nat -A POSTROUTING -m owner --uid-owner
 jjaso -p tcp -j SNAT --to-source 10.1.1.23:20000-20099
```

De la même manière, les scripts que vous créez doivent également permettre à la configuration de routage de la table des adresses IP de supprimer dynamiquement le mappage SNAT, lorsque l'utilisateur se déconnecte ou que l'allocation de ports change :

```
[root@ts1 ~]# iptables -t nat -D POSTROUTING 1
```

**STEP 6 |** Déterminez la méthode de mise en package des fichiers d'entrée XML contenant les événements de configuration, de connexion et de déconnexion dans les messages wget ou cURL pour la transmission au pare-feu.

**Pour appliquer le fichier sur le pare-feu à l'aide de wget :**

```
> wget --post file <filename> “https://<Firewall-IPaddress>/api/?type=user-id&key=<key>&file-name=<input_filename.xml>&client=wget&vsys=<VSYS_name>”
```

Par exemple, la syntaxe d'envoi d'un fichier d'entrée nommé login.xml au pare-feu à l'adresse 10.2.5.11 avec la clé `k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg` à l'aide de wget est la suivante :

```
> wget --post file login.xml “https://10.2.5.11/api/?type=user-id&key=k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg&file-name=login.xml&client=wget&vsys=vsys1”
```

**Pour appliquer le fichier sur le pare-feu à l'aide de cURL :**

```
> curl --form file=@<filename> https://<Firewall-IPaddress>/api/?type=user-id&key=<key>&vsys=<VSYS_name>
```

Par exemple, la syntaxe d'envoi d'un fichier d'entrée nommé login.xml au pare-feu à l'adresse 10.2.5.11 avec la clé `k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg` à l'aide de cURL est la suivante :

```
> curl --form file@login.xml “https://10.2.5.11/api/?type=user-id&key=k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg&vsys=vsys1”
```

**STEP 7 |** Vérifiez que le pare-feu parvient à recevoir les événements de connexion des serveurs de terminaux.

Vérifiez la configuration en établissant une connexion SSH sur le pare-feu puis en exécutant les commandes CLI suivantes :

**Pour vérifier si le serveur de terminaux se connecte au pare-feu via XML :**

```
admin@PA-5250> show user xml-api multiusersystem
Host            Vsys    Users   Blocks
-------------------------------------
10.5.204.43   vsys1      5         2
```

**Pour vérifier si le pare-feu reçoit des mappages d'un serveur de terminaux via XML :**

```
admin@PA-5250> show user ip-port-user-mapping all

Global max host index 1, host hash count 1

XML API Multi-user System 10.5.204.43
Vsys 1, Flag 3
Port range: 20000 - 39999
Port size: start 200; max 2000
```

```
Block count 100, port count 20000
20000-20199: acme\administrator

Total host: 1
```

## Envoi de mappages d'utilisateurs à User-ID à l'aide de l'API XML

User-ID offre de nombreuses méthodes novatrices d'obtenir les informations de mappage d'utilisateur. Vous pourriez toutefois disposer d'applications ou de périphériques qui capturent les informations des utilisateurs sans toutefois pouvoir s'intégrer nativement à User-ID. Par exemple, vous pourriez disposer d'une application personnalisée, qui a été développée à l'interne, ou d'un périphérique qu'aucune méthode de mappage d'utilisateur standard prend en charge. Dans de tels cas, vous pouvez utiliser l'API XML PAN-OS pour créer des scripts personnalisés qui envoient les informations à l'agent User-ID intégré à PAN-OS ou directement au pare-feu. L'API XML PAN-OS utilise des requêtes HTTP standard pour envoyer et recevoir des données. Des appels API peuvent être émis directement par des utilitaires de ligne de commande, comme cURL, ou en utilisant des structures de scripts ou d'applications prenant en charge les requêtes POST et GET.

Pour permettre à un système externe d'envoyer des informations de mappage d'utilisateur à l'agent User-ID intégré à PAN-OS, créez des scripts qui extraient les événements de connexion et de déconnexion utilisateur et les utilisent pour la saisie de requête de l'API XML PAN-OS. Puis définissez les méthodes d'envoi des requêtes de l'API XML au pare-feu (à l'aide de cURL, par exemple) et utilisez la clé API du pare-feu pour la communication sécurisée. Pour plus d'informations, reportez-vous au Guide d'utilisation de l'API XML PAN-OS.

# Activation d'une politique basée sur l'utilisateur et le groupe

Après avoir effectué l'activation d'User-ID, vous serez en mesure de configurer la Politique de sécurité qui s'applique à des utilisateurs et groupes donnés. Le contrôle des règles basé sur les utilisateurs peut également inclure des informations sur les applications (y compris la catégorie et sous-catégorie auxquelles elles appartiennent, la technologie sous-jacente ou les caractéristiques de l'application). Vous pouvez définir des règles de politique pour sécuriser l'accès aux applications en fonction des utilisateurs ou de groupes d'utilisateurs, qu'il s'agisse d'un trafic montant ou descendant.

Exemples de règles basées sur les utilisateurs :

- Restriction des outils comme SSH, Telnet et FTP sur le port standard au département informatique uniquement.
- Autorisation pour le groupe des services d'assistance d'utiliser Slack.
- Possibilité pour tous les utilisateurs d'accéder à Facebook, mais blocage des applications Facebook, et limiter la publication au seul département marketing.

# Activation d'une politique pour les utilisateurs disposant de plusieurs comptes

Si un utilisateur de votre entreprise compte plusieurs attributions, cet utilisateur peut disposer de plusieurs noms d'utilisateurs (comptes), chacun étant doté de droits d'accès distincts à un ensemble de services spécifiques, mais tous les noms d'utilisateurs partagent la même adresse IP (système client de l'utilisateur). Toutefois, l'agent User-ID peut mapper une adresse IP (ou l'adresse IP et la plage de ports pour les utilisateurs de serveurs de terminaux) à un seul nom d'utilisateur pour mettre en œuvre une politique, et vous ne pouvez pas savoir quel nom d'utilisateur sera mappé par l'agent. Pour contrôler l'accès pour tous les noms d'utilisateurs d'un utilisateur, vous devez apporter des modifications aux règles, groupes d'utilisateurs et à l'agent User-ID.

Par exemple, supposons que le pare-feu inclut une règle autorisant le nom d'utilisateur corp_user à accéder à la messagerie et une règle autorisant le nom d'utilisateur admin_user à accéder au serveur MySQL. L'utilisateur se connecte avec l'un des noms d'utilisateurs à partir de la même adresse IP client. Si l'agent User-ID mappe l'adresse IP à corp_user, si l'utilisateur se connecte en tant que corp_user ou admin_user, le pare-feu identifie alors cet utilisateur comme étant corp_user et autorise l'accès à la messagerie mais non au serveur MySQL. Par ailleurs, si l'agent User-ID mappe l'adresse IP à admin_user, le pare-feu identifie toujours l'utilisateur comme étant admin_user, quelle que soit sa connexion, et autorise l'accès au serveur MySQL mais non à la messagerie. Les étapes suivantes décrivent comment appliquer les deux règles de cet exemple.

**STEP 1 |** Configurez un groupe d'utilisateurs pour chaque service qui requiert des droits d'accès distincts.

Dans cet exemple, chaque groupe correspond à un seul service (messagerie ou serveur MySQL). Toutefois, il est classique de configurer chaque groupe pour un ensemble de services qui requièrent les mêmes droits (par exemple, un groupe pour tous les services utilisateur de base et un groupe pour tous les services administratifs).

Si votre entreprise dispose déjà de groupes d'utilisateurs pouvant accéder aux services nécessaires à l'utilisateur, ajoutez simplement le nom d'utilisateur utilisé pour les services moins limités à ces groupes. Dans cet exemple, le serveur de messagerie requiert un accès moins limité que le serveur MySQL, et corp_user est le nom d'utilisateur pour accéder à la messagerie. Vous ajoutez donc corp_user à un groupe ayant accès à la messagerie (corp_employees) et à un groupe ayant accès au serveur MySQL (network_services).

Si l'ajout d'un nom d'utilisateur à un groupe existant spécifique est susceptible d'enfreindre les pratiques de votre entreprise, vous pouvez créer un groupe personnalisé basé sur un filtre LDAP. Dans cet exemple, network_services correspond à un groupe personnalisé, que vous configurez comme suit :

1. Sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Group Mapping Settings (Paramètres de mappage de groupe)** et **Add (Ajoutez)** une configuration de mappage de groupe avec un **Name (Nom)** distinct.
2. Sélectionnez un **Server Profile (Profil de serveur)** LDAP et vérifiez que la case **Enabled (Activée)** est cochée.
3. Sélectionnez l'onglet **Custom Group (Groupe personnalisé)** et cliquez sur **Add (Ajouter)** pour ajouter un groupe personnalisé avec le **Name (Nom)** network_services.
4. Spécifiez un **LDAP Filter (Filtre LDAP)** correspondant à un attribut LDAP de corp_user et cliquez sur **OK (OK)**.

5. Cliquez sur **OK**, puis sur **Commit (Valider)**.

   ***Ultérieurement, si d'autres utilisateurs du groupe de services moins limités se voient attribuer d'autres noms d'utilisateurs permettant d'accéder à des services plus limités, vous pouvez ajouter ces noms d'utilisateurs au groupe de services plus limités. Ce scénario est plus fréquent que l'inverse ; généralement, un utilisateur ayant accès aux services plus limités a déjà accès aux services moins limités.***

**STEP 2 |** Configurez les règles contrôlant l'accès utilisateur en fonction des groupes que vous venez de configurer.

Pour obtenir de plus amples renseignements, reportez-vous à la section Activer la mise en œuvre d'une politique basée sur un utilisateur et sur un groupe.

1. Configurez une règle de sécurité qui autorise le groupe corp_employees à accéder à la messagerie.
2. Configurez une règle de sécurité qui autorise le groupe network_services à accéder au serveur MySQL.

**STEP 3 |** Configurez la liste d'exceptions l'agent User-ID.

Cela garantit que l'agent User-ID mappe l'adresse IP client au nom d'utilisateur membre des groupes affectés aux règles que vous venez de configurer uniquement. La liste d'exceptions doit contenir tous les noms d'utilisateurs des utilisateurs non membres de ces groupes.

Dans cet exemple, vous ajoutez admin_user à la liste d'exceptions de l'agent User-ID basé sur Windows pour vous assurer qu'il mappe l'adresse IP client à corp_user. Cela garantit que, si l'utilisateur se connecte en tant que corp_user ou admin_user, le pare-feu identifie l'utilisateur comme étant corp_user et applique les deux règles que vous avez configurées car corp_user est membre des groupes auxquels les règles font référence.

1. Créez un fichier `ignore_user_list.txt`.
2. Ouvrez le fichier et ajoutez admin_user.

   Si vous ajoutez d'autres noms d'utilisateurs ultérieurement, chaque nom doit se trouver sur une nouvelle ligne.
3. Enregistrez le fichier dans le dossier de l'agent User-ID sur le serveur de domaines où l'agent est installé.

   ***Si vous utilisez l'agent User-ID intégré à PAN-OS, reportez-vous à la section Configuration du mappage d'utilisateur à l'aide de l'agent User-ID intégré à PAN-OS pour obtenir des instructions sur la configuration de la liste d'exceptions.***

**STEP 4 |** Configurez l'authentification du terminal pour les services limités.

Le terminal peut vérifier les informations d'identification de l'utilisateur et autoriser l'accès pour les utilisateurs disposant de plusieurs noms d'utilisateurs.

Dans cet exemple, vous avez configuré une règle de pare-feu qui autorise corp_user, en tant que membre du groupe network_services, à envoyer une demande de service au serveur MySQL. Vous devez maintenant configurer le serveur MySQL pour qu'il réponde à un nom

d'utilisateur non autorisé (corp_user par exemple) en invitant l'utilisateur à saisir les informations d'identification de connexion d'un nom d'utilisateur autorisé (admin_user).

***Si l'utilisateur se connecte au réseau en tant que admin_user, l'utilisateur peut alors accéder au serveur MySQL sans que les informations d'identification de admin_user lui soient redemandées.***

Dans cet exemple, corp_user et admin_user disposent de comptes de messagerie. Le serveur de messagerie ne demandera donc pas d'autres informations d'identification, quel que soit le nom d'utilisateur saisi par l'utilisateur lors de la connexion au réseau.

Le pare-feu est désormais prêt à appliquer les règles pour un utilisateur disposant de plusieurs noms d'utilisateurs.

# Vérification de la configuration de User-ID

Une fois que vous avez configuré le mappage des utilisateurs et groupes, activé l'User-ID dans votre politique de sécurité et configuré la politique d'authentification, vous devez vérifier que l'User-ID fonctionne correctement.

**STEP 1 |** Accédez à la CLI du pare-feu.

**STEP 2 |** Vérifiez le bon fonctionnement du mappage de groupe.

À l'aide de la CLI, saisissez la commande opérationnelle suivante :

```
> show user group-mapping statistics
```

**STEP 3 |** Vérifiez le bon fonctionnement du mappage d'utilisateur.

Si vous utilisez l'agent User-ID intégré à PAN-OS, vous pouvez le vérifier à l'aide de la CLI en exécutant la commande suivante :

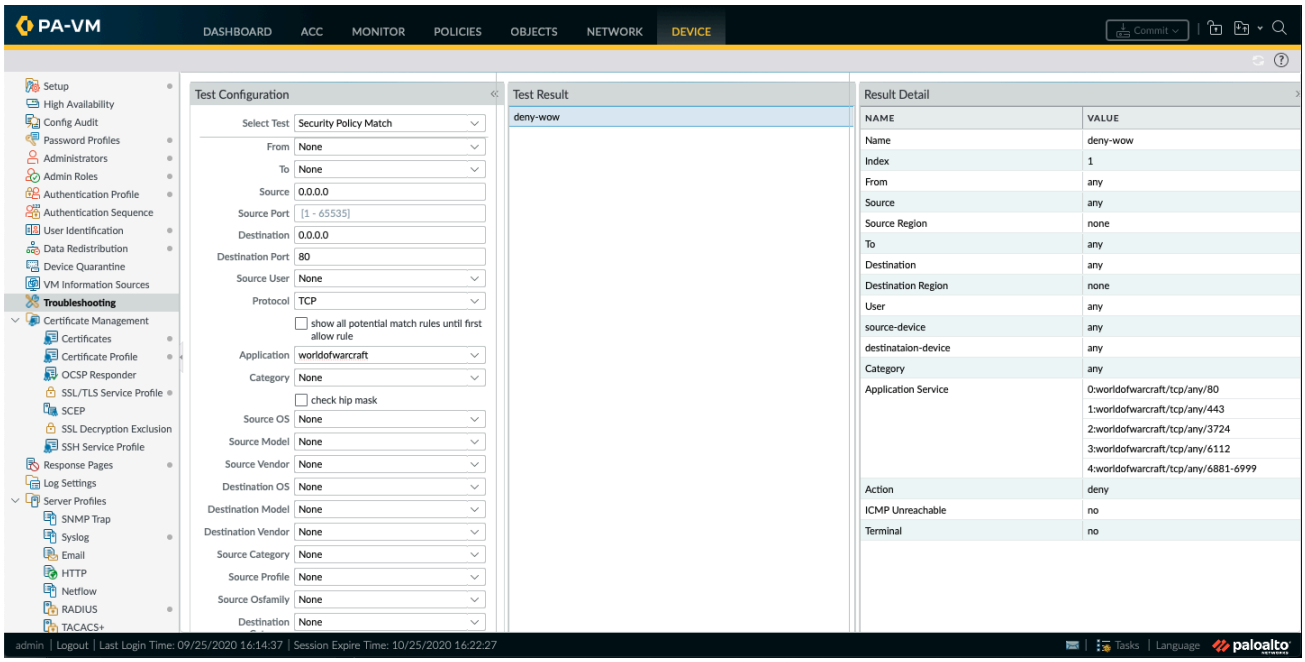
```
> show user ip-user-mapping-mp all
IP              Vsys  From  User         Timeout (sec)
------------------------------------------------------
192.168.201.1   vsys1 UIA   acme\george            210
192.168.201.11  vsys1 UIA   acme\duane             210
192.168.201.50  vsys1 UIA   acme\betsy             210
192.168.201.10  vsys1 UIA   acme\administrator     210
192.168.201.100 vsys1 AD    acme\administrator     748
Total: 5 users
*: WMI probe succeeded
```

**STEP 4 |** Testez votre Règle de politique de sécurité.

- Sur une machine située dans la zone où l'agent User-ID est activé, tentez d'accéder à des sites et des applications pour tester les règles définies dans votre politique et vérifier que le trafic est autorisé ou refusé comme souhaité.
- Vous pouvez également dépanner la configuration active pour déterminer si la politique est correctement configurée. Par exemple, supposons que vous disposez d'une règle interdisant à des utilisateurs de jouer à World of Warcraft. Vous pouvez tester la politique comme suit :

  1. Sélectionnez **Device (Périphérique)** > **Troubleshooting (Résolution des problèmes)**, puis sélectionnez **Security Policy Match (Correspondance de la politique de sécurité)** dans la liste déroulante Select Test (Sélectionner le test).
  2. Saisissez **`0.0.0.0`** en tant qu'adresses IP source et de destination. Le test de correspondance de la politique aux adresses IP source et de destination sera alors exécuté.
  3. Saisissez le port de destination.
  4. Saisissez le protocole.
  5. **Execute (Exécutez)** le test de correspondance de la politique de sécurité.



**STEP 5 |** Testez votre politique d'authentification et la configuration du portail d'authentification.

1. Dans la même zone, accédez à une machine ne faisant pas partie de votre annuaire, un système Mac OS par exemple, et tentez d'exécuter une commande ping sur un système en dehors de la zone. La commande ping doit fonctionner sans demander d'authentification.
2. Sur cette même machine, ouvrez un navigateur et accédez à un site Web dans une zone de destination conforme à la règle d'authentification que vous avez définie. Le formulaire Web du portail d'authentification devrait s'afficher et vous demander vos identifiants.
3. Connectez-vous avec les informations d'identification appropriées et vérifiez que vous êtes redirigé vers la page demandée.
4. Vous pouvez également tester votre politique d'authentification à l'aide de la commande opérationnelle **`test authentication-policy-match`** comme suit :

```
> test authentication-policy-match from corporate to internet
  source 192.168.201.10 destination 8.8.8.8
Matched rule: 'authentication portal' action: web-form
```

**STEP 6 |** Vérifiez que les fichiers journaux affichent les noms d'utilisateur.

Sélectionnez une page de journaux (par exemple, **Monitor (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)**) et vérifiez que les noms d'utilisateur figurent dans la colonne Source User (Utilisateur source).

**STEP 7 |** Vérifiez que les noms d'utilisateur figurent dans les rapports.

1. Sélectionnez **Monitor (Surveillance)** > **Reports (Rapports)**.
2. Sélectionnez un type de rapport qui inclut les noms d'utilisateur. Par exemple, la liste des utilisateurs qui ont tenté d'accéder aux applications devrait figurer dans la colonne Source User (Utilisateur source) du rapport Denied Applications (Applications refusées).

# Déploiement de User-ID dans un réseau à grande échelle

Un réseau à grande échelle peut posséder des centaines de sources d'informations que les pare-feu interrogent pour mapper les adresses IP aux noms d'utilisateur et pour mapper les noms d'utilisateur aux groupes d'utilisateurs. Vous pouvez simplifier l'administration User-ID d'un tel réseau en groupant les informations de mappage utilisateurs et de mappage de groupes avant que les agents User-ID les recueillent, réduisant ainsi le nombre d'agents requis.

Un réseau à grande échelle peut également posséder de nombreux pare-feu qui utilisent les informations de mappage pour appliquer les politiques. Vous pouvez réduire la quantité de ressources que les pare-feu et les sources d'information utilisent dans le cadre du processus d'interrogation en configurant certains pare-feu pour qu'ils acquièrent les informations de mappage via la redistribution plutôt que via une interrogation directe. La redistribution permet également aux pare-feux d'appliquer les politiques basées sur l'utilisateur lorsque les utilisateurs dépendent des sources locales pour s'authentifier (par exemple, services d'annuaire régionaux), mais qui doivent avoir accès à des services et des applications à distance (par exemple, des applications de centres de données globales).

Si vous effectuez la Configuration de la politique d'authentification, vos pare-feu doivent également redistribués les Horodatages d'authentification associés aux réponses données par les utilisateurs aux demandes d'authentification. Les pare-feux utilisent les horodatages pour évaluer les délais d'expiration des Règles de politiques d'authentification. Les délais d'expiration permettent à l'utilisateur qui s'authentifie avec succès de faire des requêtes ultérieures de services ou d'applications sans avoir à s'authentifier à nouveau avant le délai d'expiration. La Redistribution des horodatages vous permet d'appliquer des délais d'expiration uniformes pour chaque utilisateur même si le pare-feu qui autorise initialement l'accès à un utilisateur n'est pas le même pare-feu qui contrôle ultérieurement l'accès pour cet utilisateur.

Si vous avez configuré plusieurs systèmes virtuels, vous pouvez partager les informations de mappage adresse/nom d'utilisateur sur l'ensemble des systèmes virtuels en sélectionnant un système virtuel en tant que pôle User-ID.

- Déploiement de User-ID pour de nombreuses sources d'informations de mappage
- Redistribution des données et horodatages d'authentification
- Partage des mappages User-ID sur l'ensemble des systèmes virtuels

## Déploiement de User-ID pour de nombreuses sources d'informations de mappage

Vous pouvez utiliser le transfert des journaux Windows et des serveurs de catalogues globaux pour simplifier le mappage d'utilisateur et le mappage de groupe dans un réseau à grande échelle de contrôleurs de domaines Microsoft Active Directory (AD) ou de serveurs Exchange. Ces méthodes simplifient l'administration User-ID en groupant les informations de mappage avant que les agents User-ID les recueillent, réduisant ainsi le nombre d'agents requis.

- Transfert des journaux Windows et des serveurs de catalogues globaux
- Planification d'un déploiement User-ID à grande échelle
- Configuration du transfert des journaux Windows
- Configuration de User-ID pour de nombreuses sources d'informations de mappage

## Transfert des journaux Windows et des serveurs de catalogues globaux

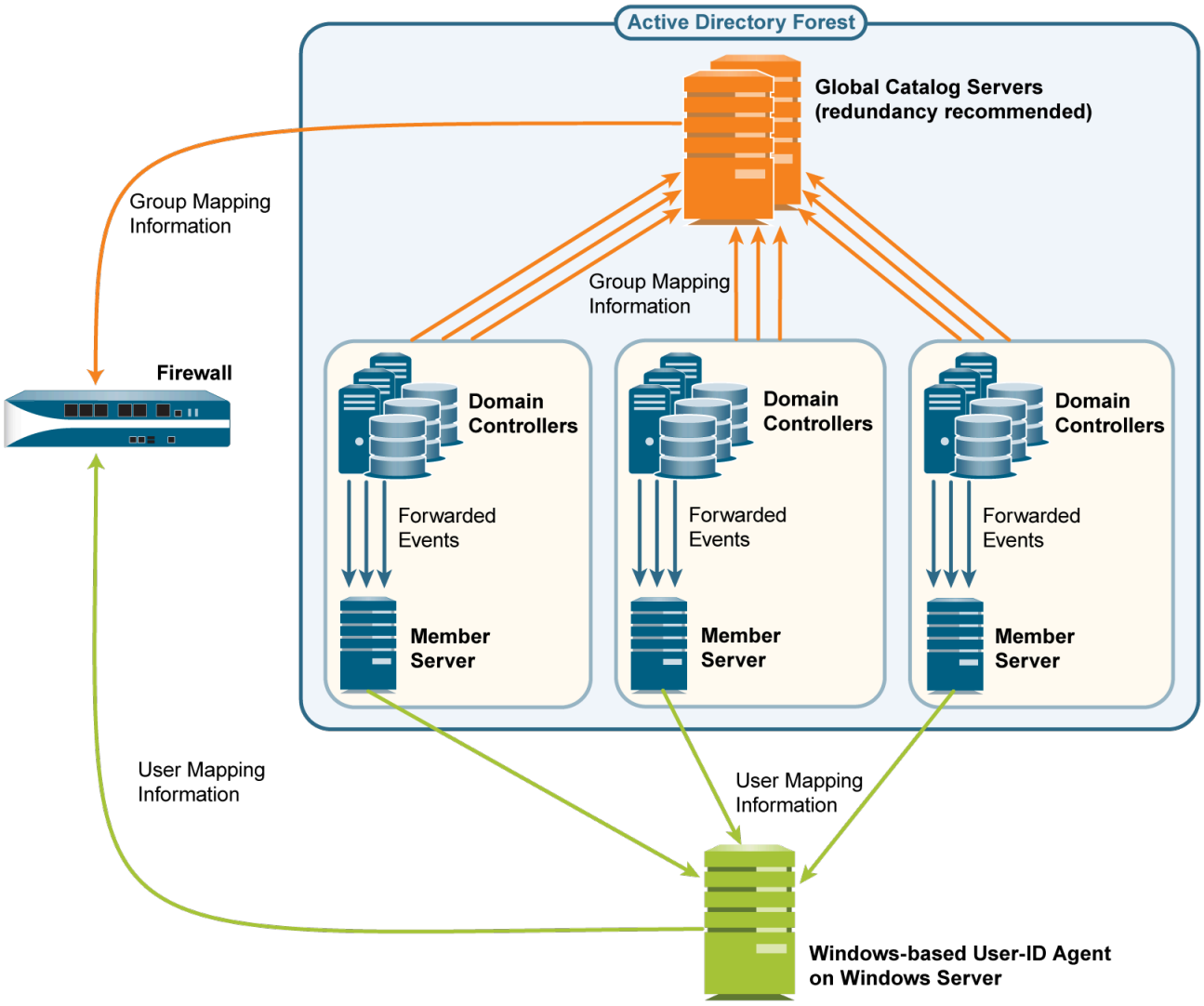
Chaque agent User-ID pouvant surveiller jusqu'à 100 serveurs, le pare-feu a besoin de plusieurs agents User-ID pour surveiller un réseau comptant des milliers de contrôleurs de domaines AD ou serveurs Exchange. La création et la gestion d'un grand nombre d'agents User-ID implique une surcharge administrative conséquente, notamment pour le développement des réseaux dans lesquels le suivi de nouveaux contrôleurs de domaines est difficile. Le transfert des journaux Windows vous permet de minimiser la surcharge administrative en réduisant le nombre de serveurs à surveiller, réduisant ainsi le nombre d'agents User-ID à gérer. Lorsque vous configurez le transfert des journaux Windows, les différents contrôleurs de domaines exportent leurs événements de connexion vers un seul membre à partir duquel un agent User-ID collecte les informations de mappage d'utilisateur.

***Vous pouvez configurer le transfert des journaux Windows pour Windows Server versions 2012 et 2012 R2. Le transfert des journaux Windows n'est pas possible pour les serveurs non Microsoft.***

Pour collecter des informations de mappage de groupe dans un réseau à grande échelle, vous pouvez configurer le pare-feu pour interroger un serveur de catalogues global qui reçoit des informations de compte des contrôleurs de domaines.

La figure ci-dessous illustre le mappage d'utilisateur et le mappage de groupe pour un réseau à grande échelle dans lequel le pare-feu utilise un agent User-ID basé sur Windows. Reportez-vous à la section Planification d'un déploiement User-ID à grande échelle pour savoir si ce déploiement est adapté à votre réseau.




## Planification d'un déploiement User-ID à grande échelle

Lors de la décision d'utiliser le transfert des journaux Windows ou les serveurs de catalogues globaux pour votre mise en œuvre de User-ID, contactez votre administrateur système pour déterminer ce qui suit :

- Bande passante nécessaire aux contrôleurs de domaines pour transférer des événements de connexion aux serveurs membres. La bande passante est un multiple du taux de connexion (nombre de connexions par minute) des contrôleurs de domaines à la taille en octet de chaque événement de connexion.

  Les contrôleurs de domaine ne transmettent pas l'intégralité de leurs journaux de sécurité, mais uniquement les événements dont le processus de mappage des utilisateurs a besoin par connexion : quatre événements pour Windows Server 2012 et MS Exchange.

- ☐ Si les éléments réseau suivants prennent en charge la bande passante requise :
  - **Contrôleurs de domaines** : doit prendre en charge la charge de traitement associée à la transmission des événements.
  - **Serveurs membres** : doit prendre en charge la charge de traitement associée à la réception des événements.
  - **Connexions** : la répartition géographique (local ou à distance) des contrôleurs de domaines, serveurs membres et serveurs de catalogues globaux est un facteur. Une distribution à distance prend généralement en charge moins de bande passante.

## Configuration du transfert des journaux Windows

Pour configurer le transfert des journaux Windows, vous devez disposer de droits administratifs pour la configuration de politiques de groupe sur des serveurs Windows. Configurez le transfert des journaux Windows sur tous les ***collecteurs d'événements Windows***—les serveurs membres qui collectent des événements de connexion auprès des contrôleurs de domaines. Vous trouverez ci-dessous une présentation des tâches ; consultez la documentation de votre serveur Windows pour les étapes spécifiques.

**STEP 1 |** Sur chaque collecteur d'événements Windows, activez la collecte d'événement, ajoutez les contrôleurs de domaines en tant que sources d'événements, et configurez la requête de collecte d'événement (abonnement). Les événements que vous indiquez dans l'abonnement varient en fonction de la plate-forme du contrôleur de domaine :

- **Windows Server 2012 (R2 inclus) et 2016 ou MS Exchange** : les ID d'événement des événements requis sont 4768 (ticket d'authentification émis), 4769 (ticket de service émis), 4770 (ticket émis renouvelé) et 4624 (connexion réussie).

*Pour transférer le plus rapidement possible des événements, **Minimize Latency (Réduisez la latence)** lors de la configuration de l'abonnement.*

Les agents User-ID surveillent le journal de Sécurité, et non pas l'emplacement des événements transmis par défaut, sur les collecteurs d'événements Windows. Ainsi, vous devriez effectuer les étapes suivantes sur chaque collecteur d'événements Windows pour modifier le chemin de journalisation des événements vers le journal de sécurité.

1. Ouvrez l'Observateur d'événements.
2. Faites un clic droit sur le journal **Security (de Sécurité)** et sélectionnez **Properties (Propriétés)**.
3. Copiez le **Log path (Chemin du journal)** (par défaut **`%SystemRoot%\System32\Winevt\Logs\security.evtx`**), puis cliquez sur **OK**.
4. Faites un clic droit sur le dossier **Forwarded Events (Événements transférés)** et sélectionnez **Properties (Propriétés)**.
5. Remplacez le **Log path (Chemin du journal)** par défaut (**`%SystemRoot%\System32\Winevt\Logs\ForwardedEvents.evtx`**) en collant la valeur du journal de **Security (Sécurité)**, puis cliquez sur **OK**.

**STEP 2 |** Configurez une politique de groupe pour activer Windows Remote Management (WinRM) sur les contrôleurs de domaines.

**STEP 3 |** Configurez une politique de groupe pour activer le transfert des journaux Windows sur les contrôleurs de domaines.

## Configuration de User-ID pour de nombreuses sources d'informations de mappage

**STEP 1 |** Configurez le transfert des journaux Windows sur les serveurs membres qui collecteront des événements de connexion.

Configuration du transfert des journaux Windows. Cette étape requiert des droits administratifs pour la configuration de politiques de groupe sur des serveurs Windows.

**STEP 2 |** Installez l'agent User-ID basé sur Windows.

Procédez à l'installation de l'agent User-ID basé sur Windows sur un serveur Windows qui peut accéder aux serveurs membres. Assurez-vous que le système qui hébergera l'agent User-ID est membre du même domaine que les serveurs qu'il surveillera.

**STEP 3 |** Configurez l'agent User-ID pour collecter des informations de mappage d'utilisateur sur les serveurs membres.

1. Démarrez l'agent User-ID basé sur Windows.
2. Sélectionnez **User Identification (Identification utilisateur)** > **Discovery (Détection)** et effectuez les étapes suivantes pour chaque serveur membre qui recevra des événements des contrôleurs de domaines :
   1. Dans la section Servers (Serveurs), cliquez sur **Add (Ajouter)** et saisissez un **Name (Nom)** pour identifier le serveur membre.
   2. Dans le champ **Server Address (Adresse du serveur)**, saisissez le FQDN ou l'adresse IP du serveur membre.
   3. Pour le **Server Type (Type de serveur)**, sélectionnez **Microsoft Active Directory (Microsoft Active Directory)**.
   4. Cliquez sur **OK (OK)** pour enregistrer l'entrée du serveur.
3. Configurez les derniers paramètres de l'agent User-ID : reportez-vous à la section Configuration de l'agent User-ID Windows pour le mappage d'utilisateur.
4. Si les sources User-ID fournissent des noms d'utilisateur en plusieurs formats, spécifiez le formation du **Primary Username (Nom d'utilisateur principal)** lorsque vous Mappage d'utilisateurs à des groupes.

   Le nom d'utilisateur principal est le nom d'utilisateur qui identifie l'utilisateur sur le pare-feu et représente l'utilisateur dans les rapports et les journaux, peu importe le formation que la source User-ID fournit.

**STEP 4 |** Configurez un profil de serveur LDAP pour préciser comment le pare-feu se connecte aux serveurs de catalogues globaux (jusqu'à quatre) pour obtenir les informations de mappage de groupe.

*Pour améliorer la disponibilité, utilisez deux serveurs de catalogues globaux minimum pour la redondance.*

Vous ne pouvez collecter des informations de mappage de groupe que pour des groupes universels, et non des groupes de domaines locaux (sous-domaines).

1. Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveur)** > **LDAP (LDAP)**, cliquez sur **Add (Ajouter)** et saisissez un **Name (Nom)** pour le profil.
2. Dans la section Servers (Serveurs), pour chaque catalogue global, cliquez sur **Add (Ajouter)** et saisissez le **Name (Nom)** de serveur, l'adresse IP (**LDAP Server (Serveur LDAP)**), ainsi que le **Port (Port)**. Pour une connexion en texte brut ou Start Transport Layer Security (Start TLS), utilisez le **Port (Port)** 3268. Pour une connexion LDAP sur SSL, utilisez le **Port (Port)** 3269. Si la connexion doit utiliser Start TLS ou LDAP sur SSL, cochez la case **Require SSL/TLS secured connection (Exiger une connexion sécurisée SSL/TLS)**.
3. Dans le champ **Base DN (DN de base)**, sélectionnez le Distinguished Name (nom unique - DN) du point du serveur de catalogues global à partir duquel le pare-feu commencera sa recherche d'informations de mappage de groupe (par exemple, `DC=acbdomain,DC=com`).
4. Pour le **Type (Type)**, sélectionnez **active-directory (Active Directory)**.

**STEP 5 |** Configurez un profil de serveur LDAP pour préciser comment le pare-feu se connecte aux serveurs (jusqu'à quatre) contenant les informations de mappage de domaine.

User-ID utilise ces informations pour mapper les noms de domaines DNS aux noms de domaines NetBIOS. Ce mappage garantit des références domaine/nom d'utilisateur cohérentes dans les règles de politique.

*Pour améliorer la disponibilité, utilisez deux serveurs minimum pour la redondance.*

Les étapes sont identiques à celles du profil de serveur LDAP que vous avez créé pour les catalogues globaux à l'étape précédente, à l'exception des champs suivants :

- **LDAP Server (Serveur LDAP)** : saisissez l'adresse IP du contrôleur de domaine contenant les informations de mappage de domaine.
- **Port (Port)** : pour une connexion en texte brut ou Start TLS, utilisez le **Port (Port)** 389. Pour une connexion LDAP sur SSL, utilisez le **Port** 636. Si la connexion doit utiliser Start TLS ou LDAP sur SSL, cochez la case **Require SSL/TLS secured connection (Exiger une connexion sécurisée SSL/TLS)**.
- **Base DN (DN de base)** : sélectionnez le DN du point du contrôleur de domaine à partir duquel le pare-feu commencera sa recherche d'informations de mappage de domaine. La valeur doit commencer par la chaîne suivante : `cn=partitions,cn=configuration` (par exemple, `cn=partitions,cn=configuration,DC=acbdomain,DC=com`).

**STEP 6 |** Créez une configuration de mappage de groupe pour chaque profil de serveur LDAP que vous avez créé.

1. Sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Group Mapping Settings (Paramètres de mappage de groupe)**.
2. Cliquez sur **Add (Ajouter)** et saisissez un **Name (Nom)** pour identifier la configuration de mappage de groupe.
3. Sélectionnez un **Server Profile (Profil de serveur)** LDAP et vérifiez que la case **Enabled (Activé)** est cochée.

   *Si les serveurs de catalogues globaux et de mappage de domaine font référence à plus de groupes que ceux requis par vos règles de sécurité, configurez la liste **Group Include List (Liste d'inclusion de groupes)** et/ou la liste **Custom Group (Groupe personnalisé)** pour limiter les groupes pour lesquels User-ID procède au mappage.*
4. Cliquez sur **OK**, puis sur **Commit (Valider)**.

## Insertion du nom d'utilisateur dans les en-têtes HTTP

Lorsque vous configurez un appareil d'application secondaire avec votre pare-feu Palo Alto Networks pour appliquer la politique basée sur les utilisateurs, l'appareil secondaire pourrait ne pas avoir le mappage nom d'utilisateur/adresse IP du pare-feu. Pour transmettre les renseignements de l'utilisateur à des appareils en aval, vous pourriez avoir besoin de déployer des appareils supplémentaires, comme des proxys. De plus la transmission pourrait nuire à l'expérience utilisateur (par exemple, les utilisateurs pourraient être forcés de se connecter à plusieurs reprises). En partageant l'identité de l'utilisateur dans les en-têtes HTTP, vous pouvez appliquer la politique basée sur les utilisateurs sans compromettre l'expérience utilisateur ou déployer une infrastructure supplémentaire.

Lorsque vous configurez cette fonction, appliquez le profil d'URL à votre politique de sécurité et validez vos modifications, le pare-feu :

1. Charge les valeurs liées à l'utilisateur et au domaine en respectant le format du nom d'utilisateur principal dans le mappage de groupe de l'utilisateur source.
2. Encode cette information à l'aide de Base64.
3. Ajoute l'en-tête codé en Base64 à la charge utile.
4. Achemine le trafic vers l'appareil en aval.

Si vous souhaitez inclure le nom d'utilisateur et le domaine uniquement lorsque l'utilisateur accède aux domaines spécifiques, configurez une liste de domaines, et le pare-feu insère l'en-tête uniquement lorsqu'un domaine de la liste correspond à l'en-tête de l'hôte de la requête HTTP.

Pour partager les informations utilisateur avec des appareils en aval, vous devez d'abord enable (activer) User-ID et configurer le mappage de groupe.

*Pour inclure le nom d'utilisateur et le domaine dans l'en-tête, le pare-feu exige le mappage nom d'utilisateur/adresse IP de l'utilisateur. Si l'utilisateur n'est pas mappé,le pare-feu insère `unknown` en codage Base64 pour le nom d'utilisateur et le domaine contenus dans l'en-tête.*

Pour inclure le nom d'utilisateur et le domaine dans les en-têtes du trafic HTTP, vous devez d'abord créer un profil de déchiffrement pour déchiffrer le profil HTTPS.

*Cet fonctionnalité prend en charge le trafic de déchiffrement du transfert de proxy.*

**STEP 1 |** Create (Créez) ou modifiez un **URL Filtering Profile (Profil de filtrage des URL)**.

*Le pare-feu n'insère pas d'en-têtes si l'action prise à l'égard du profil de filtrage des URL est définie sur* ***block*** *(bloquer) pour le domaine.*

**STEP 2 |** Créez ou modifiez une entrée d'insertion d'en-têtes HTTP à l'aide de types prédéfinis.

Vous pouvez définir jusqu'à cinq en-têtes pour chaque profil.

**STEP 3 |** Sélectionnez **Dynamic Fields (Champs dynamiques)** comme **Type** d'en-tête.

**STEP 4 |** **Add (Ajoutez)** les **Domains (Domaines)** pour lesquels vous insérerez des en-têtes. Lorsque l'utilisateur accès à un domaine de la liste, le pare-feu insère l'en-tête spécifié.

**STEP 5 |** **Add (Ajoutez)** un nouveau **Header (En-tête)** ou sélectionnez **X-Authenticated-User** pour le modifier.

**STEP 6 |** Sélectionnez un format de **Value (valeur)** (soit **`($domain)\($user)`** ou **`WinNT://($domain)/($user)`**) ou saisissez votre propre format au moyen des jetons dynamiques **`($domain)`** et **`($user)`** (par exemple, **`($user)@($domain)`** pour UserPrincipalName).

*N'utilisez pas le même jeton dynamique (**`($user)`** ou **`($domain)`**) plus d'une fois par valeur.*

Chaque valeur peut comporter un maximum de 512 caractères. Le pare-feu remplit les jetons dynamiques de l'utilisateur **`($user)`** et du domaine **`($domain)`** en utilisant le nom d'utilisateur principal dans le profil de mappage de groupe. Par exemple :

- Si le nom d'utilisateur principal est le sAMAccountName, la valeur de **`($user)`** est le sAMAccountName est la valeur de **`($domain)`** est le nom de domaine NetBios.
- Si le nom d'utilisateur principal est le UserPrincipalName, **`($user)`** est le nom de compte de l'utilisateur (préfixe) et **`($domain)`** est le nom du Domain Name System (système de noms de domaine ; DNS).

**STEP 7 |** (Facultatif) Sélectionnez **Log (Journal)** pour activer la journalisation de l'insertion d'en-têtes.

**STEP 8 |** Appliquez le profil de filtrage des URL à la ou aux règles de politique de sécurité qui autorisent le trafic HTTP ou HTTPS.

**STEP 9 |** Sélectionnez **OK** deux fois pour confirmer la configuration d'en-têtes HTTP.

**STEP 10 |** **Commit (Validez)** vos modifications.

**STEP 11 |** Vérifiez que le pare-feu inclut le nom d'utilisateur et le domaine dans les en-têtes HTTP.

- Utilisez la commande **`show user user-ids all`** pour vérifier que le mappage de groupe est correct.
- Utilisez la commande **`show counter global name ctd_header_insert`** pour afficher le nombre d'en-têtes HTTP qui ont été insérés par le pare-feu.
- Si vous avez configuré la journalisation à l'étape 7, vérifiez les journaux de la charge utile codée Base64 qui a été insérée (par exemple, **`corpexample\testuser`** qui apparaît dans le journal sous le nom de **`Y29ycGV4YW1wbGVcdGVzdHVzZXI=`**).

# Redistribution des données et horodatages d'authentification

Sur des réseaux de grande envergure, vous pouvez optimiser l'utilisation des ressources en configurant quelques pare-feux pour qu'ils recueillent des données grâce à la redistribution, au lieu de configurer tous vos pare-feux pour qu'ils fassent des requêtes directes auprès des sources de données de mappage.

*Vous pouvez redistribuer les informations de mappage d'utilisateur recueillies à l'aide de n'importe quelle méthode, à l'exception des agents Terminal Server (TS). Vous ne pouvez pas redistribuer les informations de* Mappage de groupe *ou de* Correspondance HIP*.*

*Si vous utilisez Panorama pour gérer des pare-feux ou rassembler des journaux de pare-feux, vous pouvez utiliser Panorama pour* manage User-ID redistribution (Gérer la redistribution de User-ID)*. Tirer parti de Panorama est une solution plus simple que de créer des connexions supplémentaires entre les pare-feux pour redistribuer les informations d'ID utilisateur.*

Pour Configurer la politique d'authentification, vos pare-feux doivent également redistribuer les Horodatages d'authentification générés quand les utilisateurs s'authentifient pour accéder aux applications et services. Les pare-feux utilisent les horodatages pour évaluer les délais d'expiration des Règles de politiques d'authentification. Les délais d'expiration permettent à l'utilisateur qui s'authentifie avec succès de faire des requêtes ultérieures de services ou d'applications sans avoir à s'authentifier à nouveau avant le délai d'expiration. Redistribuer les horodatages vous permet d'instaurer des délais d'expiration cohérents sur tous les pare-feux de votre réseau.

Les pare-feux partagent les données et les horodatages d'authentification dans le cadre d'un même flux de redistribution ; vous n'avez pas à configurer de redistribution pour chaque type d'information séparément.

- Déploiement du pare-feu pour la redistribution des données
- Configuration de la redistribution des données

## Déploiement du pare-feu pour la redistribution des données

Dans un réseau à grande échelle, au lieu de configurer tous vos pare-feu pour interroger directement les sources de données, vous pouvez rationaliser l'utilisation des ressources en configurant certains pare-feu pour collecter les données par redistribution. La redistribution des données offre également une granularité, vous permettant de redistribuer uniquement les types d'informations que vous spécifiez aux seuls périphériques que vous sélectionnez. Vous pouvez également filtrer les mappages

des utilisateurs IP ou les mappages des étiquettes IP à l'aide de sous-réseaux et de plages afin de garantir que les pare-feu ne collectent que les mappages dont ils ont besoin pour appliquer la politique.

La redistribution des données peut être unidirectionnelle (l'agent fournit les données au client) ou bidirectionnelle, où l'agent et le client peuvent simultanément envoyer et recevoir des données.

Pour redistribuer les données, vous pouvez utiliser les types d'architecture suivants :

- **Architecture en étoile pour une seule région :**

  Pour redistribuer les données entre les pare-feu, la meilleure pratique consiste à utiliser une architecture en étoile. Dans cette configuration, un pare-feu concentrateur collecte les données à partir de sources telles que les agents Windows User-ID, les serveurs Syslog, les contrôleurs de domaine ou d'autres pare-feu. Configurez les pare-feu clients de redistribution pour qu'ils collectent les données du pare-feu concentrateur.

  Par exemple, un concentrateur (composé d'une paire de VM-50 pour la résilience) pourrait se connecter aux sources d'identification des utilisateurs pour les mappages des utilisateurs. Le concentrateur serait alors en mesure de redistribuer les mappages des utilisateurs lorsque les pare-feu clients qui utilisent les mappages des utilisateurs pour appliquer la politique se connectent au concentrateur pour recevoir des données.
- **Architecture en étoile à plusieurs concentrateurs pour plusieurs régions :**

  Si vous avez des pare-feu déployés dans plusieurs régions et que vous souhaitez distribuer les données aux pare-feu de toutes ces régions afin de pouvoir appliquer la politique de manière cohérente quel que soit l'endroit où l'utilisateur se connecte, vous pouvez utiliser une architecture en étoile à plusieurs concentrateurs pour plusieurs régions.

  Commencez par configurer un pare-feu dans chaque région pour collecter les données à partir des sources. Ce pare-feu agit comme un concentrateur local pour la redistribution. Ce pare-feu collecte les données de toutes les sources dans cette région afin de pouvoir les redistribuer aux pare-feu clients. Ensuite, configurez les pare-feu clients pour qu'ils se connectent aux concentrateurs de redistribution de leur région et de toutes les autres régions afin que les pare-feu clients disposent de toutes les données de tous les concentrateurs.

  Comme meilleure pratique, autorisez une redistribution bidirectionnelle au sein d'une région si les pare-feu doivent à la fois envoyer et recevoir des données. Par exemple, si un pare-feu agit comme une passerelle GlobalProtect pour les utilisateurs distants et comme un pare-feu de branche pour les utilisateurs locaux, le pare-feu doit envoyer les mappages d'utilisateurs qu'il collecte pour les utilisateurs distants au pare-feu concentrateur ainsi que recevoir les mappages d'utilisateurs des utilisateurs locaux du pare-feu concentrateur.
- **Architecture hiérarchique :**

  Pour redistribuer les données, vous pouvez également utiliser une architecture hiérarchique. Par exemple, pour redistribuer des données telles que les informations d'identification de l'utilisateur, organiser la séquence de redistribution en couches, où chaque couche a un ou plusieurs pare-feu. Dans la couche du bas, les agents User-ID intégrés à PAN-OS s'exécutant sur les pare-feu et les agents User-ID Windows s'exécutant sur les serveurs Windows mappent les adresses IP et les noms d'utilisateur. Dans chacune des couches supérieures se trouvent les pare-feu qui reçoivent les informations de mappage et les horodatages d'authentification d'un maximum de 100 points de redistribution situés dans la couche inférieure. Les pare-feu de la couche supérieure regroupent les informations et les horodatages de toutes les couches. Ce déploiement offre la possibilité de configurer des politiques applicables à tous les utilisateurs des pare-feu de

la couche supérieure ainsi que des politiques propres à une fonction ou à une région applicables à un sous-ensemble d'utilisateurs se trouvant dans les domaines correspondants desservis par les pare-feu des couches inférieures.

Dans ce scénario, trois couches de pare-feu redistribuent les mappages et les horodatages des bureaux locaux vers les bureaux régionaux, puis vers un centre de données mondial. Le pare-feu du centre de données qui recueille l'ensemble des informations communique ces informations aux autres pare-feu du centre de données pour qu'ils puissent tous appliquer la politique et générer des rapports pour les utilisateurs de l'ensemble de votre réseau. Seuls les pare-feu de la couche inférieure utilisent les agents User-ID pour interroger les serveurs d'annuaire.

Les sources d'informations que les agents User-ID interrogent ne sont pas prises en compte dans les dix ***sauts*** maximum de la séquence. Cependant, les agents User-ID Windows qui transmettent des informations de mappage aux pare-feu sont pris en compte. De même, dans cet exemple, la couche supérieure dispose de deux sauts : le premier sert à regrouper les informations dans un pare-feu du centre de données et le second, à communiquer les informations aux autres pare-feu du centre de données.

## Configuration de la redistribution des données

Avant de configurer la redistribution des données :

- ☐ Planifiez l'architecture de redistribution. Voici certains facteurs à prendre en compte :
  - Quels sont les pare-feu qui mettront en œuvre les politiques qui concernent l'ensemble des types de données et quels sont les pare-feu qui mettront en œuvre les politiques propres à une fonction ou à une région qui ne touchent qu'un sous-ensemble de données ?
  - Combien de sauts la séquence de redistribution doit-elle prévoir pour grouper toutes les données ? Le nombre maximum de sauts autorisés pour les mappages d'utilisateurs est de dix et le nombre maximum de sauts autorisés pour les mappages nom d’utilisateur/adresse IP et les mappages étiquette/adresse IP est de un.
  - De quelle façon pouvez-vous minimiser le nombre de pare-feu qui interrogent les sources d'informations de mappage d'utilisateur ? Plus le nombre de pare-feu qui interrogent les sources d'informations est faible, plus la charge de traitement exercée sur les pare-feu et les sources est réduite.
- ☐ Configurez les sources de données à partir desquelles vos agents de redistribution obtiennent les données à redistribuer à leurs clients :
  - mappages d'utilisateur à partir des agents User-ID intégrés à PAN-OS ou des agents User-ID basés sur Windows.
  - mappages étiquette/adresse IP pour les dynamic address groups (groupes d’adresses dynamiques)
  - mappages étiquette/nom d'utilisateur pour les dynamic user groups (groupes d’utilisateurs dynamiques)
  - GlobalProtect pour la HIP-based Policy Enforcement (Mise en œuvre de la politique basée sur HIP)
  - données pour la quarantaine du périphérique (Panorama uniquement)
- ☐ Configuration de la politique d'authentification.

La redistribution des données se compose de :

- L'agent de redistribution qui fournit les informations
- Le client de redistribution qui reçoit les informations

Sur le pare-feu, effectuez les étapes suivantes en respectant la séquence de distribution des données.

**STEP 1 |** Sur un pare-feu client de redistribution, configurez un pare-feu, un agent Panorama ou Windows User-ID comme agent de redistribution des données.

1. Sélectionnez **Device (Périphérique)** > **Data Redistribution (Redistribution des données)** > **Agents**.
2. **Add (Ajoutez)** un agent de redistribution et saisissez un **Name (Nom)**.
3. Confirmez que l'agent est **Enabled (Activé)**.

**STEP 2 |** Ajoutez l'agent à l'aide de son **Serial Number (numéro de série)** ou de son **Host and Port (Hôte et port)**.

- Pour ajouter un agent utilisant un numéro de série, sélectionnez le **Serial Number (numéro de série)** du pare-feu que vous souhaitez utiliser comme agent de redistribution.
- Pour ajouter un agent en utilisant ses informations d'hôte et de port :

  1. Saisissez les informations pour l'**Host (Hôte)**.
  2. Indiquez si l'hôte est un **LDAP Proxy**.
  3. Saisissez le **Port** (de 1 à 65535, la valeur par défaut est 5007).
  4. (Systèmes virtuels multiples uniquement) Saisissez le **Collector Name (Nom du collecteur)** pour identifier le système virtuel que vous souhaitez utiliser comme agent de redistribution.
  5. (Systèmes virtuels multiples uniquement) Saisissez et confirmez la **Collector Pre-Shared Key (Clef pré-partagée du collecteur)** pour le système virtuel que vous souhaitez utiliser comme agent de redistribution.

**STEP 3 |** Sélectionnez un ou plusieurs **Data Type (Type de données)** que l'agent doit redistribuer.

- **IP User Mappings (Mappages d'utilisateur IP)** : mappages nom d'utilisateur/adresse IP pour User-ID.
- **IP Tags (Étiquettes IP)** : mappages étiquette/adresse IP pour les groupes d'adresses dynamiques.
- **User Tags (Étiquettes utilisateur)** : mappages étiquette/nom d'utilisateur pour les groupes d'utilisateurs dynamiques.
- **HIP** : données du profil d'informations sur l'hôte (HIP) de GlobalProtect, qui comprennent les objets et les profils HIP.
- **Quarantine List (Liste de quarantaine)** : périphériques que GlobalProtect identifie comme étant en quarantaine.

**STEP 4 |** (Systèmes virtuels multiples uniquement) Configurez un système virtuel comme un collecteur qui peut redistribuer des données.

Sautez cette étape si le pare-feu reçoit les données sans les redistribuer.

*Vous pouvez redistribuer les informations entre les systèmes virtuels de pare-feu différents ou du même pare-feu. Dans les deux cas, chaque système virtuel représente un saut de la séquence de redistribution.*

1. Sélectionnez **Device (Périphérique)** > **Data Redistribution (Redistribution des données)** > **Collector Settings (Paramètres du collecteur)**.
2. Modifiez la **Data Redistribution Agent Setup (Configuration de l'agent de redistribution des données)**.
3. Saisissez un **Collector Name (Nom du collecteur)** et une **Pre-Shared Key (Clé prépartagée)** pour identifier ce pare-feu ou ce système virtuel en tant qu'agent User-ID.
4. Cliquez sur **OK** pour enregistrer vos modifications.

**STEP 5 |** (Facultatif mais recommandé) Configurez les réseaux que vous souhaitez inclure dans la redistribution des données et ceux que vous souhaitez exclure de la redistribution des données.

Vous pouvez inclure ou exclure des réseaux et des sous-réseaux lors de la redistribution des mappages étiquette/adresse IP ou nom d'utilisateur/adresse IP.

*Il est recommandé de toujours spécifier les réseaux à inclure et à exclure pour garantir que l'agent ne communique qu'avec les ressources internes.*

1. Sélectionnez **Device (Périphérique)** > **Data Redistribution (Redistribution des données)** > **Include/Exclude Networks (Inclure/Exclure des réseaux)**.
2. **Add (ajoutez)** une entrée et saisissez un **Name (Nom)**.
3. Vérifiez que l'entrée est **Enabled (Activée)**.
4. Indiquez si vous voulez **Include (Inclure)** ou **Exclude (Exclure)** l'entrée.
5. Saisissez la **Network Address (Adresse réseau)** pour l'entrée.
6. Cliquez sur **OK**.

**STEP 6 |** Configurez l'itinéraire de service que le pare-feu utilise pour interroger d'autres pare-feu pour recueillir des informations de User-ID.

Sautez cette étape si le pare-feu reçoit uniquement les informations de mappage des agents User-ID Windows ou directement des sources d'information (comme les serveurs d'annuaires) plutôt que des autres pare-feu.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Services**
2. (**Pare-feu comportant des systèmes virtuels multiples uniquement**) Sélectionnez **Global (Global)** (pour configurer un itinéraire de service devant servir à l'ensemble des pare-feu) ou **Virtual Systems (Systèmes virtuels)** (pour configurer un itinéraire de service propre aux systèmes virtuels), puis configurez l'itinéraire de service.
3. Cliquez sur **Service Route Configuration (Configuration des itinéraires de service)**, sélectionnez **Customize (Personnaliser)**, puis sélectionnez **IPv4 (IPv4)** ou **IPv6 (IPv6)**,

selon les protocoles de votre réseau. Si votre réseau utilise les deux protocoles, configurez l'itinéraire de service pour les deux.

4. Sélectionnez **UID Agent (Agent UID)**, puis sélectionnez la **Source Interface (Interface source)** et la **Source Address (Adresse source)**.
5. Cliquez deux fois sur **OK (OK)** pour enregistrer l'itinéraire de service.

**STEP 7 |** Activez le pare-feu pour qu'il réponde lorsque les autres pare-feu l'interrogent à propos des données à redistribuer.

Sautez cette étape si le pare-feu reçoit les données sans les redistribuer.

Configurez un profil de gestion d'interface pour lequel le service **User-ID (User-ID)** est activé et affectez le profil à une interface du pare-feu.

**STEP 8 |** (Facultatif mais recommandé) Utilisez un certificat personnalisé de la PKI de votre entreprise pour établir une chaîne de confiance unique du client de redistribution à l'agent de redistribution.

1. Sur le pare-feu du client de redistribution, créez un SSL certificate profile (profil de certificat SSL) personnalisé à utiliser pour les connexions sortantes.
2. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **Secure Communication Settings (Paramètres de communication sécurisée)**.
3. **Edit (Modifiez)** les paramètres.
4. Sélectionnez l'option **Customize Secure Server Communication (Personnaliser la communication sécurisée avec le serveur)**.
5. Sélectionnez le **Certificate Profile (Profil de certificat)** que vous avez créé à la sous-étape 1.
6. Cliquez sur **OK**.
7. **Customize Communication (Personnalisez la communication)** pour la **Data Redistribution (Redistribution des données)**.
8. **Commit (Validez)** vos modifications.
9. Entrez la commande CLI suivante pour confirmer que le profil du certificat (`SSL config`) utilise des `Custom certificates (Certificats personnalisés)` : **`show redistribution agent state <agent-name>`** (où *<agent-name>* est le nom de l'agent de redistribution ou de l'agent User-ID.

**STEP 9 |** (Facultatif mais recommandé) Utilisez un certificat personnalisé de la PKI de votre entreprise pour établir une chaîne de confiance unique de l'agent de redistribution au client de redistribution.

1. Sur le pare-feu de l'agent de redistribution, créez un SSL/TLS service profile (Profil de service SSL/TLS) personnalisé que le pare-feu utilisera pour les connexions entrantes.
2. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **Secure Communication Settings (Paramètres de communication sécurisée)**.
3. **Edit (Modifiez)** les paramètres.
4. Sélectionnez l'option **Customize Secure Server Communication (Personnaliser la communication sécurisée avec le serveur)**.
5. Sélectionnez le **SSL/TLS Service Profile (Profil de service SSL/TLS)** que vous avez créé à l'étape 1.
6. Cliquez sur **OK**.
7. **Commit (Validez)** vos modifications.
8. Entrez la commande CLI suivante pour confirmer que le profil de certificat (`SSL config`) utilise des `Custom certificates (Certificats personnalisés)` : **`show redistribution service status`**.

**STEP 10 |** Vérifiez que les agents redistribuent correctement les données aux clients.

1. Affichez les statistiques de l'agent (**Device (Périphérique)** > **Data Redistribution (Redistribution des données)** > **Agents** et sélectionnez **Status (État)** pour afficher un résumé de l'activité de l'agent de redistribution, comme le nombre de mappages que le pare-feu client a reçu.
2. Confirmez que l'état **Connected (Connecté)** est **yes (oui)**.
3. Sur l'agent, access the CLI (accédez à la CLI) et saisissez la commande CLI suivante pour vérifier l'état de la redistribution : **`show redistribution service status`**.
4. Sur l'agent, saisissez la commande CLI suivante pour afficher les clients de redistribution : **`show redistribution service client all`**.
5. Sur le client, saisissez la commande CLI suivante pour vérifier l'état de la redistribution: **`show redistribution service client all`**.
6. Confirmez que le **Source Name (Nom de la source)** dans les journaux User-ID (**Monitor** > **Logs** > **User-ID** Surveiller les journaux User-ID) pour vérifier que le pare-feu reçoit les mappages des agents de redistribution.
7. Sur le client, affichez le journal d'indicateur d'adresse IP (**Monitor (Moniteur)** > **Logs (Journaux)** > **IP-Tag (IP-étiquette)**) pour confirmer que le pare-feu client reçoit des données.
8. Sur le client, saisissez la commande CLI suivante et vérifiez que la source `From (De)` laquelle pare-feu reçoit les mappages est `REDIST` : **`show user ip-user-mapping all`**.

**STEP 11 |** (Facultatif) Pour résoudre les problèmes de redistribution des données, activez l'option traceroute.

Lorsque vous activez l'option traceroute, le pare-feu qui reçoit les données ajoute son adresse IP au champ `<route>`, qui est une liste de toutes les adresses IP du pare-feu que les données ont traversées. Cette option exige que tous les dispositifs PAN-OS dans la voie de redistribution

utilisent la version 10.0 de PAN-OS. Si un périphérique PAN-OS dans la route de redistribution utilise PAN-OS 9.1.x ou des versions antérieures, les informations de traceroute se terminent à ce périphérique.

1. Sur l'agent de redistribution d'où provient la source, saisissez la commande CLI suivante : **debug user-id test cp-login traceroute yes ip-address *<ip-address>* user *<username>*** (où ***<ip-address>*** est l'adresse IP du mappage nom d'utilisateur/adresse IP à vérifier et ***<username>*** est le nom d'utilisateur du mappage nom d'utilisateur/adresse IP à vérifier.
2. Sur un client du pare-feu où vous avez configuré le traceroute, vérifiez que le pare-feu redistribue les données en saisissant la commande CLI suivante : **show user ip-user-mapping all**.

   Le pare-feu affiche l'horodatage de la création du mappage (`SeqNumber`) et si l'utilisateur possède GlobalProtect (`GP User`).

```
admin > show user ip-user-mapping-mp ip 192.0.2.0

IP address:  192.0.2.0 (vsys1)
User:    jimdoe
From:   REDIST
Timeout:  889s
Created:  11s ago
Origin:   198.51.100.0
SeqNumber:  15895329682-67831262
GP User:  No
Local HIP:  No
Route Node 0: 198.51.100.0 (vsys1)
Route Node 1: 198.51.100.1 (vsys1)
```

## Partage des mappages User-ID sur l'ensemble des systèmes virtuels

Pour simplifier la configuration de la source User-ID™ lorsque vous disposez de plusieurs systèmes virtuels, configurez les sources User-ID sur un seul virtual system (système virtuel) pour le partage des mappages adresse IP vers nom d'utilisateur et les mappages nom d'utilisateur vers groupe avec tous les autres systèmes virtuels sur le pare-feu.

La configuration d'un seul système virtuel en tant que ***User-ID hub (pôle User-ID)*** simplifie le mappage d'utilisateur en éliminant la nécessité de configurer les sources sur plusieurs systèmes virtuels, particulièrement si le trafic passera par plusieurs systèmes virtuels en fonction des ressources auxquelles l'utilisateur cherche à accéder (par exemple, dans un environnement de réseautage universitaire où un étudiant accédera à divers départements dont le trafic est géré par différents systèmes virtuels).

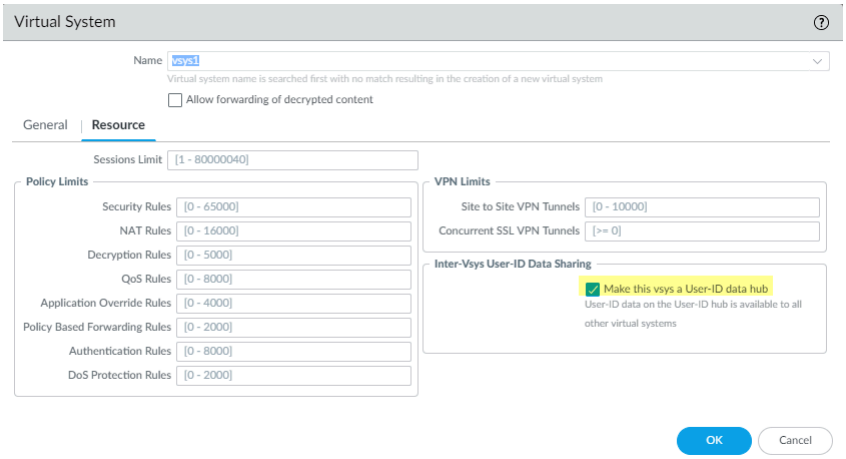
Pour mapper l'utilisateur ou le groupe, le pare-feu utilise le tableau de mappage sur le système virtuel local et applique la politique de cet utilisateur ou de ce groupe. Si le pare-feu ne trouve pas le mappage d'un utilisateur ou groupe sur le système virtuel d'où le trafic de l'utilisateur provient, le pare-feu interroge le pôle pour extraire les informations de mappage adresse IP/nom d'utilisateur de cet utilisateur ou les informations de mappage de groupe pour ce groupe. Si le pare-feu trouve le mappage sur le pôle User-ID et le système virtuel local, le pare-feu utilise le mappage dont il prend connaissance localement. Si le mappage sur le pare-feu local diffère du mappage sur le pôle de système virtuel, le pare-feu utilise le mappage local.

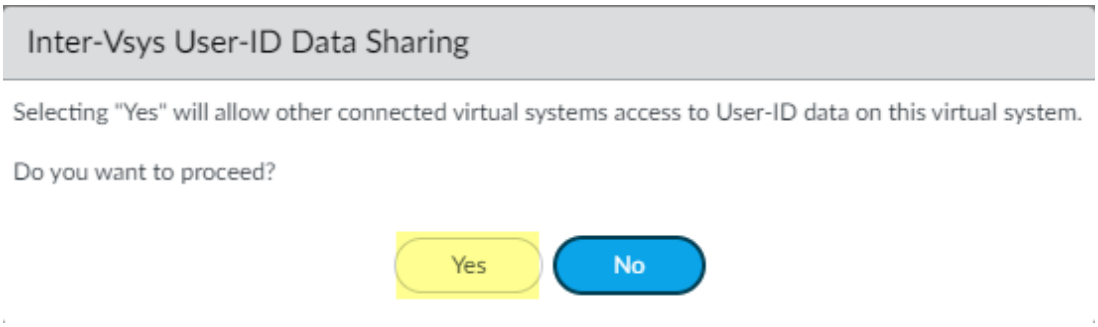
Après avoir configuré le pôle User-ID, le système virtuel peut utiliser la table de mappage du pôle User-ID lorsqu'il a besoin d'identifier un utilisateur pour l'application de la politique basée sur l'utilisateur ou d'afficher le nom d'utilisateur dans un journal ou un rapport, mais que la source n'est pas disponible localement. Lorsque vous sélectionnez un pôle, le pare-feu conserve les mappages sur d'autres systèmes virtuels. Nous recommandons donc de consolider les sources User-ID sur le hub. Cependant, si vous ne voulez pas partager les mappages d'une source donnée, vous pouvez configurer un système virtuel pour qu'il effectue le mappage d'utilisateur ou groupe.

**STEP 1 |** Affectez le système virtuel en tant que pôle User-ID.

1. Sélectionnez **Device (Périphérique)** > **Virtual Systems (Systèmes virtuels)**, puis sélectionnez le système virtuel dans lequel vous avez consolidé vos sources User-ID.
2. À l'onglet **Resource (Ressource)**, **Make this vsys a User-ID data hub (Faites de ce système virtuel un centre de données User-ID)**, puis cliquez sur **Yes (Oui)** pour confirmer. Cliquez ensuite sur **OK**.

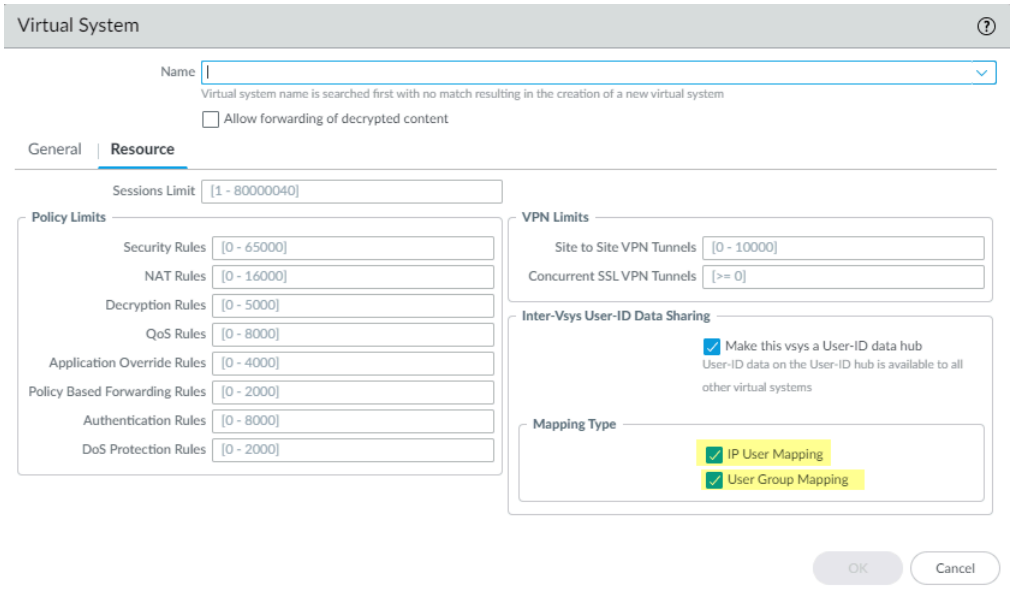



**STEP 2 |** Cliquez sur **Yes (Oui)** pour confirmer.



**STEP 3 |** Sélectionnez le **Mapping Type (type de mappage)** que vous souhaitez partager, puis cliquez sur **OK**.




- **IP User Mapping (Mappage d'utilisateur IP)** : partagez les informations de mappage adresse IP-nom d'utilisateur avec d'autres systèmes virtuels.
- **User Group Mapping (Mappage de groupe d'utilisateurs)** : partagez les informations de mappage de groupe avec d'autres systèmes virtuels.

*Vous devez sélectionner au moins un type de mappage.*

**STEP 4 |** Consolidez vos sources User-ID et migrez-les vers le système virtuel que vous voulez utiliser en tant que pôle User-ID.

Vous consolidez ainsi la configuration User-ID pour une simplicité opérationnelle. En configurant le pôle pour qu'il surveille des serveurs et se connecte aux agents qui faisaient préalablement l'objet d'une surveillance par d'autres systèmes virtuels, c'est le pôle qui collecte les informations de mappage de l'utilisateur plutôt que chaque système virtuel qui les collecte individuellement. Si vous ne voulez pas partager les mappages de systèmes virtuels donnés, configurer ces mappages sur un système virtuel qui ne fera pas office de hub.

*Utilisez le même format pour le nom d'utilisateur principal sur les systèmes virtuels et les pare-feux.*

1. Supprimez les sources qui sont inutiles ou obsolètes.

2. Identifiez toutes les configurations de vos agents Windows ou intégrés et de toutes les sources qui envoient les mappages d'utilisateur à l'aide de l'API XML et copiez-les sur le système virtuel que vous voulez utiliser en tant que hub User-ID.

   *Sur le pôle, vous pouvez configurer n'importe quelle source User-ID qu est actuellement configurée sur un système virtuel. Cependant, les informations de mappage adresse IP et port/nom d'utilisateur obtenues auprès des agents Terminal Server ne sont pas partagées entre le pôle User-ID et les systèmes virtuels connectés.*

3. Spécifiez les sous-réseaux que User-ID doit inclure ou exclure du mappage.
4. Définissez la **Ignore User List (Liste des utilisateurs ignorés)**.
5. Sur tous les autres systèmes virtuels, supprimez les sources qui se trouvent sur le pôle User-ID.

**STEP 5 |** **Commit (Validez)** les modifications pour activer le pôle User-ID et commencer à collecter les mappages pour les sources consolidées.

**STEP 6 |** Confirmez que le pôle User-ID mappe les utilisateurs.

1. Utilisez la commande **`show user ip-user-mapping all`** pour montrer les mappages adresse IP/nom d'utilisateur et le système virtuel qui fournit les mappages.
2. Utilisez la commande **`show user user-id-agent statistics`** pour montrer le système virtuel qui fait office de pôle User-ID.
3. Confirmez que le pôle partage les mappages de groupe à l'aide des commandes CLI suivantes :
   - `show user group-mapping statistics`
   - `show user group-mapping state all`
   - `show user group list`
   - `show user group name (afficher le nom du groupe utilisateur)<group-name>`

# App-ID

Pour activer en toute sécurité les applications sur votre réseau, les pare-feu Palo Alto Networks de nouvelle génération fournissent à la fois une perspective applicative et Web, App-ID et le filtrage des URL, vous protégeant contre tout un éventail de risques liés à la législation, à la réglementation, à la productivité et à l'utilisation des ressources.

App-ID confère une visibilité au sein des applications présentes sur le réseau, pour que vous puissiez découvrir leur fonctionnement, leurs caractéristiques comportementales et leurs risques relatifs. La connaissance de ces applications vous permettra de créer et d'appliquer des règles de politiques de sécurité pour activer, inspecter et façonner des applications de votre choix et bloquer les applications indésirables. Lorsque vous définissez des règles de politiques pour autoriser le trafic, App-ID commence à classer le trafic sans aucune configuration supplémentaire.

Les App-ID nouveaux et modifiés sont lancés dans le cadre des Applications and Threat Content Updates (Mises à jour du contenu Applications et Menaces) ; suivez les Best Practices for Applications and Threats Content Updates (Meilleures pratiques pour les mises à jour du contenu des menaces et des applications) pour tenir les signatures des applications et des menaces à jour.

# Présentation d'App-ID

App-ID, un système de classification du trafic breveté, disponible uniquement sur les pare-feu Palo Alto Networks, sert à définir une application, indépendamment du port, du protocole, du cryptage (SSH ou SSL) ou de toute autre tactique évasive utilisée par l'application. Il applique de multiples mécanismes de classification (signatures d'applications, décodage de protocole d'application et analyse heuristique) à votre flux de trafic réseau pour identifier avec exactitude les applications.

Voici comment le système App-ID identifie les applications traversant votre réseau :

- Le trafic est mis en correspondance avec une politique pour vérifier s'il est autorisé sur le réseau.
- Des signatures sont ensuite appliquées au trafic autorisé afin d'identifier l'application en se basant sur des propriétés d'application uniques et les caractéristiques des transactions associées. La signature détermine également si l'application est utilisée sur son port par défaut ou si elle utilise un port non-standard. Si le trafic est autorisé par la politique, il est ensuite analysé pour détecter des menaces et analysé de façon plus approfondie pour identifier l'application de façon plus granulaire.
- Si App-ID détermine que le cryptage (SSL ou SSH) est en cours d'utilisation et qu'une règle de politique de Déchiffrement a été mise en place, la session est décryptée et les signatures d'applications sont appliquées une nouvelle fois au flux décrypté.
- Des décodeurs pour les protocoles connus sont ensuite utilisés afin d'appliquer des signatures supplémentaires basées sur le contexte afin de détecter d'autres applications susceptibles de fonctionner par tunnel à l'intérieur du protocole (par exemple Yahoo ! Instant Messenger utilisé sur HTTP). Les décodeurs valident la conformité du trafic avec la spécification du protocole et fournissent un support pour les pinholes dynamiques d'ouverture et de parcours NAT pour les applications telles que SIP et FTP.
- Pour les applications qui sont particulièrement évasives et qui ne peuvent pas être identifiées par une analyse avancée de la signature et du protocole, une analyse heuristique ou comportementale peut être lancée pour déterminer l'identité de l'application.

Dès que l'application est identifiée, la vérification de la politique détermine comment traiter l'application, par exemple, bloquer ou autoriser et analyser pour détecter toute menace, inspecter pour détecter des transferts de fichiers et des modèles de données non autorisés, ou façonner en utilisant QoS.

# Règles de politique App-ID simplifiées

Permettez en toute sécurité un large ensemble d'applications ayant des attributs communs en utilisant une seule règle de politique (par exemple, donner à vos utilisateurs un large accès aux applications web ou permettre en toute sécurité toutes les applications VoIP d'entreprise). Palo Alto Networks se charge de la recherche d'applications ayant des attributs communs, ce qu'elle fait par le biais de balises dans des mises à jour de contenu dynamiques. Cela :

- Minimise les erreurs et fait gagner du temps.
- Vous aide à créer des politiques qui se mettent automatiquement à jour pour traiter les demandes récemment publiées.
- Simplifie la transition vers un ensemble de règles basées sur l'App-ID en utilisant l'optimisateur de politique.

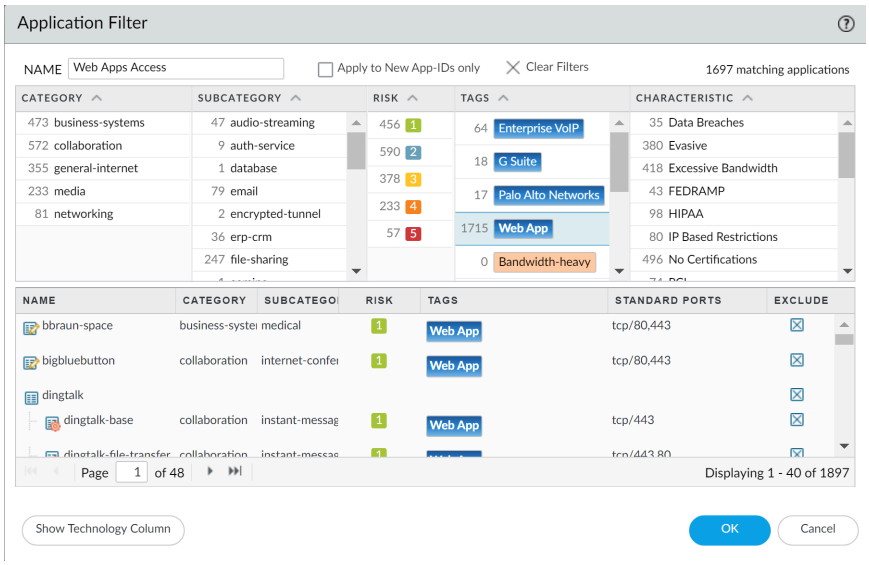
Votre pare-feu peut alors utiliser votre filtre d'application basé sur des étiquettes pour appliquer dynamiquement les nouveaux ID d'application et les mises à jour sans que vous ayez à revoir ou à mettre à jour les règles de politique chaque fois que de nouvelles applications sont ajoutées. Si vous choisissez d'exclure des applications d'une étiquette spécifique, les nouvelles mises à jour de contenu honorent ces exclusions. Vous pouvez également utiliser vos propres étiquettes pour définir les types de demandes en fonction des exigences de votre politique.

- Création d'un filtre d'application à l'aide d'étiquettes
- Création d'un filtre d'application basé sur des étiquettes personnalisées

## Création d'un filtre d'application à l'aide d'étiquettes

**STEP 1 |** Créez un filtre d'application à l'aide d'une ou plusieurs étiquettes.

Si vous sélectionnez plus d'une étiquette, les applications doivent correspondre aux deux étiquettes à inclure dans le filtre.




**STEP 2 |** (Optional (Facultatif)) Excluez les balises de votre filtre en cochant la case dans la colonne **Exclude (Exclure)**.

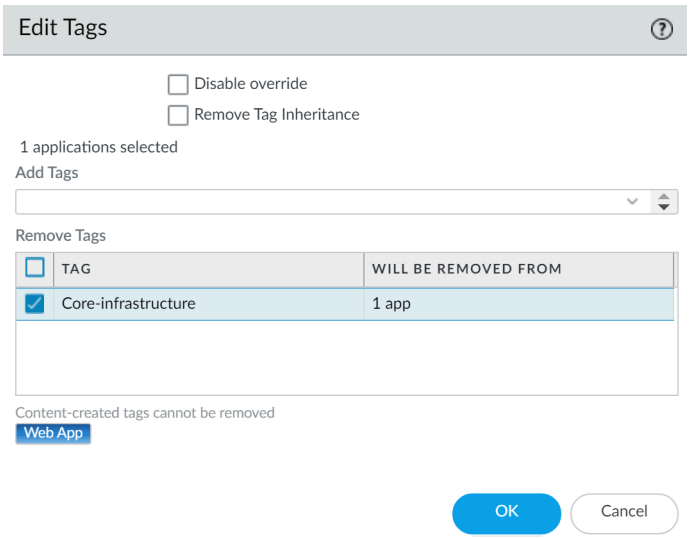
**STEP 3 |** Créez une règle de politique de sécurité et **Add (Ajoutez)** votre nouveau filtre d'application à l'onglet **Application**.

**STEP 4 |** **Commit (Validez)** vos modifications.

## Création d'un filtre d'application basé sur des étiquettes personnalisées

**STEP 1 |** Créez une étiquette personnalisée et appliquez-la aux App-ID.

1. (Facultatif) Supprimez les étiquettes d'une application.
2. Filtrez ou cherchez des applications, puis sélectionnez les applications spécifiques pour lesquelles supprimer les étiquettes.
3. **Edit Tags (Modifiez les étiquettes)**, puis sélectionnez les étiquettes à supprimer.

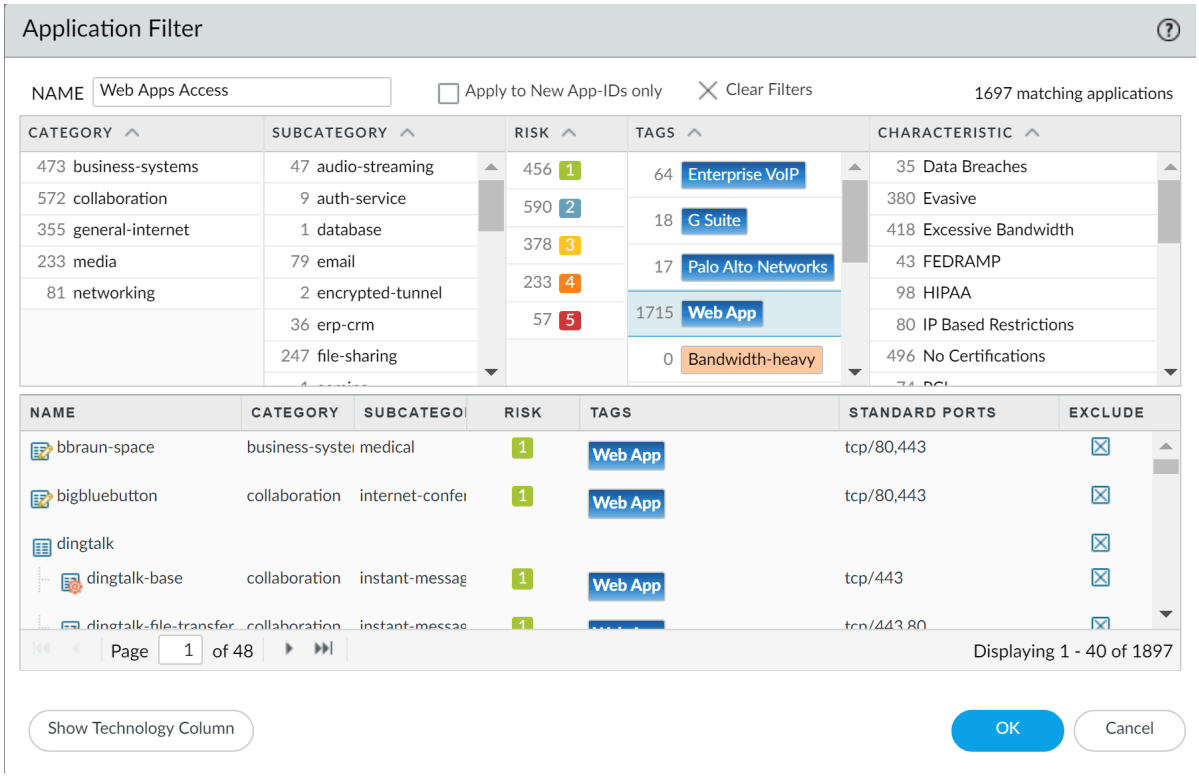



4. Cliquez sur **OK**.

**STEP 2 |** Créez un filtre d'application à l'aide d'une ou plusieurs étiquettes.

Si vous sélectionnez plus d'une étiquette, les applications doivent correspondre aux deux étiquettes à inclure dans le filtre.



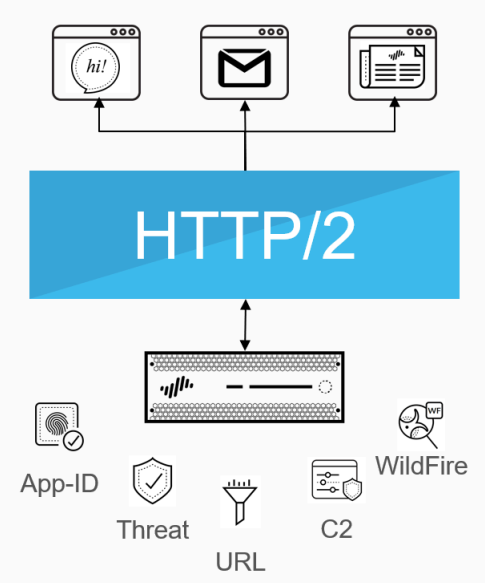

**STEP 3 |** Créez une règle de politique de sécurité et **Add (Ajoutez)** votre nouveau filtre d'application à l'onglet **Application**.

**STEP 4 |** **Commit (Validez)** vos modifications.

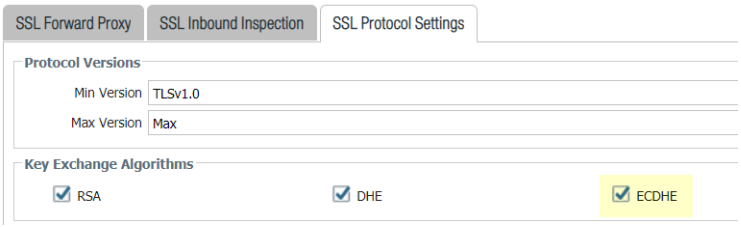
 

# Inspection d'App-ID et HTTP/2

Vous pouvez désormais activer en toute sécurité les applications qui utilisent HTTP/2 sans effectuer de configuration supplémentaire sur le pare-feu. Au fur et à mesure de l'augmentation de l'adoption de HTTP/2 pour les sites Web, le pare-feu peut appliquer la politique de sécurité et toutes les capacités de prévention et de détection des menaces sur une base flux par flux. Cette visibilité du trafic HTTP/2 vous permet de sécuriser les serveurs web qui fournissent des services sur HTTP/2 et permet aux utilisateurs de profiter de la vitesse et des gains d'efficacité en matière de ressources que procure HTTP/2.




Le pare-feu traite et inspecte le trafic HTTP/2 par défaut lorsque le déchiffrement SSL est activé. Pour que l'inspection HTTP/inspection 2 fonctionne correctement, le pare-feu doit pouvoir utiliser elliptic curve Diffie-Hellman (Diffie-Hellman basé sur les courbes elliptiques ; ECDHE) en tant qu'algorithmes d'échange de clés pour les sessions SSL. ECDHE est activée par défaut, mais vous pouvez confirmer qu'il est activé en sélectionnant **Objects (Objets)** > **Decryption (Déchiffrement)** > **Decryption Profile (Profil de déchiffrement)** > **SSL Decryption (Déchiffrement SSL)** > **SSL Protocol Settings (Paramètres du protocole SSL)**.



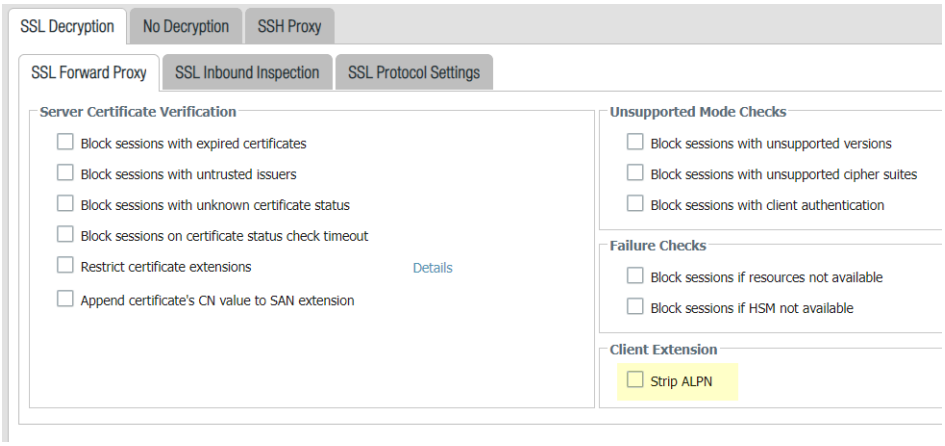

*Lorsque les journaux de décryptage introduits dans PAN-OS 10.1 sont activés, vous devez activer la* Tunnel Content Inspection (Inspection du contenu du tunnel) *pour obtenir l'App-ID pour le trafic HTTP/2.*

Vous pouvez désactiver l'inspection HTTP/2 du trafic cible ou globalement :

- Désactivez l'inspection HTTP/2 du trafic cible.

  Vous devrez spécifier que le pare-feu doit supprimer toute valeur contenue l'extension TLS Application-Layer Protocol Negotiation (ALPN). ALPN est utilisé pour sécuriser les connexions HTTP/2 connections, lorsqu'aucune valeur n'est indiquée pour cet extension TLS, le pare-feu déclasse le trafic HTTP/2 en HTTP/1.1 ou le classe en tant que trafic TCP inconnu.




  1. Sélectionnez **Objects (Objets)** > **Decryption (Déchiffrement)** > **Decryption Profile (Profil de déchiffrement)** > **SSL Decryption (Déchiffrement SSL)** > **SSL Forward Proxy (Proxy de transfert SSL)**, puis sélectionnez **Strip ALPN (Enlever l'ALPN)**.
  2. Associez le profil de déchiffrement à une politique de déchiffrement (**Policies (Politiques)** > **Decryption (Déchiffrement)**) pour désactiver l'inspection HTTP/2 pour le trafic qui correspond à la politique.
  3. **Commit (Validez)** vos modifications.

- Désactivez l'inspection HTTP/2 globalement :

  Utilisez la commande de la CLI suivante : `set deviceconfig setting http2 enable no` et **Commit (Validez)** vos modifications. Le pare-feu classifiera le trafic HTTP/2 en tant que trafic inconnu.

# Gestion des applications propres à l'entreprise ou inconnues

Palo Alto Networks fournit des mises à jour hebdomadaires pour les applications afin d'identifier les nouvelles signatures App-ID. Par défaut, App-ID est toujours activé sur le pare-feu et vous n'avez pas besoin d'activer une série de signatures pour identifier les applications bien connues. Normalement, les seules applications qui sont classées en tant que trafic inconnu, tcp, udp ou non-syn-tcp, dans l'ACC et les journaux du trafic sont des applications commercialisées qui n'ont pas encore été ajoutées au système App-ID, des applications internes ou personnalisées sur votre réseau ou des menaces potentielles.

Parfois, le pare-feu peut signaler une application comme inconnue pour les raisons suivantes :

- Données incomplètes : un établissement de liaison s'est produit, mais aucun paquet de données n'a été envoyé avant l'expiration du délai.
- Données insuffisantes : un établissement de liaison s'est produit, suivi d'un ou de plusieurs paquets de données. Toutefois, le nombre de paquets de données échangés était insuffisant pour identifier l'application.

Les choix suivants sont disponibles pour gérer des applications inconnues :

- Créer des politiques de sécurité pour contrôler des applications inconnues par un protocole TCP inconnu, un protocole UDP inconnu ou en combinant une zone source, une zone de destination et des adresses IP.
- Demander un système App-ID à Palo Alto Networks : si vous souhaitez inspecter et contrôler les applications qui traversent votre réseau, pour détecter tout trafic inconnu, vous pouvez enregistrer une capture de paquets. Si la capture de paquets révèle que l'application est une application commerciale, vous pouvez envoyer cette capture de paquets à Palo Alto Networks pour le développement du système App-ID. S'il s'agit d'une application interne, vous pouvez créer un système App-ID personnalisé et/ou définir une politique de contrôle prioritaire sur l'application.
- Procédez à la Création d'une application propre à l'entreprise avec une signature et joignez-la à une politique de sécurité ou créez une application propre à l'entreprise et définissez une politique de contrôle prioritaire sur l'application. Une application propre à l'entreprise vous permet de personnaliser la définition de l'application interne (caractéristiques, catégorie et sous-catégorie, risque, port, délai d'expiration) et d'exercer un contrôle granulaire des politiques afin de minimiser l'étendue du trafic non identifié sur votre réseau. La création d'une application propre à l'entreprise vous permet aussi d'identifier correctement l'application dans **l'ACC (ACC)** et les journaux du trafic, mais elle est aussi utile dans l'audit/la génération de rapports sur les applications présentes sur votre réseau. Dans le cas d'une application propre à l'entreprise, vous pouvez définir une signature et un modèle qui identifient de façon unique l'application et les joindre à une politique de sécurité qui autorise ou rejette l'application.

  En revanche, si vous souhaitez que le pare-feu traite l'application propre à l'entreprise en utilisant un acheminement rapide (inspection de la Couche 4 au lieu d'utiliser App-ID pour l'inspection de la Couche 7), vous pouvez également référencer l'application propre à l'entreprise dans une règle de politique de contrôle prioritaire sur l'application. Dans le cas d'une application propre à l'entreprise, un contrôle prioritaire sur l'application empêche la session d'être traitée par le moteur App-ID, qui est une inspection de la Couche 7. Il force plutôt le pare-feu à gérer la session

comme un pare-feu à inspection d'état régulière au niveau de la Couche 4 et permet ainsi de gagner du temps pour le traitement de l'application.

Par exemple, si vous concevez une application propre à l'entreprise qui se déclenche sur un en-tête de l'hôte ***www.monsiteweb.com***, les paquets sont d'abord identifiés comme étant du type ***navigation-web***, puis sont associés à votre application propre à l'entreprise (dont l'application parente est navigation-web. Comme l'application parente est de type navigation-web, l'application propre à l'entreprise est inspectée à la Couche 7 et analysée pour identifier son contenu et ses vulnérabilités.

Si vous définissez un contrôle prioritaire sur l'application, le pare-feu arrête le traitement à la Couche 4. Le nom de l'application personnalisée est affecté à la session pour permettre de l'identifier dans les journaux, et le trafic n'est pas analysé pour détecter des menaces.

# Gestion des App-ID nouveaux et modifiés

Les ID d'application nouveaux et modifiés sont fournis au pare-feu dans le cadre des mises à jour de contenu d'applications et de menaces. Tandis que les ID d'application nouveaux et modifiés permettent au pare-feu de renforcer votre stratégie de sécurité avec une précision toujours croissante, les modifications de la politique de sécurité qui peuvent survenir lors de l'installation d'une mise à jour de contenu peuvent affecter la disponibilité des applications. Pour cette raison, vous devrez réfléchir à la meilleure façon de déployer les mises à jour de contenu afin de bénéficier de la toute dernière prévention des menaces et d'ajuster votre stratégie de sécurité afin de tirer le meilleur parti des ID d'application nouveaux et modifiés.

Les options suivantes vous permettent d'évaluer l'impact de nouveaux App-ID sur l'application des politiques existantes, de désactiver (et d'activer) des App-ID et de directement mettre à jour les règles des politiques pour sécuriser et exécuter les applications récemment identifiées :

- Flux de travail pour mieux intégrer les App-ID nouveaux et modifiés
- Afficher les App-ID nouveaux et modifiés dans une version de contenu
- Reportez-vous à la section Incidence des App-ID nouveaux et modifiés sur votre politique de sécurité.
- S'assurer que les nouveaux App-ID critiques sont autorisés
- Surveillance des nouveaux App-ID
- Activation et désactivation des App-ID

Vous pouvez également profiter des Règles de politique App-ID simplifiées qui utiliser les étiquettes d'application fournies dans les mises à jour de contenu.

## Flux de travail pour mieux intégrer les App-ID nouveaux et modifiés

Reportez-vous à ce flux de travail principal pour configurer dans un premier temps les mises à jour du contenu de menace et des applications, puis intégrer au mieux les App-ID nouveaux et modifiés à votre politique de sécurité. Tout ce dont vous avez besoin pour déployer des mises à jour de contenu est mentionné ici.

**STEP 1 |** Harmonisez vos besoins d'affaires avec une approche de déploiement des mises à jour du contenu de menace et des applications.

Apprenez-en davantage sur le fonctionnement des Mises à jour du contenu de menace et des applications et déterminez si l'approche adoptée par votre organisation est stratégique ou si elle dispose d'un niveau de sécurité optimal. En comprenant ce qui compte le plus pour votre entreprise, vous serez plus à même de décider de la meilleure façon de déployer les mises à jour du contenu et d'appliquer les meilleures pratiques pour satisfaire vos besoins d'affaires. Il se peut que vous souhaitiez appliquer une combinaison des deux approches, peut-être selon le déploiement du pare-feu (centre de données ou périmètre) ou l'emplacement du bureau (à distance ou siège social).

**STEP 2 |** Passez en revue les Best Practices for Applications and Threats Content Updates (Meilleures pratiques pour les mises à jour du contenu de menace et des applications) et appliquez-les en fonction des exigences en matière de disponibilité et de sécurité du réseau de votre organisation.

**STEP 3 |** Configurez une règle de politique de sécurité pour toujours autoriser les nouveaux App-ID qui pourraient avoir une incidence à l'échelle du réseau, comme les applications d'authentification ou de développement de logiciels.

Les caractéristiques des nouveaux App-IP correspondent uniquement aux App-ID introduits dans la dernière version de contenu. Lorsqu'elles sont utilisées dans une politique de sécurité, vous disposez d'une période d'un mois pour peaufiner votre politique de sécurité en fonction des nouveaux App-ID tout en garantissant la disponibilité continue pour les App-ID qui tombent dans des catégories essentielles (S'assurer que les nouveaux App-ID critiques sont autorisés).

**STEP 4 |** Définissez l'horaire du déploiement des mises à jour du contenu de menace et des applications, ce qui comprend l'option de repousser l'installation des nouveaux App-ID jusqu'à ce que vous ayez eu le temps de mettre à jour la politique de sécurité comme il se doit (au moyen du **New App-ID Threshold (seuil des nouveaux App-ID)**).

**STEP 5 |** Après avoir établi un calendrier d'installation des mises à jour de contenu, vérifiez régulièrement pour Afficher les App-ID nouveaux et modifiés dans une version de contenu.

**STEP 6 |** Vous pouvez ensuite Voir l'incidence des App-ID nouveaux et modifiés sur votre politique de sécurité et apportez les ajustements nécessaires à votre politique de sécurité.

**STEP 7 |** Procédez à la Surveillance des nouveaux App-ID pour avoir un aperçu de l'activité des nouveaux App-ID de votre réseau, afin d'être parfaitement équipé pour apporter les mises à jour les plus efficaces à votre politique de sécurité.

## Afficher les App-ID nouveaux et modifiés dans une version de contenu

Pour les mises à jour de contenu téléchargées et installées, vous pouvez consulter une liste des App-ID nouveaux et modifiés que la mise à jour contient. Des détails complets sur l'application sont donnés, et, plus important encore, les mises à jour des applications ayant une incidence à l'échelle du réseau (par exemple, LDAP ou IKE) sont clairement indiquées et un examen de la politique est recommandé. Dans le cas des App-ID modifiés, les détails de l'application décrivent également comment la nouvelle couverture a été étendue ou ce qui la rend plus précise.

**STEP 1 |** Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**, puis **Check Now (Vérifier maintenant)** pour actualiser la liste des mises à jour du contenu disponibles.

**STEP 2 |** Pour une version de contenu téléchargée ou actuellement installée, cliquez sur le lien **Review Apps (Consulter les applications)** dans la colonne **Actions** pour voir les détails des applications nouvellement identifiées ou modifiées qui composent cette version :

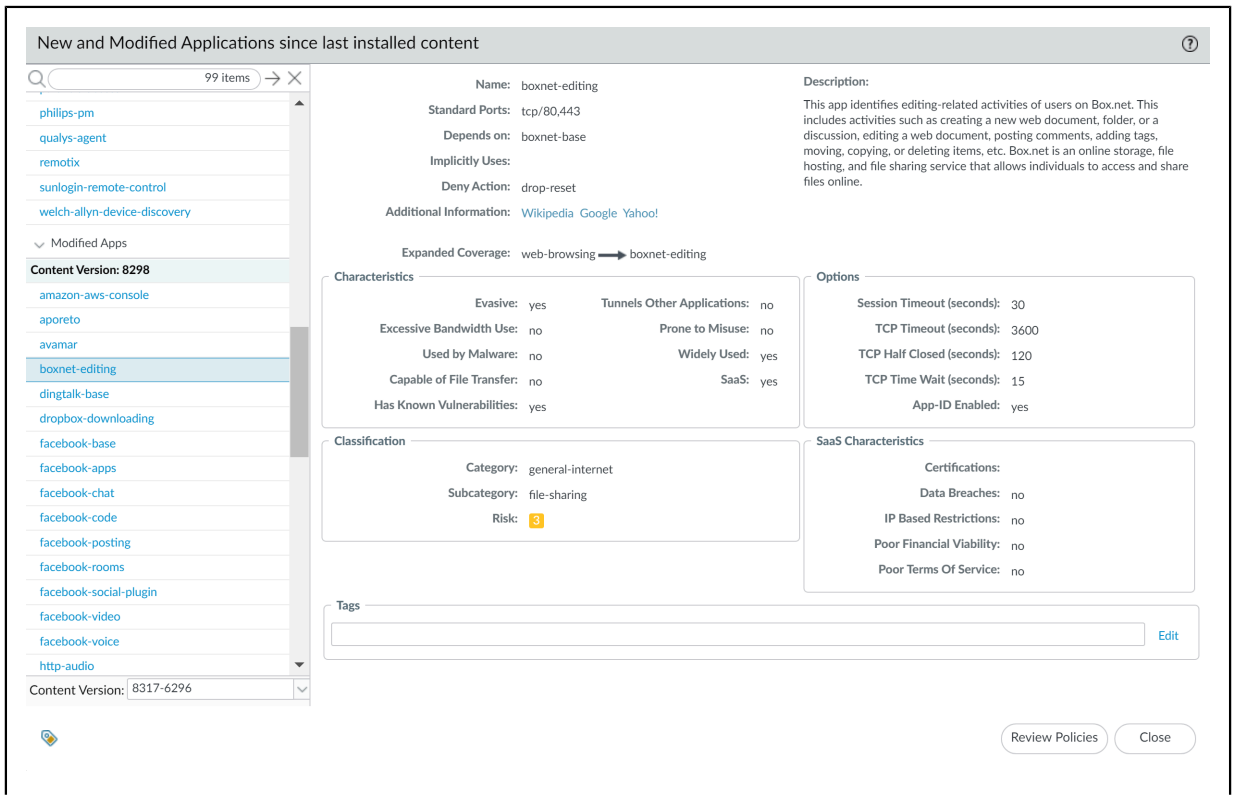
Applications and Threats **Last checked:** 2020/09/23 01:02:02 PDT **Schedule:** Every Wednesday at 01:02 (Download only)

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 8292-6181 | panupv2-all-apps-8292-6181 | Apps | Full | 47 MB | | 2020/07/13 11:46:39 PDT | ✓ previously | | Revert | Release Notes |
| 8317-6296 | panupv2-all-apps-8317-6296 | Apps | Full | 48 MB | | 2020/09/08 17:55:10 PDT | | ✓ | Review Policies<br>Review Apps | Release Notes |
| 8320-6309 | panupv2-all-contents-8320-6309 | Apps, Threats | Full | 56 MB | 192cfd8c2ff0058c188d0... | 2020/09/14 18:13:54 PDT | | | Download | Release Notes |
| 8320-6310 | panupv2-all-contents-8320-6310 | Apps, Threats | Full | 57 MB | 2436f79a8f02aeef37b82... | 2020/09/15 10:19:15 PDT | | | Download | Release Notes |
| 8321-6311 | panupv2-all-contents-8321-6311 | Apps, Threats | Full | 56 MB | d3ac74a854c08527869cf... | 2020/09/15 13:44:29 PDT | | | Download | Release Notes |
| 8321-6312 | panupv2-all-contents-8321-6312 | Apps, Threats | Full | 57 MB | a4275ee394b5d942c09e... | 2020/09/15 14:26:20 PDT | | | Download | Release Notes |

**STEP 3 |** Consultez les App-ID que cette version de contenu introduit ou modifie, par rapport à la dernière version de contenu.

Les nouveaux App-ID sont répertoriés distinctement des App-ID modifiés. Des détails complets de l'application sont fournis pour chacun d'eux. Les App-ID qui, selon Palo Alto Networks, auront une incidence sur l'ensemble du réseau sont assortis d'un indicateur recommandant l'examen de la politique.




Les détails des nouveaux App-ID que vous pouvez utiliser pour évaluer leur impact éventuel sur l'application des politiques sont les suivants :

- **Depends on (Dépend de)** : répertorie les signatures d'applications sur lesquelles l'App-ID s'appuie pour identifier l'application de façon unique. Si l'une des signatures d'applications répertoriées dans le champ **Depends On (Dépend de)** est désactivée, l'App-ID dépendant sera également désactivé.
- **Previously Identified As (Précédemment identifié en tant que)** : répertorie les App-ID correspondant à l'application avant l'installation d'un nouvel App-ID pour identifier l'application de manière unique.
- **App-ID Enabled (App-ID activé)** : tous les App-ID s'affichent comme étant activés lors du téléchargement d'une version du contenu, à moins que vous ne choisissiez de désactiver manuellement la signature des App-ID avant d'installer la mise à jour du contenu.

Pour les App-ID modifiés, les détails comprennent des informations sur ce qui suit : **Expanded Coverage (Couverture étendue)**, **Remove False Positive (Suppression de faux positifs)** et modifications des métadonnées de l'application. Les champs Expanded Coverage (Couverture étendue) et Remove False Positive (Suppression de faux positifs) indiquent tous deux ce qui a changé dans la couverture de l'application (soit qu'elle est plus exhaustive, soit qu'elle a été

restreinte) et une icône en forme d'horloge indique un changement dans les métadonnées, qui implique la mise à jour de certains détails de l'application.

**STEP 4 |** Selon vos constats, cliquez sur **Review Policies (Consulter les politiques)** vous voir quelle est l'incidence des App-ID nouveaux et modifiés sur l'application de la politique de sécurité : Reportez-vous à la section Incidence des App-ID nouveaux et modifiés sur votre politique de sécurité.

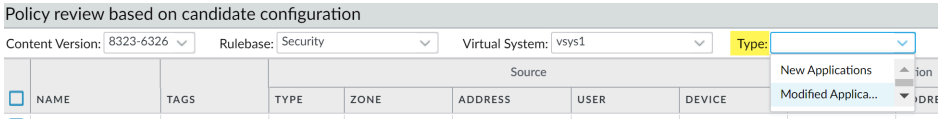
## Reportez-vous à la section Incidence des App-ID nouveaux et modifiés sur votre politique de sécurité.

Les App-ID nouvellement catégorisés et modifiés peuvent modifier la manière dont le pare-feu applique le trafic. Effectuez un examen de la politique de mise à jour du contenu pour voir comment les App-ID nouveaux et modifiés influent sur votre politique de sécurité et pour facilement apporter les ajustements nécessaires. Vous pouvez effectuer un examen de la politique de mise à jour du contenu pour le contenu téléchargé et installé.

**STEP 1 |** Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**.

**STEP 2 |** Reportez-vous à la section Afficher les App-ID nouveaux et modifiés dans une version de contenu pour en apprendre davantage sur chaque App-ID qu'une version de contenu introduit ou modifie.

**STEP 3 |** Pour une version de contenu téléchargée ou actuellement installée, cliquez sur **Review Policies (Réviser les politiques)** dans la colonne Action. La boîte de dialogue **Policy review based on candidate configuration (Vérification des politiques selon la configuration candidate)** vous permet de filtrer par **Content Version (Version du contenu)** et d'afficher les App-ID nouveaux ou modifiés introduits dans une version spécifique (vous pouvez également filtrer l'impact des nouveaux App-ID sur les politiques par **Rulebase (Base de règles)**, **Virtual System (Système virtuel)** et **Application**).




**STEP 4 |** Sélectionnez un App-ID dans le menu déroulant **Application** pour afficher les règles de politiques actuellement en vigueur dans l'application. Les règles affichées se basent sur les App-ID correspondant à une application avant l'installation du nouvel App-ID (consultez les détails d'une application pour afficher la liste des signatures d'applications auxquelles elle était **Previously Identified As (Précédemment identifié en tant que)** préalablement à l'installation du nouvel App-ID).

**STEP 5 |** Utilisez les détails fournis dans la vérification des politiques pour planifier la mise à jour des règles de politiques dès l'installation de l'App-ID ou, si la version du contenu qui est comprise dans App-ID est déjà installée, les changements que vous apportez prennent effet immédiatement.

Vous pouvez **Add app to selected policies (Ajouter l'application aux politiques sélectionnées)** ou **Remove app from selected policies (Supprimer l'application des politiques sélectionnées)**.

# S'assurer que les nouveaux App-ID critiques sont autorisés

Les nouveaux App-ID peuvent entraîner un changement de l'application de la politique pour le trafic nouvellement identifié comme appartenant à une certaine application. Pour atténuer l'incidence sur l'application de la politique de sécurité, vous pouvez utiliser la caractéristique du **New App-ID (Nouveau App-ID)** dans une règle de politique de sécurité, pour que la règle applique toujours les App-ID les plus récemment introduits sans vous demander d'apporter des modifications à la configuration lorsque de nouveaux App-ID sont installés. Les caractéristiques des nouveaux App-IP correspondent toujours uniquement aux nouveaux App-ID introduits dans la dernière version de contenu installée. Lorsqu'une nouvelle version du contenu est installée, les caractéristiques du nouveau App-ID commencent automatiquement à se mettre en correspondance avec les nouveaux App-ID de cette version du contenu.

Vous pouvez choisir d'appliquer tous les nouveaux App-ID ou cibler la règle de politique de sécurité qui doit appliquer certains types de nouveaux App-ID qui pourraient avoir une incidence à l'échelle du réseau ou une incidence critique (par exemple, n'appliquez que les applications de développement de logiciels ou d'authentification). Définissez la règle de politique de sécurité sur **Allow (Autoriser)** pour vous assurer que le pare-feu continue d'autoriser les-App même si une version d'App-ID introduit une couverture étendue ou plus précise des applications critiques.

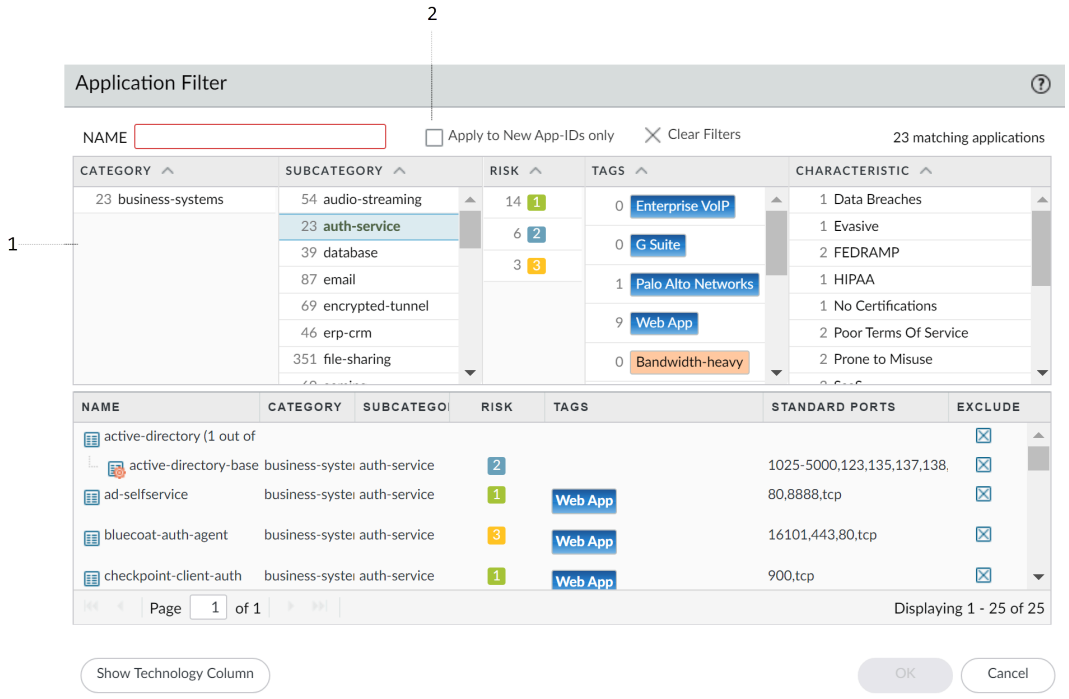
Les nouveaux App-ID sont lancés mensuellement. Ainsi, une politique de sécurité qui autorise les plus récents App-ID vous donne donc un mois (ou si le pare-feu n'installe pas les mises à jour de contenu selon un calendrier, jusqu'à la prochaine mise à jour du contenu manuelle) pour évaluer l'incidence qu'ont les applications nouvellement catégorisées sur l'application de la politique de sécurité et pour apporter les ajustements nécessaires.

**STEP 1 |** Sélectionnez **Object (Objet)** > **Applications (Applications)**, puis **Add (Ajoutez)** un nouveau filtre d'applications.

**STEP 2 |** Définissez les types de nouvelles applications pour lesquelles vous voulez garantir une disponibilité permanente selon la sous-catégorie ou la caractéristique. Par exemple, sélectionnez la catégorie service d'authentification pour garantir l'autorisation des applications nouvellement installées qui sont connues pour fournir ou soutenir l'authentification.

**STEP 3 |** Uniquement après restreint les types de nouvelles applications que vous souhaitez autoriser immédiatement après leur installation, sélectionnez **Apply to New App-IDs only (Appliquer aux nouveaux App-ID uniquement)**.




**STEP 4 |** Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis ajoutez ou modifiez une règle de politique qui est configurée pour autoriser le trafic correspondant.

**STEP 5 |** Sélectionnez **Application** et ajoutez le nouveau **Application Filter (Filtre d'applications)** à la règle de politique en tant que critère de correspondance.

**STEP 6 |** Cliquez sur **OK (OK)** puis sur **Commit (Valider)** pour enregistrer vos modifications.

**STEP 7 |** Pour continuer à ajuster votre politique de sécurité pour tenir compte des changements dans l'application de la politique que les nouveaux App-ID introduisent :

- Procédez à la Surveillance des nouveaux App-ID : surveillez l'activité des nouveaux App-ID et obtenez des rapports sur celle-ci.
- Reportez-vous à la section Afficher les App-ID nouveaux et modifiés dans une version de contenu : voyez l'incidence que les App-ID nouvellement installés ont sur vos règles de politique existantes.

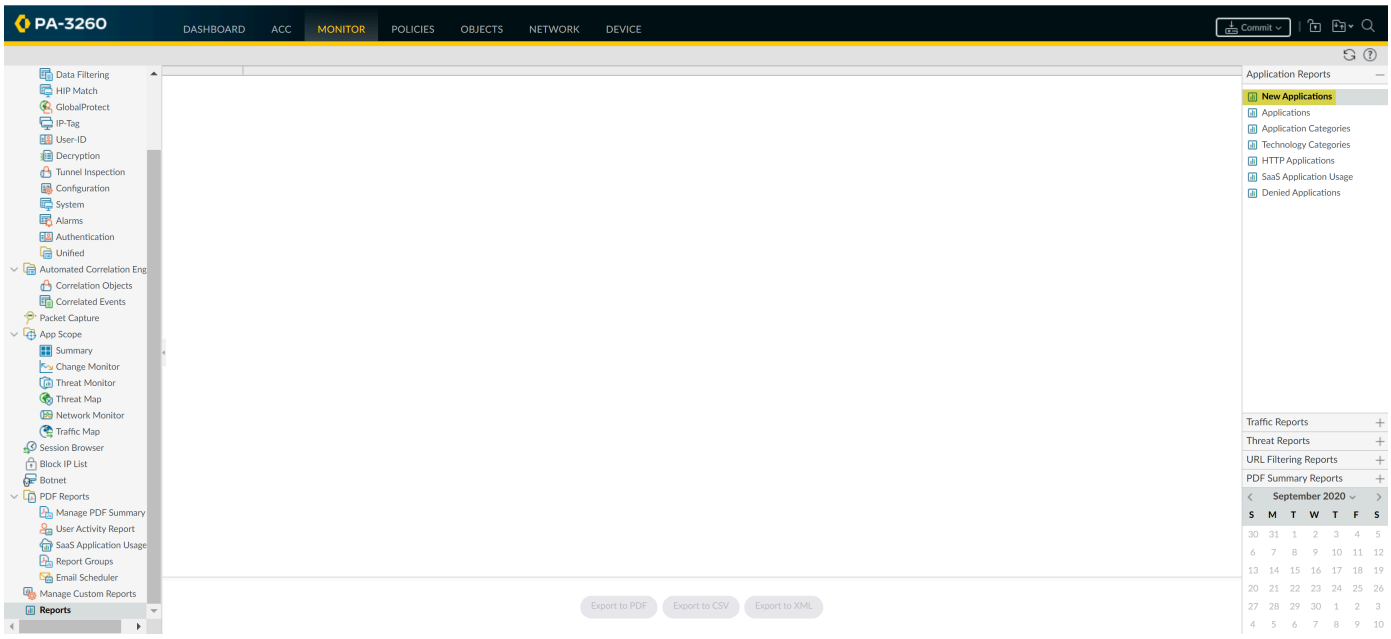
## Surveillance des nouveaux App-ID

La **nouvelle caractéristique App-ID** vous permet de surveiller les nouvelles applications sur votre réseau, ce qui vous permet de mieux évaluer les mises à jour de la politique de sécurité que vous souhaitez effectuer. Utilisez la nouvelle caractéristique App-ID sur l'ACC pour obtenir une visibilité sur les nouvelles applications de votre réseau et pour générer des rapports détaillant l'activité de l'application nouvellement catégorisée. Ce que vous apprenez peut vous aider à prendre les bonnes décisions concernant la mise à jour de votre politique de sécurité afin de faire appliquer les ID d'application les plus récents. Que vous l'utilisiez sur l'ACC ou pour générer des rapports (ou pour

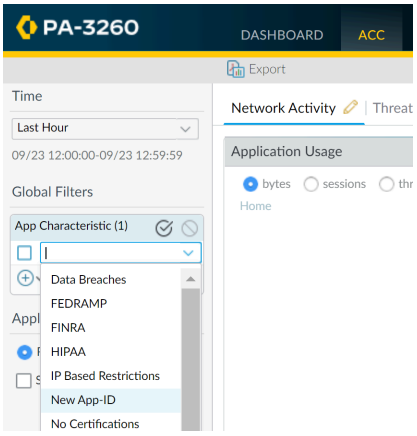
 

vous assurer que les nouveaux ID d'application critiques soient autorisés), la nouvelle caractéristique d'ID d'application correspond toujours aux nouveaux ID d'application dans les dernières versions de contenu installées. Lorsqu'une nouvelle version du contenu est installée, les caractéristiques du nouveau App-ID commencent automatiquement à se mettre en correspondance avec les nouveaux App-ID de cette version du contenu.

- Générer un rapport avec des détails spécifiques concernant les nouvelles applications (applications introduites uniquement dans la dernière version de contenu).




- Utilisez l'ACC pour surveiller l'activité d'une nouvelle application: sélectionnez **ACC** et sous **Global FIlters (Filtres globaux)**, sélectionnez **Application** > **Application Characteristics (Caractéristiques d'application)** > **New App-ID (Nouvel ID)**.




# Activation et désactivation des App-ID

Vous pouvez désactiver tous les App-ID introduits dans une version de contenu si vous souhaitez bénéficier immédiatement de la plus récente prévention contre les menaces et que vous prévoyez d'activer les App-ID ultérieurement. Vous pouvez également désactiver les App-ID pour des applications données.

Les règles de politiques référençant des App-ID appliquent et correspondent uniquement au trafic en fonction des App-ID activés.

Certains App-ID ne peuvent pas être désactivés et n'autorisent que l'état Activé. Les App-ID ne pouvant pas être désactivés comprennent des signatures d'applications implicitement utilisées par d'autres App-ID (tels que unknown-tcp). La désactivation d'un App-ID de base pourrait entraîner la désactivation de ses App-ID dépendants. Par exemple, la désactivation de facebook-base va désactiver tous les autres App-ID Facebook.

- Désactivez tous les App-ID dans une version du contenu ou pour effectuer des mises à jour planifiées du contenu.

  Bien que cette option vous permette d'être protégé contre les menaces, en vous donnant l'option d'activer App-ID ultérieurement, au lieu de régulièrement désactiver les App-ID, Palo Alto Networks vous recommande de configurer une règle de politique de sécurité pour autoriser temporairement de nouveaux App-ID. Cette règle autorisera toujours les nouveaux App-ID introduits uniquement dans la dernière version de contenu. Comme les mises à jour de contenu qui comprennent de nouveaux App-ID ne sont lancées qu'une fois par mois, vous avez le temps d'évaluer les nouveaux App-ID et d'ajuster votre politique de sécurité pour couvrir les nouveaux App-ID, au besoin, tout en vous assurant que la disponibilité des applications essentielles n'est pas touchée.

  - Pour désactiver tous les nouveaux App-ID introduits dans une version du contenu, sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)** et cliquez sur **Install (Installer)** pour installer une version du contenu Application et Menaces. Lorsque vous y êtes invité, sélectionnez **Disable new apps in content update (Désactiver les nouvelles applications dans la mise à jour du contenu)**. Cochez la case visant à désactiver les applications, puis procédez à l'installation de la mise à jour du contenu.
  - Sur la page **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**, cliquez sur **Schedule (Calendrier)**. Sélectionnez **Disable new apps in content update (Désactiver les nouvelles applications dans la mise à jour du contenu)** pour les téléchargements et l'installation des versions du contenu.

- Désactivez simultanément les App-ID d'une application ou de plusieurs applications.

  - Pour désactiver simultanément une ou plusieurs applications en un clin d'œil, cliquez sur **Objects (Objets)** > **Applications (Applications)**. Cochez une ou plusieurs cases d'applications et cliquez sur **Disable (Désactiver)**.
  - Pour passer en revue les détails d'une application unique et désactiver son App-ID correspondant, sélectionnez **Objects (Objets)** > **Applications (Applications)** et **Disable App-ID (Désactiver l'App-ID)**. Vous pouvez utiliser cette étape pour désactiver les App-ID en attente (où la version du contenu incluant l'App-ID est téléchargée sur le pare-feu, mais n'est pas installée) ou les App-ID installés.

- Activez des App-ID.

  Activez les App-ID que vous avez précédemment désactivés en sélectionnant **Objects (Objets)** > **Applications (Applications)**. Cochez une ou plusieurs cases d'applications et cliquez sur **Enable (Activer)** ou consultez les détails d'une application spécifique et cliquez sur **Enable App-ID (Activer l'App-ID)**.

# Utilisation d'objets d'une application dans une politique

Utilisez les objets d'application pour définir la manière dont votre politique de sécurité gère les applications.

- Création d'un groupe d'applications
- Création d'un filtre d'application
- Création d'une application propre à l'entreprise
- Résolution des dépendances d'application

## Création d'un groupe d'applications

Un groupe d'applications est un objet qui contient des applications que vous voulez traiter de façon identique dans une politique. Les groupes d'applications sont utiles pour permettre d'accéder aux applications dont vous autorisez explicitement l'utilisation au sein de votre entreprise. Le regroupement d'applications autorisées simplifie l'administration de vos bases de règles. Au lieu d'avoir à mettre à jour les règles de chaque politique lorsque des modifications sont effectuées dans les applications prises en charge, vous pouvez uniquement mettre à jour les groupes d'applications concernés.

Lorsque vous décidez de la manière dont vous allez regrouper les applications, prévoyez comment vous allez permettre l'accès à vos applications autorisées et créez un groupe d'applications qui respecte chacun des objectifs de vos politiques. Par exemple, vous pouvez autoriser vos administrateurs informatiques seuls à accéder à certaines applications et autoriser tout autre utilisateur connu dans votre entreprise à accéder à d'autres applications. Dans ce cas, vous pouvez créer des groupes d'applications distincts pour chaque objectif de ces politiques. Même si vous souhaitez généralement autoriser l'accès aux applications uniquement sur le port par défaut, vous pouvez regrouper les applications faisant exception à cette règle et autoriser leur accès via une règle distincte.

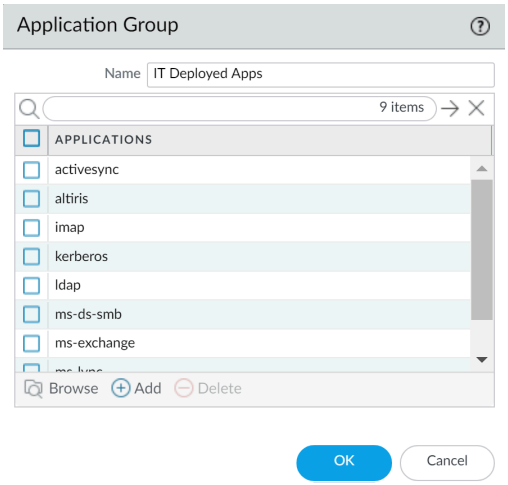
**STEP 1 |** Sélectionnez **Objects (Objets)** > **Application Groups (Groupes d'applications)**.

**STEP 2 |** Cliquez sur **Add (Ajouter)** pour ajouter un groupe et donnez-lui un **Name (Nom)** descriptif.

**STEP 3 |** (Facultatif) Sélectionnez **Shared (Partagé)** pour créer l'objet dans un emplacement partagé de manière à ce qu'il puisse être accessible en tant qu'objet partagé dans Panorama ou utilisé par tous les systèmes virtuels d'un pare-feu disposant de systèmes virtuels multiples.

**STEP 4 |** Cliquez sur **Add (Ajouter)** pour ajouter les applications de votre choix dans le groupe, puis cliquez sur **OK (OK)**.




**STEP 5 |** **Commit (Validez)** la configuration.

## Création d'un filtre d'application

Un filtre d'application est un objet qui regroupe dynamiquement des applications en fonction de leurs attributs que vous aurez définis, notamment la catégorie, la sous-catégorie, la technologie, les facteurs de risques et les caractéristiques. Ce filtre est utile lorsque vous souhaitez autoriser un accès sûr à des applications que vous n'avez pas explicitement autorisées mais auxquelles vos utilisateurs pourront accéder. Par exemple, vous pouvez permettre à vos employés de choisir leurs propres programmes de bureautique (tels qu'Evernote, Google Docs ou Microsoft Office 365) dans le cadre de leur travail. Pour activer ces types d'applications en toute sécurité, vous pouvez créer un filtre d'application correspondant à la Catégorie **business-systems (systèmes-entreprise)** et à la Sous-catégorie **office-programs (programmes-bureautique)**. À mesure que de nouveaux programmes de bureautique apparaissent et que de nouveaux App-ID sont créés, ces nouvelles applications vont automatiquement correspondre au filtre que vous aurez défini. Vous n'aurez aucune modification supplémentaire à apporter à la base de règles de votre politique pour autoriser en toute sécurité une application correspondant aux attributs que vous aurez définis pour le filtre.

**STEP 1 |** Sélectionnez **Objects (Objets)** > **Application Filters (Filtres d'application)**.

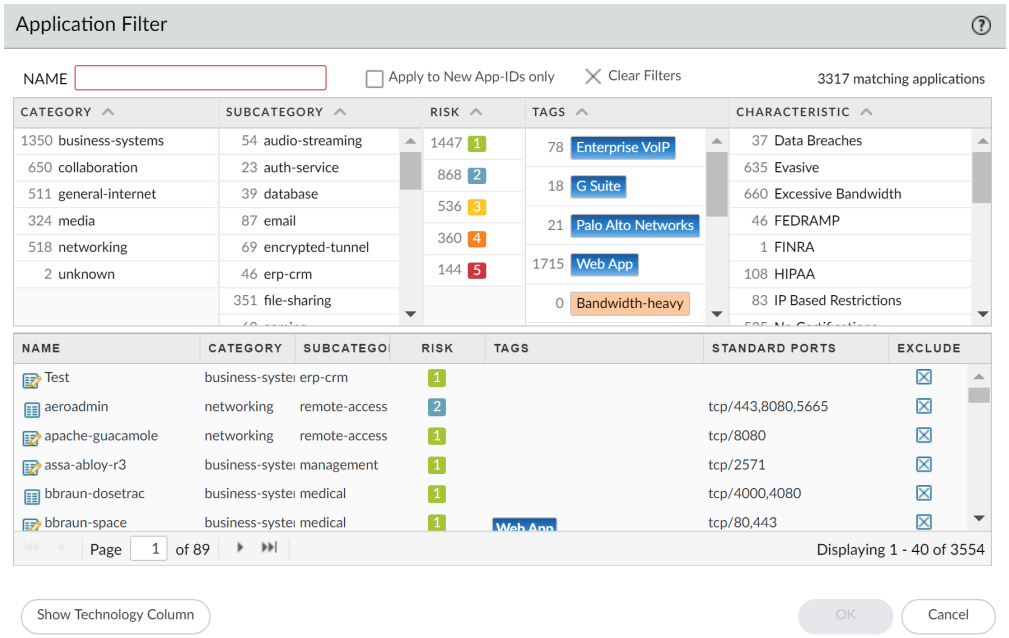
**STEP 2 |** Cliquez sur **Add (Ajouter)** pour ajouter un filtre et donnez-lui un **Name (Nom)** descriptif.

**STEP 3 |** (Facultatif) Sélectionnez **Shared (Partagé)** pour créer l'objet dans un emplacement partagé de manière à ce qu'il puisse être accessible en tant qu'objet partagé dans Panorama ou utilisé par tous les systèmes virtuels d'un pare-feu disposant de systèmes virtuels multiples.

**STEP 4 |** Définissez le filtre en sélectionnant des valeurs d'attribut dans les sections Catégorie, Sous-catégorie, Technologie, Risques et Caractéristiques. À mesure que vous sélectionnez des valeurs, vous remarquerez que la liste des applications correspondantes située en bas de la boîte de dialogue se réduit. Une fois que vous aurez ajusté les attributs du filtre afin qu'ils

correspondent aux types d'applications que vous souhaitez activer en toute sécurité, cliquez sur **OK (OK)**.




**STEP 5 |** **Commit (Validez)** la configuration.

## Création d'une application propre à l'entreprise

Pour activer des applications en toute sécurité, vous devez systématiquement classer l'ensemble du trafic sur tous les ports. Avec un système App-ID, les seules applications qui sont habituellement classées en tant que trafic inconnu (tcp, udp ou non-syn-tcp), dans l'ACC et les journaux du trafic sont des applications commercialisées qui n'ont pas encore été ajoutées au système App-ID, des applications internes ou propres à l'entreprise sur votre réseau ou des menaces potentielles.

***Si vous remarquez un trafic inconnu pour une application commerciale qui n'a pas encore d'App-ID, vous pouvez demander un nouvel App-ID à l'adresse suivante :*** http://researchcenter.paloaltonetworks.com/submit-an-application/**.**

Pour vous assurer que vos applications propres à l'entreprise internes ne s'affichent pas en tant que trafic inconnu, créez une application propre à l'entreprise. Ces applications vous permettront de contrôler vos politiques de manière granulaire afin de minimiser l'étendue du trafic non identifié sur votre réseau, tout en réduisant la surface d'attaque. La création d'une application propre à l'entreprise vous permet aussi d'identifier correctement l'application dans l'ACC et les journaux du trafic, ce qui vous permet de contrôler/générer des rapports sur les applications présentes sur votre réseau.

Pour créer une application propre à l'entreprise, vous devez définir ses attributs : caractéristiques, catégorie et sous-catégorie, risques, port, délai d'expiration. Vous devez également définir des modèles ou des valeurs que le pare-feu pourra utiliser pour les faire correspondre aux flux de trafic mêmes (la ***signature***). Pour finir, vous pouvez joindre l'application propre à l'entreprise à une politique de sécurité qui autorise ou interdit l'application (ou l'ajoute à un groupe d'applications ou la fait correspondre à un filtre d'application). Vous pouvez aussi créer des applications propres à l'entreprise

pour identifier des applications éphémères ayant un intérêt particulier, telles qu'ESPN3-Video pour la coupe du monde de football ou March Madness.

*Afin de recueillir les données adéquates pour créer une signature d'application propre à l'entreprise, vous devez bien avoir compris la notion de captures de paquets et de formation de datagrammes. Si la signature est créée de façon trop vague, vous pourriez inclure un autre trafic similaire par inadvertance ; si elle est définie de façon trop étroite, le trafic contournera la détection s'il ne correspond pas strictement au modèle.*

*Les applications propres à l'entreprise sont stockées dans une base de données distincte sur le pare-feu et cette dernière n'est pas concernée par les mises à jour App-ID hebdomadaires.*

*Les décodeurs de protocole d'application pris en charge qui activent le pare-feu afin qu'il détecte les applications susceptibles de fonctionner par tunnel à l'intérieur du protocole sont les suivants, conformément à la version de contenu 609 : FTP, HTTP, IMAP, POP3, SMB et SMTP.*

Voici un exemple basique de création d'une application propre à l'entreprise :

**STEP 1 |** Regroupez des informations concernant l'application que vous pourrez utiliser pour rédiger des signatures personnalisées.

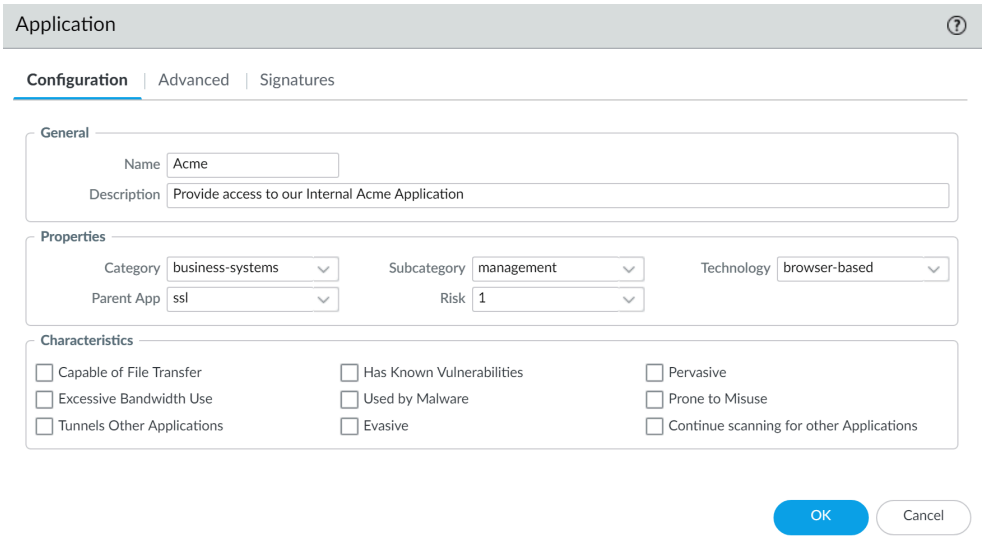
Pour cela, vous devez connaître l'application et savoir comment contrôler son accès. Par exemple, vous pouvez limiter les opérations que les utilisateurs peuvent exécuter à l'intérieur de l'application (telles que le chargement, le téléchargement ou la diffusion en direct). Ou vous pouvez autoriser l'application, mais appliquer une politique QoS.

- Capturez des paquets d'applications pour identifier les caractéristiques uniques de l'application sur laquelle vous allez baser la signature de votre application propre à l'entreprise. Pour cela, exécutez un programme d'analyse de protocole, tel que Wireshark, sur le système client pour capturer des paquets entre le client et le serveur. Exécutez différentes actions dans l'application, telles que le chargement et le téléchargement, pour localiser chaque type de session dans les captures de paquets (PCAP) résultants.
- Étant donné que le pare-feu prend par défaut des captures de paquets pour tout trafic inconnu, si le pare-feu se trouve entre le client et le serveur, vous pourrez afficher la capture de paquets du trafic inconnu directement dans le journal du trafic.
- Utilisez les captures de paquets pour identifier des modèles ou des valeurs dans les ***contextes*** des paquets qui vous serviront à créer des signatures correspondant de manière unique au trafic d'une application. Par exemple, recherchez des modèles de chaînes dans les en-têtes de requêtes ou de réponses HTTP, des chemins URI ou des noms d'hôtes. Pour plus d'informations sur les différents contextes de chaîne que vous pouvez utiliser pour créer des signatures d'applications et dans lesquels vous pouvez trouver des paquets contenant les valeurs correspondantes, consultez l'article Création de signatures de menaces personnalisées.

**STEP 2 |** Ajoutez l'application propre à l'entreprise.

1. Sélectionnez **Objects (Objets)** > **Applications (Applications)** et cliquez sur **Add (Ajouter)**.
2. Dans l'onglet **Configuration (Configuration)**, saisissez un **Name (Nom)** et une **Description (Description)** de l'application propre à l'entreprise qui permettra aux autres administrateurs de comprendre la raison pour laquelle vous avez créé l'application.
3. (Facultatif) Sélectionnez **Shared (Partagé)** pour créer l'objet dans un emplacement partagé de manière à ce qu'il puisse être accessible en tant qu'objet partagé dans Panorama ou utilisé par tous les systèmes virtuels d'un pare-feu disposant de systèmes virtuels multiples.
4. Définissez les propriétés et les caractéristiques de l'application.




**STEP 3 |** Fournissez des informations détaillées concernant l'application, telles que le protocole sous-jacent, le numéro de port utilisé pour exécuter l'application, les valeurs du délai d'expiration et tout type d'analyse que vous souhaitez réaliser sur le trafic.

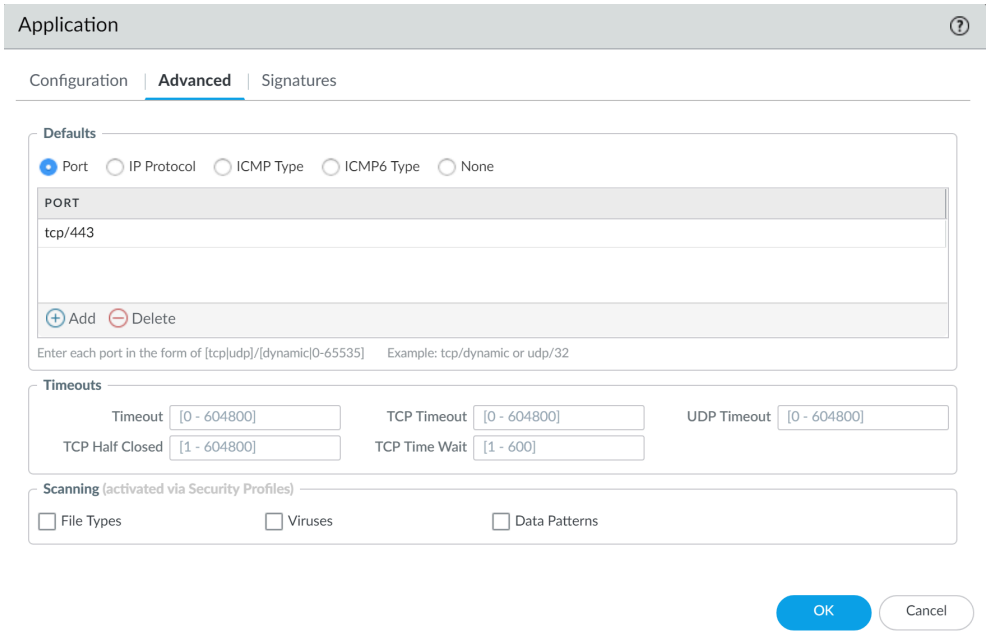
Dans l'onglet **Advanced (Avancé)**, définissez les paramètres qui permettront au pare-feu d'identifier le protocole de l'application :

- Indiquez les ports ou le protocole par défaut utilisés par l'application.
- Indiquez les valeurs de délai d'expiration de la session. Si vous n'indiquez aucune valeur pour le délai d'expiration, celles par défaut seront utilisées.
- Indiquez un type d'analyse supplémentaire que vous prévoyez de réaliser sur le trafic de l'application.

Par exemple, pour créer une application TCP propre à l'entreprise qui s'exécute sur SSL, mais qui utilise le port 4443 (au lieu du port 443 pour SSL par défaut), vous devrez indiquer le numéro de port. En ajoutant un numéro de port pour une application propre à l'entreprise, vous pouvez créer

des règles de politiques utilisant le port par défaut de l'application, plutôt que d'ouvrir des ports supplémentaires sur le pare-feu. Votre niveau de sécurité n'en sera que plus renforcé.




**STEP 4 |** Définissez des critères que le pare-feu peut utiliser pour faire correspondre le trafic à la nouvelle application.

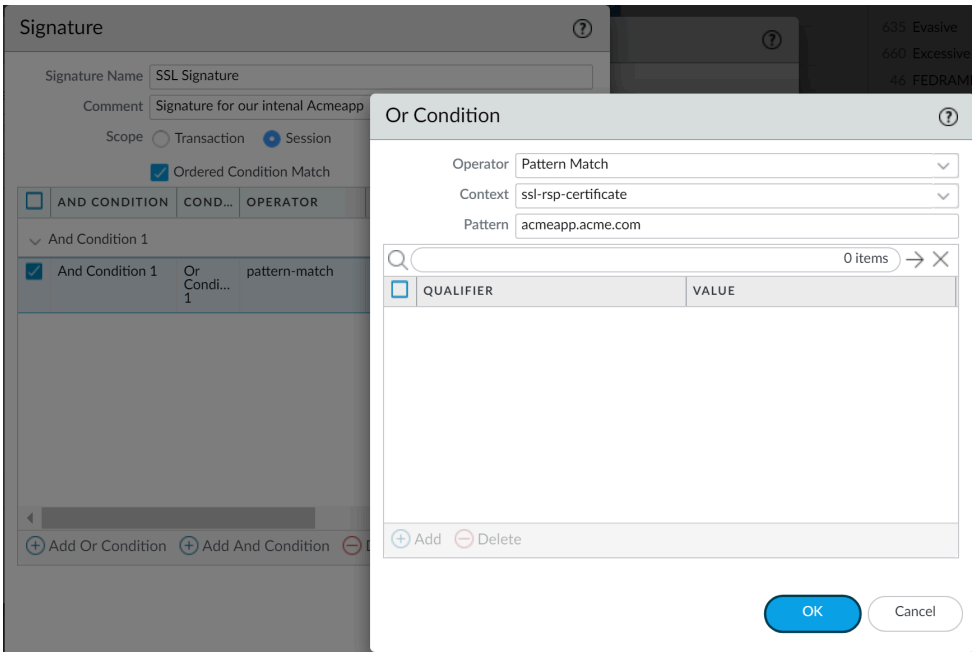
Vous utiliserez les informations que vous aurez regroupées dans les captures de paquets pour indiquer des valeurs de contextes de chaîne uniques que le pare-feu pourra utiliser pour faire correspondre des modèles dans le trafic de l'application.

1. Dans l'onglet **Signatures (Signatures)**, cliquez sur **Add (Ajouter)** et indiquez un **Signature Name (Nom de signature)** et saisissez éventuellement un **Comment (Commentaire)** pour indiquer comment vous prévoyez d'utiliser cette signature.
2. Indiquez la **Scope (Étendue)** de la signature : si elle correspond à une **Session (Session)** complète ou à une **Transaction (Transaction)** unique.
3. Indiquez des conditions afin de définir vos signatures en cliquant sur **Add And Condition (Ajouter une condition Et)** ou **Add Or Condition (Ajouter une condition Ou)**.
4. Sélectionnez un **Operator (Opérateur)** pour définir le type de condition de correspondance que vous utiliserez : **Pattern Match (Correspond au modèle)** ou **Equal To (Égal à)**.
   - Si vous avez sélectionné **Pattern Match (Correspond au modèle)**, indiquez le **Context (Contexte)**, puis utilisez une expression régulière pour indiquer le **Pattern (Modèle)** à faire correspondre avec le contexte sélectionné. Vous pouvez éventuellement cliquer sur **Add (Ajouter)** pour définir une paire qualificatif/valeur. La liste **Qualifier (Qualificatif)** est spécifique au **Context (Contexte)** choisi.
   - Si vous avez sélectionné **Equal To (Égal à)**, indiquez le **Context (Contexte)**, puis utilisez une expression régulière pour définir la **Position (Position)** des octets dans l'en-tête des paquets à faire correspondre avec le contexte sélectionné. Choisissez **first-4bytes (4-premiers-octets)** ou **second-4bytes (4-seconds-octets)**. Définissez une valeur

hexadécimale sur 4 octets pour le **Mask (Masque)** (par exemple, 0xffffff00) et pour la **Value (Valeur)** (par exemple, 0xaabbccdd).

Par exemple, si vous créez une application propre à l'entreprise pour l'une de vos applications internes, vous pouvez utiliser le **ssl-rsp-certificate Context (Contexte certificat-ssl-rsp)** pour définir une correspondance de modèle pour le message de réponse du certificat d'une négociation SSL dans le serveur et créer un **Pattern (Modèle)** correspondant au nom commun du serveur dans le message, comme indiqué ci-dessous :




5. Répétez les étapes 4.c et 4.d pour chaque condition de correspondance.
6. Si l'ordre dans lequel le pare-feu essaie d'établir une correspondance avec des définitions de signature est important, veillez à cocher la case **Ordered Condition Match (Correspondance avec les conditions ordonnées)**, puis ordonnez les conditions afin qu'elles soient évaluées dans l'ordre approprié. Sélectionnez une condition ou un groupe, puis cliquez sur **Move Up (Monter)** ou **Move Down (Descendre)**. Vous ne pouvez pas déplacer les conditions d'un groupe vers un autre.
7. Cliquez sur **OK (OK)** pour enregistrer la définition de la signature.

**STEP 5 |** Enregistrez l'application.

1. Cliquez sur **OK (OK)** pour enregistrer la définition de l'application propre à l'entreprise.
2. Cliquez sur **Commit (Valider)**.

**STEP 6 |** Validez comme prévu la correspondance entre le trafic et l'application propre à l'entreprise.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et cliquez sur **Add (Ajouter)** pour ajouter une règle de politique de sécurité afin d'autoriser la nouvelle application.
2. Exécutez l'application depuis un système client qui se trouve entre le pare-feu et l'application, puis consultez les journaux du trafic (**Monitor (Surveillance)** > **Traffic (Trafic)**) pour vous assurer que votre trafic correspond à la nouvelle application (et qu'elle est gérée par votre règle de politique).

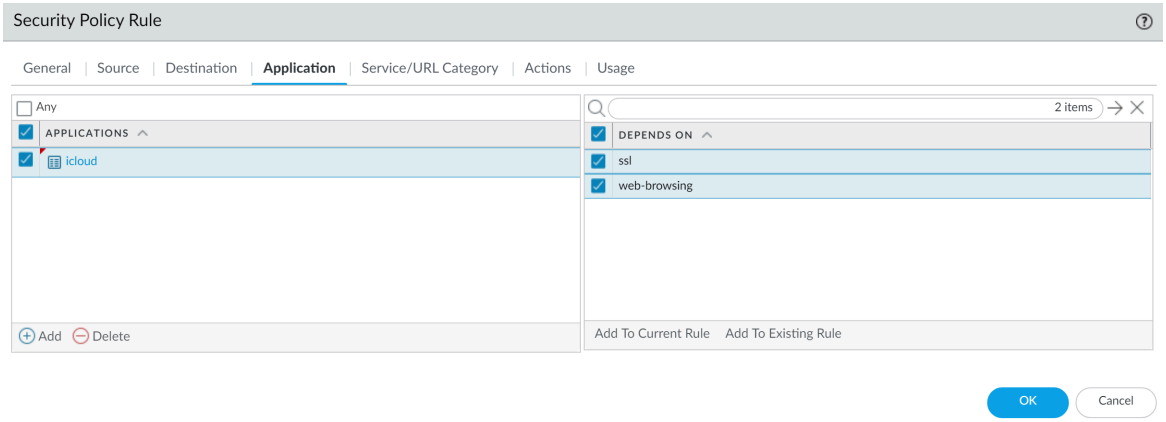
# Résolution des dépendances d'application

Vous pouvez aussi voir les dépendances d'application quand vous créer une nouvelle politique de sécurité et que vous effectuez un Commit. Quand une politique n'inclut pas toutes les dépendances d'application, vous pouvez directement accéder à la politique correspondante pour ajouter les applications requises.

**STEP 1 |** Création d'une règle de politique de sécurité

**STEP 2 |** Précisez l'application que la règle autorisera ou interdira.

1. À l'onglet **Applications (Applications)**, **Add (Ajoutez)** l'**Application (Application)** que vous souhaitez autoriser en toute sécurité. Vous pouvez sélectionner plusieurs applications ou vous pouvez utiliser des groupes d'applications ou des filtres d'applications.
2. Visualisez les dépendances pour les applications et **Ajouter à la règle actuelle** ou **Ajouter à la règle existante**.

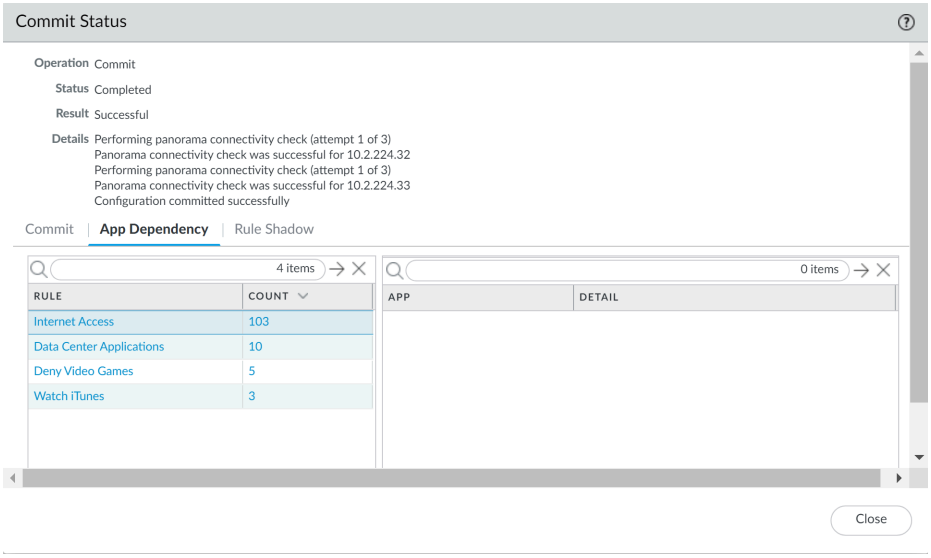



3. Si ajout à une règle existante, **Sélectionnez la règle** et cliquer sur **OK**.

**STEP 3 |** Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.

1. Examiner tous les avertissements de Commit dans l'onglet **App Dependency**.




2. Sélectionnez le **Compteur** pour voir les dépendances d'application non incluses.
3. Sélectionnez le nom de la **Règle** pour ouvrir une politique et ajouter les dépendances.

   *Résoudre toutes les dépendances d'application ou elles continueront à générer des avertissements durant les Commits.*

4. Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.

# Autoriser en toute sécurité les applications sur les ports par défaut

Les applications s'exécutant sur des ports inhabituels peuvent indiquer la présence d'un pirate qui tente de contourner les protections basées sur les ports. Par défaut de l'application est une fonction des pare-feu Palo Alto Networks qui vous offre un moyen facile de prévenir ce type d'attaque et d'activer les applications en toute sécurité sur leurs ports les plus fréquemment utilisés. Il est recommandé d'utiliser la fonction Par défaut de l'application pour les politiques de sécurité basées sur des applications, car elle réduit les frais administratifs et comble les lacunes en matière de sécurité qu'une politique basé sur les ports présente :

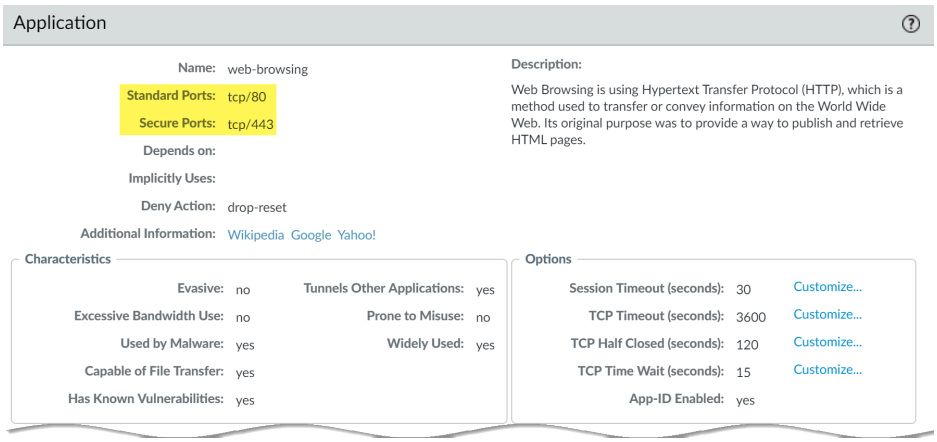
- **Less overhead (Moins contraignant)** : rédigez des règle de politique de sécurité basées sur les applications qui sont fondées sur vos besoins d'affaires, plutôt que de chercher et de conserver des mappages application/port. Nous avons défini les ports par défaut pour toutes les applications ayant un App-ID.
- **Stronger security (Sécurité renforcée)** : pour la sécurité, il est recommandé de ne permettre aux applications que de s'exécuter que sur leurs ports par défaut. La fonction Par défaut de l'application vous aide à vous assurer que les applications essentielles sont disponibles sans compromettre la sécurité si une application se comporte d'une manière inattendue.

  De plus, les ports par défaut utilisée par une application peuvent parfois varier selon que l'application est chiffrée ou en texte clair. Avec une politique basée sur les ports, vous devez ouvrir tous les ports par défaut qu'une application pourrait utiliser afin de tenir compte du chiffrement. Les ports ouverts comportent des lacunes en matière de sécurité dont un pirate peut tirer profit pour contourner votre politique de sécurité. Cependant, la fonction Par défaut de l'application fait la distinction entre le trafic d'applications en texte clair ou déchiffré. C'est à dire qu'elle peut appliquer le port par défaut pour une application, qu'elle soit chiffrée ou non.

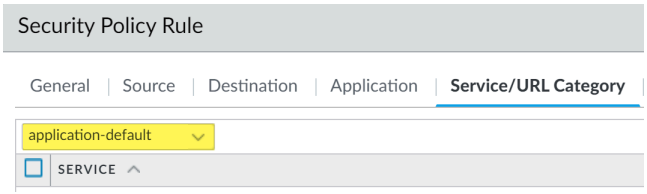
  Par exemple, sans la fonction Par défaut de l'application, vous devriez ouvrir les ports 80 et 443 pour permettre le trafic de navigation Web. Vous autoriseriez donc le trafic de navigation Web en texte clair et chiffré sur les deux ports. Si la fonction Par défaut de l'application est activée, le pare-feu applique strictement le trafic de navigation Web en texte clair uniquement sur le port 80 et le trafic par tunnel SSL uniquement sur le port 443.

Pour voir les ports qu'une application utilise par défaut, vous pouvez visiter Applipedia ou sélectionner **Objects (Objets)** > **Applications**. Les détails de l'application présentent, notamment, le port standard, c'est-à-dire le port qu'elle utilise le plus souvent en texte clair. Pour la navigation Web, les détails de SMTP, FTP, LDAP, POP3, et IMAP comprennent également le port sécuritaire de l'application, c'est-à-dire le port que l'application utilise lorsque le chiffrement est utilisé.




Sélectionnez **Policy (Politique)** > **Security (Sécurité)** et ajoutez ou modifiez une règle pour appliquer les applications uniquement sur leurs ports par défaut :




*Il est recommandé d'utilisation la fonction Par défaut de l'application dans le cadre d'une politique de sécurité basée les applications et avec le chiffrement SSL. De plus, si vous disposez déjà de règles de politique de sécurité qui contrôlent la navigation Web avec le* ***Service*** *défini sur service-http et service-https, vous devez mettre à jour ces règles afin d'utiliser la fonction Par défaut de l'application.*

# Applications prises en charge de façon implicite

Lors de la création d'une politique pour autoriser des applications spécifiques, vous devez aussi veiller à avoir autorisé toutes les autres applications dont l'application dépend. Dans de nombreux cas, vous n'aurez pas besoin d'autoriser explicitement l'accès aux applications dépendantes pour que le trafic puisse circuler car le pare-feu peut déterminer les dépendances et les autoriser implicitement. Cette prise en charge implicite s'applique aussi aux applications propres à l'entreprise basées sur HTTP, SSL, MS-RPC ou RTSP. Pour les applications pour lesquelles le pare-feu ne peut pas déterminer d'applications dépendantes dans les délais, vous devrez autoriser explicitement les applications dépendantes lors de la définition de vos politiques. Vous pouvez déterminer les dépendances des applications à partir du workflow de votre politique de sécurité basée sur les applications à l'aide de l'un des moyens suivants :

- Optimiseur de politique
- Création d'un filtre d'application à l'aide d'étiquettes
- Création d'un filtre d'application basé sur des étiquettes personnalisées
- Résolution des dépendances d'application

Applipedia est également disponible au besoin.

Le tableau suivant dresse la liste des applications pour lesquelles le pare-feu dispose d'une prise en charge implicite (conformément à la Mise à jour du contenu 595).

| Application | Prise en charge implicite |
|---|---|
| 360-safeguard-update | http |
| apple-update | http |
| apt-get | http |
| as2 | http |
| avg-update | http |
| avira-antivir-update | http, ssl |
| blokus | rtmp |
| bugzilla | http |
| clubcooee | http |
| corba | http |
| cubby | http, ssl |

| Application | Prise en charge implicite |
|---|---|
| dropbox | ssl |
| esignal | http |
| evernote | http, ssl |
| ezhelp | http |
| facebook | http, ssl |
| discussion-facebook | jabber |
| facebook-social-plugin | http |
| fastviewer | http, ssl |
| forticlient-update | http |
| good-for-enterprise | http, ssl |
| google-cloud-print | http, ssl, jabber |
| google-desktop | http |
| google-talk | jabber |
| google-update | http |
| gotomypc-desktop-sharing | citrix-jedi |
| gotomypc-file-transfer | citrix-jedi |
| gotomypc-printing | citrix-jedi |
| hipchat | http |
| iheartradio | ssl, http, rtmp |
| infront | http |
| instagram | http, ssl |
| issuu | http, ssl |
| java-update | http |

| Application | Prise en charge implicite |
|---|---|
| jepptech-updates | http |
| kerberos | rpc |
| kik | http, ssl |
| lastpass | http, ssl |
| logmein | http, ssl |
| mcafee-update | http |
| megaupload | http |
| metatrader | http |
| mocha-rdp | t_120 |
| mount | rpc |
| ms-frs | msrpc |
| ms-rdp | t_120 |
| ms-scheduler | msrpc |
| ms-service-controller | msrpc |
| nfs | rpc |
| oovoo | http, ssl |
| paloalto-updates | ssl |
| panos-global-protect | http |
| panos-web-interface | http |
| pastebin | http |
| pastebin-posting | http |
| pinterest | http, ssl |
| portmapper | rpc |

| Application | Prise en charge implicite |
|---|---|
| prezi | http, ssl |
| rdp2tcp | t_120 |
| renren-im | jabber |
| roboform | http, ssl |
| salesforce | http |
| stumbleupon | http |
| supremo | http |
| symantec-av-update | http |
| trendmicro | http |
| trillian | http, ssl |
| twitter | http |
| whatsapp | http, ssl |
| xm-radio | rtsp |

# Optimisation de la règle de politique de sécurité

L'optimiseur de politique offre un workflow simple pour migrer votre ancienne base de règles de politique de sécurité vers une base de règles basée sur App-ID, qui améliore la sécurité en réduisant la surface d'attaque et en vous procurant une visibilité des applications, ce qui vous permet de les activer en toute sécurité. L'optimisateur de politique identifie les règles basées sur les ports afin que vous puissiez les convertir en règles d'autorisation basées sur les applications ou ajouter des applications à partir d'une règle basée sur le port à une règle existante basée sur les applications sans compromettre la disponibilité des applications. Il identifie également l'allocation de plus de règles fondées sur App-ID (les règles App-ID configurées avec des applications non utilisées). L'optimiseur de politique vous permet de prioriser les règles basées sur les ports à migrer en premier, d'identifier les règles basées sur les applications qui autorisent les applications que vous n'utilisez pas et d'analyser les caractéristiques d'utilisation des règles, comme le nombre de correspondances.

La conversion des règles basées sur les ports en règles basées sur les applications permet d'améliorer votre posture de sécurité, car vous sélectionnez les applications que vous souhaitez autoriser et refusez toutes les autres applications. Vous éliminez ainsi le trafic indésirable et potentiellement malveillant de votre réseau. Conjuguée à la restriction du trafic des applications à leurs ports par défaut (définissez le service sur **application-default [Par défaut de l'application]**), la conversion vers des règles basées sur les applications empêche également les applications utilisant des techniques d'évasion d'utiliser des ports non standard.

Vous pouvez utiliser cette fonction sur :

- Les pare-feu qui utilisent la version 9.0 de PAN-OS et sur lesquels App-ID est activé.
- Panorama utilisant la version 9.0 de PAN-OS. Vous n'avez pas à mettre à niveau les pare-feu que Panorama gère pour utiliser les capacités du **Policy Optimizer (Optimiseur de politique)**. Cependant, pour utiliser les capacité de **Rule Usage (Utilisation d'une règle)** (Surveiller l'utilisation de la règle de politique), les pare-feu doivent utilisés la version 8.1 de PAN-OS ou une version ultérieure. Si les pare-feu gérés se connectent aux collecteurs de journaux, ces collecteurs de journaux doivent également utiliser la version 9.0 de PAN-OS. Les pare-feux séries PA-7000 avec une carte de processing de log (LPC) peuvent aussi exécuter PAN-OS 8.1 (ou ultérieur)
- Pour la compatibilité avec Cortex Data Lake, Panorama exécutant PAN-OS 10.0.4 ou version ultérieure avec le plug-in Cloud Services 2.0 ou version ultérieure installé.

*Les pare-feu PA-7000 Series prennent en charge deux cartes de journalisation : la Log Processing Card (carte de traitement des journaux ; LPC) du pare-feu PA-7000 et la Firewall Log Forwarding Card (carte de transfert des journaux ; LFC) du pare-feu PA-7000 à haut rendement. Contrairement à la LPC, la LFC ne dispose pas de disques pour stocker les journaux localement. La LFC transfère plutôt tous les journaux vers un ou plusieurs systèmes de journalisation externes, comme Panorama ou un serveur syslog. Si vous utilisez la LFC, les informations relatives à l'utilisation de l'Optimiseur de politique ne s'affichent pas sur le pare-feu, parce que les journaux de trafic ne sont pas stockés localement. Si vous utilisez la LPC, les journaux du trafic sont stockés localement sur le pare-feu. Les informations relatives à l'utilisation de Policy Optimizer s'affichent donc sur le pare-feu.*

Utilisez cette fonction pour :

- **Migrer les règles basées sur les ports vers des règles basées sur les applications** : Plutôt que de passer les journaux du trafic au peigne fin et de mapper manuellement les applications en des règles basées sur les ports, utilisez l'optimiseur de politique pour identifier les règles basées sur les ports et indiquer les applications qui ont été mises en correspondance avec chaque règle, ce qui vous permet de sélectionner les applications que vous souhaitez autoriser et de les activer en toute sécurité. La conversion de vos anciennes règles basées sur les ports aux règles d'autorisation basées sur les applications appuie vos applications d'entreprise et vous permet de bloquer les applications associées à des activités malveillantes.
- **Identifier les règles basées sur les applications qui sont surdimensionnées** : Les règles qui sont trop larges autorisent des applications que vous n'utilisez pas sur votre réseau, qui augmentent la surface d'attaque et le risque d'autoriser, par inadvertance, du trafic malveillant.

  *Supprimez les applications inutilisées des règles de politique de sécurité pour réduire la surface d'attaque et dispose d'une base de règles propre. N'autorisez pas les applications qui ne sont pas utilisées sur votre réseau.*
- **Add App-ID Cloud Engine (ACE) applications to Security policy rules (Ajouter des applications App-ID Cloud Engine (ACE) aux règles de politique de sécurité)** : si vous disposez d'un abonnement SaaS Security Inline, vous pouvez utiliser la New App Viewer (nouvelle visionneuse d'applications) de l'optimiseur de politique pour gérer les App-ID fournis dans le cloud dans la politique de sécurité. La documentation ACE décrit comment utiliser Policy Optimizer pour gagner en visibilité et contrôler les App-ID fournis par le cloud.

  *Les exemples d'optimiseur de politique de cette section n'affichent pas la nouvelle visionneuse d'application car ils décrivent des pare-feux qui n'ont pas d'abonnement SaaS Security Inline.*

*Pour migrer une configuration d'un ancien pare-feu vers un périphérique Palo Alto Networks, reportez-vous à la section* Pratiques exemplaires pour la migration vers une politique basée sur les applications.

Vous ne pouvez trier les règles de politique de sécurité sous **Security (Sécurité)** > **Policies (Politiques)**, car le tri modifierait l'ordre des règles dans la base de règles. Cependant, sous **Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer (Optimiseur de politique)**, l'optimiseur de politique offre des options de tri qui n'affectent pas l'ordre des règles pour vous aider à prioriser les règles à convertir ou à nettoyer en premier. Vous pouvez trier les règles en fonction de la quantité de trafic reçu au cours des 30 derniers jours, le nombre d'applications vues dans la règle, le nombre de journées sans nouvelles applications et le nombre d'applications autorisées (pour les règles surdimensionnées).

Vous pouvez utiliser l'optimiseur de politique d'autres façons, y compris pour la validation des règles de pré-production et la résolution des règles existantes. Prenez note que l'optimiseur de politique ne respecte que la **Log at Session End (Journalisation en fin de session)** et ignore la **Log at Session Start (Journalisation en début de session)** afin d'éviter de compter des applications transitoires dans les règles.

*En raison des contraintes des ressources, le pare-feu virtuel VM-50 Lite ne prend pas en charge l'optimiseur de politique.*

- Concepts relatifs à l'optimiseur de politique

- Migration des règles de sécurité basées sur le port vers des règles de politique de sécurité basées sur App-ID
- Cas d'utilisation de la migration du clonage de règles : Navigation Web et trafic SSL
- Ajout d'applications à une règle existante
- Identification des règles de politique de sécurité comportant des applications non utilisées
- Haute disponibilité pour les statistiques d'utilisation des applications
- Désactivation de l'optimiseur de politique

# Concepts relatifs à l'optimiseur de politique

Passez en revue les rubriques suivantes pour en apprendre davantage sur le support de cette fonction :

- Tri et filtrage des règles de politique de sécurité
- Suppression des données d'utilisation des applications

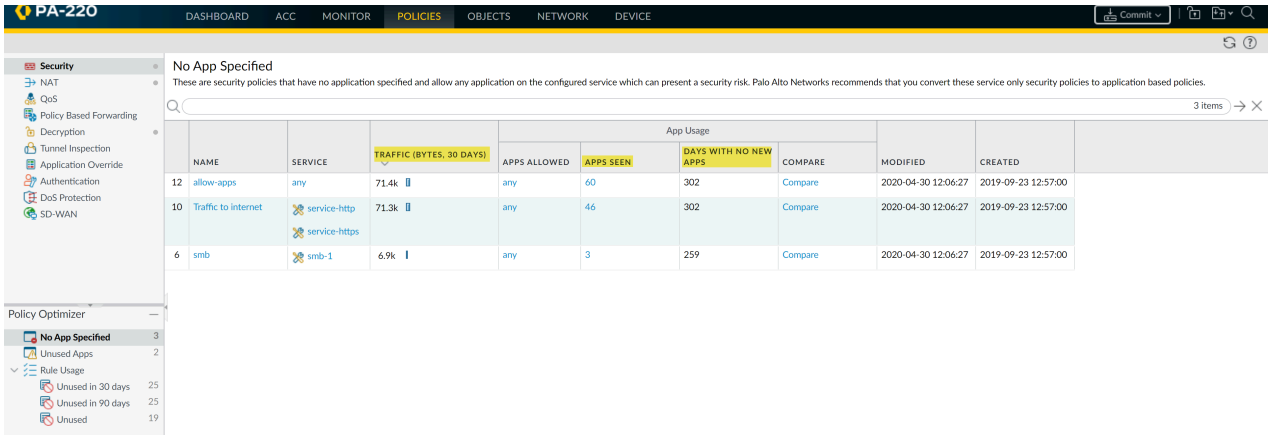
## Tri et filtrage des règles de politique de sécurité

Vous pouvez filtrer les règles de politique de sécurité pour voir les règles basées sur les ports, pour lesquelles aucune application n'est configurée (**Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer (Optimiseur de politique)** > **No App Specified (Aucune application spécifiée)**). Vous pouvez également filtrer pour afficher les règles sur lesquelles des applications sont configurées, mais le trafic ne correspond qu'à certaines des applications configurées : la règle est surprovisionnée et inclut des applications qui ne sont pas visibles sur la règle (**Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer (Optimiseur de politique)** > **Unused Apps (Applications non utilisées)**). En outre, si vous disposez d'une licence SaaS Security Inline, vous pouvez utiliser la New App Viewer (nouvelle visionneuse d'applications) pour filtrer les règles qui ont vu de nouvelles applications App-ID Cloud Engine (ACE) (consultez la documentation ACE pour savoir comment procéder). Vous pouvez trier les règles de politiques filtrées selon divers types de statistiques pour aider à prioriser les règles à faire passer de règles basées sur les ports à des règles basées sur les applications ou à nettoyer en premier.

*Vous ne pouvez filtrer ou trier les règles sous **Policies (Politiques) > Security (Sécurité)**, car cela aurait pour effet de modifier l'ordre des règles de politique dans la base de règles. Filtrage et tri des **Policies (Politiques) > Security (Sécurité) > > No App Specified (Aucune application spécifiée)**, **Policies (Politiques) > Security (Sécurité) > Policy optimizer (Optimisation des politiques) > Unused Apps (Applications inutilisées)**, et **Policy (politique) > Security (Sécurité) > Policy optimizer (Optimiseur de politique) > New App Viewer (Nouvelle visionneuse d'applications)** (si vous disposez d'un abonnement SaaS Inline Security) ne modifie pas l'ordre des règles dans la base de règles.*

Vous pouvez cliquer sur plusieurs en-têtes de colonne pour trier les règles en fonction des statistiques d'utilisation des applications. De plus, vous pouvez Affichage de l'utilisation de la règle de politique pour identifier et supprimer les règles inutilisées afin de réduire les risques de sécurité et d'organiser votre base de règles de politique. Le suivi de l'utilisation des règles vous permet de valider rapidement les ajouts de nouvelles règles et les modifications de règles ainsi que de surveiller l'utilisation des règles pour les opérations et les tâches de dépannage.




- **Traffic (Bytes, 30 days) [Trafic, Octets, 30 jours)]** : la quantité de trafic vue sur la règle au cours des 30 derniers jours. La fenêtre de 30 jours positionne les règles qui mettent ***réellement*** le plus de trafic en correspondance au haut de la liste par défaut (une période de temps plus longue met l'accent sur les règles plus anciennes qui demeurent au haut de la liste, car elles possèdent des totaux cumulatifs important, même si elles ne voient presque plus de trafic). Cliquez pour inverser l'ordre.
- **Apps Seen (Applications vues)** : placez les règles qui comportent le plus grand nombre ou le plus faible nombre d'applications vues au haut. Le pare-feu ne purge jamais automatiquement les données sur les applications.

  *Le pare-feu met à jour les **Apps Seen (Applications vues)** environ aux heures. Cependant, s'il y a un grand volume de trafic d'applications ou un grand nombre de règle, la mise à jour pourrait prendre plus d'une heure. Après avoir ajouté une application à une règle, attendez au moins une heure avant de générer les journaux du trafic pour voir les informations journalisées de l'application.*
- **Days with No New Apps (Journées sans nouvelles applications)** : positionnez les règles qui comptent le plus ou le moins de journées depuis la dernière correspondance de la nouvelle application à la règle au haut.

- (**Unused Apps (Applications inutilisées)** uniquement) **Apps Allowed (applications autorisées)** : positionnez les règles qui possèdent le plus grand nombre ou le plus faible nombre d'applications configurées au haut.

Les statistiques sur l'utilisation des applications comptent uniquement les applications des règles qui respectent les critères suivants :

- L'action de la règle doit être définie sur **Allow (Autoriser)**.
- Le paramètre des journaux de la règle doit être défini sur **Log at Session End (Journalisation en fin de session)** (c'est le paramètre de journalisation par défaut). Les règles dont la **Log at Session Start (Journalisation a lieu en début de session)** sont ignorées pour empêcher le calcul des applications transitoires.
- Le trafic valide doit correspondre à la règle. Par exemple, si la session prend fin avant qu'une quantité de trafic suffisante ait passée par le pare-feu pour identifier l'application, elle n'est pas comptée. Les types de trafic suivants ne sont pas valides et ne sont donc pas comptabilisés dans les statistiques de l'optimiseur de politique :
  - Données insuffisantes
  - Non applicable
  - TCP non synchronisé
  - Incomplet

  Vous pouvez filtrer les journaux du trafic (**Monitor (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)**) pour voir le trafic identifié comme correspondant à l'un de ces types. Par exemple, pour voir tout le trafic identifié comme étant incomplet, utilisez le filtre **`(app eq incomplete)`**.

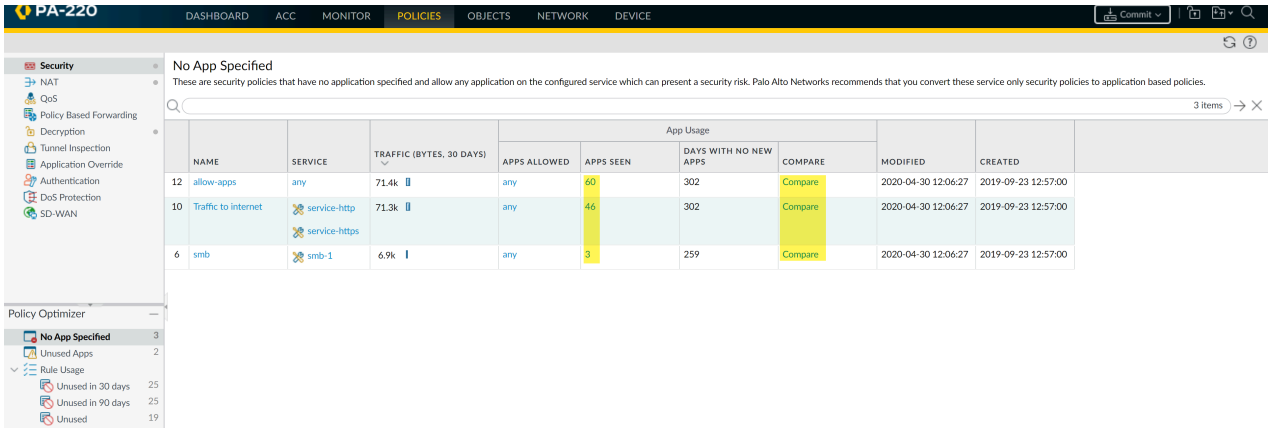
Si ces critères ne sont pas satisfaits, l'application n'est pas comptabilisée dans les statistiques comme **Apps Seen (Applications vues)**, n'affecte pas les statistiques comme **Days with No New Apps (Journées sans nouvelles applications)** et ne figure pas dans les listes d'applications.

*Le pare-feu ne fait pas le suivi des statistiques d'utilisation des applications pour les règles de politique de sécurité interzone par défaut et intrazone par défaut.*

*Si l'UUID d'une règle change, les statistiques d'utilisation des applications pour cette règle sont réinitialisées, parce que, en raison du changement d'UUID, le pare-feu voit la règle différemment (nouvelle règle).*

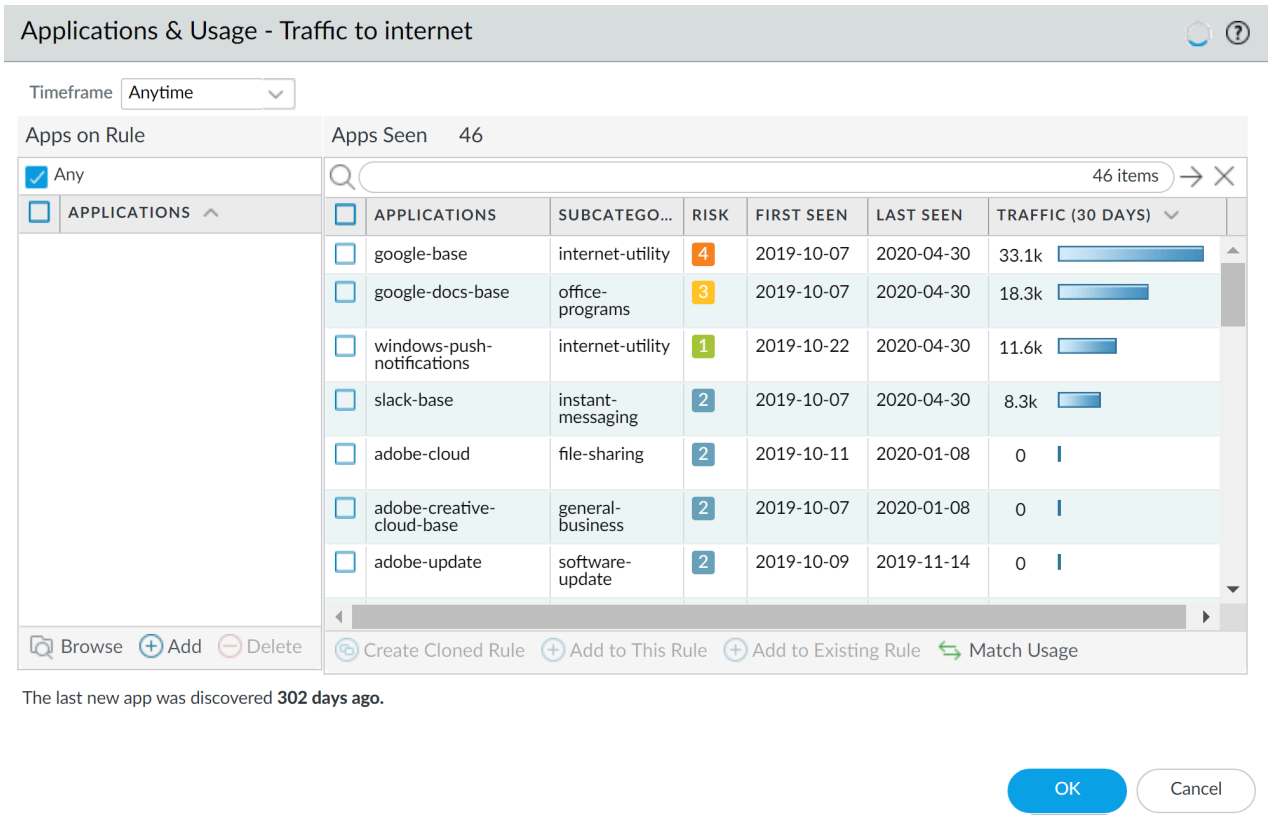
Pour voir et trier les applications vues dans une règle, dans la ligne de la règle, cliquez sur **Compare (Comparer)** ou cliquez sur le chiffre qui se trouve sous **Apps Seen (Applications vues)**.




Pour les règles que vous voyez sous **Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer (Optimiseur de politique)** > **No App Specified (Aucune application spécifiée)** et **Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer (Optimiseur de politique)** > **Unused Apps (Applications inutilisées)**, le fait de cliquer sur **Compare (Comparer)** ou le nombre de **Apps Seen (Applications vues)** fait apparaître **Applications & Usage (Applications et utilisation)**, qui vous donne un aperçu des applications vues dans la règle et la capacité de les trier. **Applications & Usage (Applications et utilisation)** vous permet également de Migration des règles de sécurité basées sur le port vers des règles de politique de sécurité basées sur App-ID et de supprimer les applications inutilisées des règles.




Vous pouvez trier les applications vues dans la règle en utilisant les six statistiques des **Apps Seen (Applications vues)** (**Apps Seen [Applications vues]** n'est pas mis à jour en temps réel ; il faut attendre au moins une heure pour sa mise à jour, selon le volume de trafic et le nombre de règles).

- **Applications** : noms des applications présentés en ordre alphabétique. Si vous configurez des ports spécifiques ou des plages de ports pour le service d'une règle (le service ne peut être défini sur **any [indifférent]**), et qu'il y a des ports standard (par défaut de l'application), et que les ports configurés ne correspondent pas aux ports par défaut de l'application, vous constatez alors qu'un icône d'avertissement jaune en forme de triangle apparaît au regard de l'application.
- **Subcategory (Sous-catégorie)** : en ordre alphabétique en fonction de la sous-catégorie d'application, tirée des métadonnées du contenu des applications.
- **Risk (Risque)** : selon la cote de risque de l'application.
- **First Seen (Première apparition)** : le premier jour où l'application a été vue dans la règle. La résolution de l'horodatage affiche le jour uniquement (pas l'heure).
- **Last Seen (Dernière apparition)** : le dernier jour où l'application a été vue dans la règle. La résolution de l'horodatage affiche le jour uniquement (pas l'heure).
- **Traffic (30 days) [Trafic (30 jours)]** : le trafic en octets qui a correspondu à la règle au cours des 30 derniers jours est la méthode de tri par défaut.

Définissez la **Timeframe (Période de temps)** pour afficher les statistiques d'une période de temps donnée : **Anytime (n'importe quand)**, les **Past 7 days (7 derniers jours)**, les **Past 15 days (15 derniers jours)** ou les **Past 30 days (30 derniers jours)**.

***Traffic (30 days)[Trafic (30 jours)]** affiche toujours les 30 derniers jours de trafic en octet. La modification de la **Timeframe (Période de temps)** ne modifie pas la durée de la mesure en octets de **Traffic (30 days) [Trafic (30 jours)]**.*

Si vous cliquez l'en-tête de colonne, l'affichage sera ordonné. Si vous cliquez la même colonne une seconde fois, l'ordre est inversé. Par exemple, cliquez sur **Risk (Risque)** pour trier les applications dans l'ordre des applications à risque faible aux applications à risque élevé. Cliquez sur **Risk (Risque)** de nouveau pour trier les applications des applications à risque élevé aux applications à risque faible.

Le pare-feu ne signale pas les statistiques d'utilisation des applications en temps réel pour l'Optimiseur de politique, il ne remplace donc pas l'exécution des rapports.

- Le pare-feu met à jour les **Apps Allowed (Applications autorisées)**, les **Apps Seen (Applications vues)** et les applications indiquées sous **Applications & Usage (Applications et utilisation)** environ aux heures, et non pas en temps réel. S'il y a un grand volume de trafic ou un grand nombre de règle, la mise à jour pourrait prendre plus de temps. Après avoir ajouté une application à une règle, attendez au moins une heure avant de générer les journaux du trafic pour voir les informations journalisées de l'application.

  Le pare-feu met à jour les **Apps Seen (Applications vues)** environ aux heures. Cependant, s'il y a un grand volume de trafic d'applications ou un grand nombre de règle, la mise à jour pourrait prendre plus d'une heure. Après avoir ajouté une application à une règle, attendez au moins une heure avant de générer les journaux du trafic pour voir les informations journalisées de l'application.
- Le pare-feu met à jour **Days with No New Apps (Journées sans nouvelles applications)** et **First Seen (Première apparition)** et **Last Seen (Dernier apparition)** sous **Applications & Usage (Applications et utilisation)** une fois par jour, lorsqu'il est minuit sur le périphérique.
- Les règles qui comportent de grandes quantités d'applications vues peuvent prendre plus de temps à traiter les statistiques d'utilisation des applications.
- Les bases de règles de politique de sécurité qui comportent de grandes quantités de règles qui comprennent un grand nombre d'applications peuvent prendre plus de temps à traiter les statistiques d'utilisation des applications.
- Les données d'utilisation des applications des pare-feu gérés par Panorama sont visibles uniquement pour les règles que Panorama transmet aux pare-feu, et non pas pour les règles configurées localement sur les pare-feu individuels.

## Suppression des données d'utilisation des applications

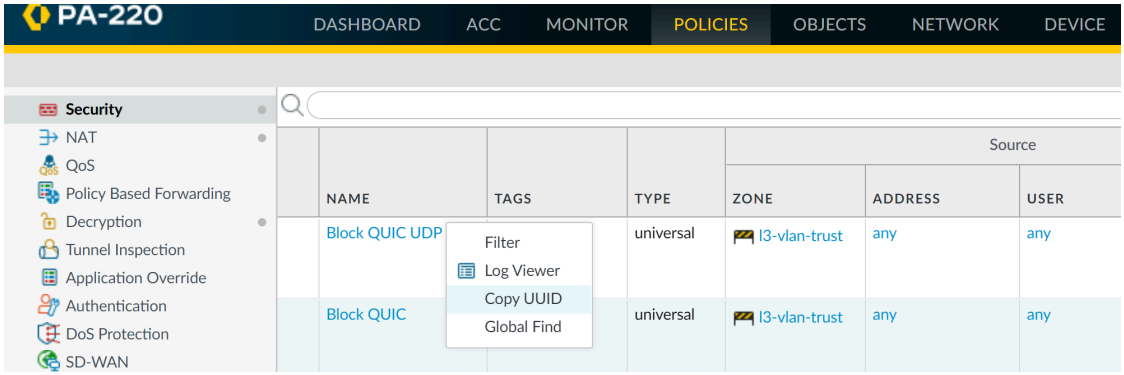
Vous pouvez utiliser une commande de la CLI pour supprimer les données d'utilisation des applications pour une règle de politique de sécurité individuelle et réinitialiser les **Apps Seen (applications vues)** et les autres données d'utilisation des applications.

**STEP 1 |** Trouvez l'UUID de la règle de politique de sécurité dont vous souhaitez supprimer les données d'utilisation des applications.

Il existe deux façons de trouver l'UUID dans l'UI :

- Sous **Policies (Politiques)** > **Security (Sécurité)**, copiez l'UUID qui figure dans la colonne **Rule UUID (UUID de la règle)**.
- Sous **Policies (Politiques)** > **Security (Sécurité)**, sélectionnez **Copy UUID (Copier l'UUID)** dans le menu déroulant **Name (Nom)** de la règle.




**STEP 2 |** Passez de l'UI à la CLI.

Utilisez l'UUID que vous avez saisi dans l'UI pour supprimer les données d'utilisation des applications :

```
admin@PA-VM>clear policy-app-usage-data ruleuuid <valeur-uuid>
```

Collez ou tapez l'UUID de la règle en tant que valeur et exécutez la commande pour supprimer les données d'utilisation des applications.

# Migration des règles de sécurité basées sur le port vers des règles de politique de sécurité basées sur App-ID

Lorsque vous passez d'un ancien pare-feu à un pare-feu Palo Alto Networks de nouvelle génération, vous héritez d'un grand nombre de règles basées sur les ports qui autorisent toutes les applications sur les ports, ce qui accroît la surface d'attaque, car n'importe quelle application peut utiliser un port ouvert. L'optimiseur de politique identifie toutes les applications vues sur une ancienne règle de politique de sécurité basée sur les ports et fournit un flux de travail facile pour la sélection des applications que vous souhaitez autoriser par cette règle. Migrez les règles basées sur les ports aux règles basée sur les applications pour réduire la surface d'attaque et activer en toute sécurité les applications sur votre réseau. Utilisez l'optimiseur de politique pour tenir à jour la base de règles au fur et à mesure que vous ajoutez de nouvelles applications.

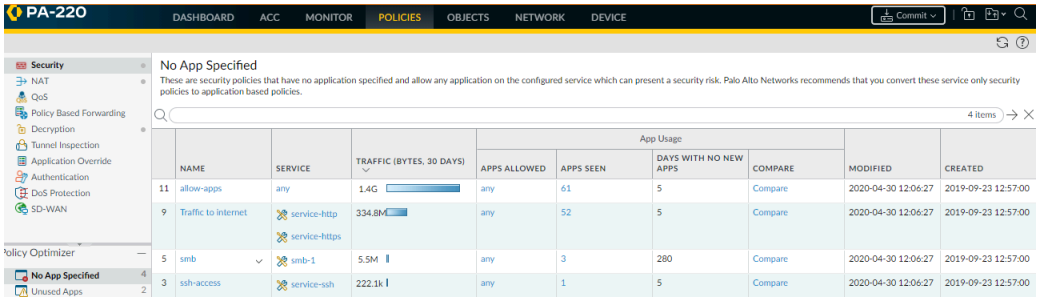
*Migrez quelques règles basées sur les ports vers des règles basées sur des applications à la fois, en suivant un ordre de priorité. Une conversion graduelle est plus sécuritaire qu'une migration d'une base de règles importantes d'une seule fois et permet de veiller plus facilement à ce que les nouvelles règles basées sur les applications contrôlent les applications nécessaires. Utilisez* ***Policy Optimizer (Optimiseur de politique)*** *pour prioriser les règles à convertir en premier.*

*Pour migrer une configuration d'un ancien pare-feu vers un périphérique Palo Alto Networks, reportez-vous à la section* Pratiques exemplaires pour la migration vers une politique basée sur les applications.

**STEP 1 |** Identifiez les règles basées sur les ports.

Les règles basées sur les ports ne comportent aucune application configurée (autorisée). **Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer (Optimiseur de politique)** > **No App Specified (Aucune application indiquée)** affiche toutes les règles basées sur les ports (**Apps Allowed (Applications autorisées)** est défini sur **any (Indifférent)**).




**STEP 2 |** Priorisez les règles basées sur les ports à convertir en premier.

**Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer (Optimiseur de politique)** > **No App Specified (Aucune application indiquée)** vous permet de trier les règles dans modifier leur ordre dans la base de règles et vous fournit d'autres informations qui vous aident à prioriser les règles à convertir selon les objectifs de votre entreprise et sa tolérance à l'égard des risques.

- **Traffic (Bytes, 30 days) (Traffic (octets, 30 jours))** : (cliquez sur cette option pour trier.) Les règles qui, ***actuellement,*** mettent en correspondance la plus grande quantité de trafic figurent au haut de la liste. C'est l'ordre de tri par défaut.
- **Apps Seen (Applications vues)** : (cliquez sur cette option pour trier.) Si vous constatez un grand nombre d'applications légitimes correspondant à une règle basée sur les ports, c'est que vous pourriez devoir remplacer cette règle par plusieurs règles basées sur les applications qui définisse strictement les applications, les utilisateurs et les sources et destinations. Par exemple, si une règle basée sur les ports contrôle le trafic de plusieurs applications pour divers groupes d'utilisateurs sur différents ensembles de périphériques, créez des règles distinctes qui associent les applications à leurs utilisateurs et périphériques légitimes afin de réduire la surface d'attaque et d'accroître la visibilité. (Si vous cliquez sur le nombre de **Apps Seen (Applications vues)** ou sur **Compare (Comparer)**, vous verrez les applications mises en correspondance avec la règle.)

  *Le pare-feu met à jour les **Apps Seen (Applications vues)** environ aux heures. Cependant, s'il y a un grand volume de trafic d'applications ou un grand nombre de règle, la mise à jour pourrait prendre plus d'une heure. Après avoir ajouté une application à une règle, attendez au moins une heure avant de générer les journaux du trafic pour voir les informations journalisées de l'application.*
- **Days with No New Apps (Journées sans nouvelles applications)** : (cliquez pour trier.) Lorsque les applications vues sur une règle basée sur les ports se stabilisent, vous pouvez être assuré que la règle est mature, que la conversion n'exclure pas accidentellement les applications légitimes et qu'aucune nouvelle application sera mise en correspondance avec la règle. Les dates de **Created (Création)** et de **Modified (Modification)** vous aident à évaluer la stabilité

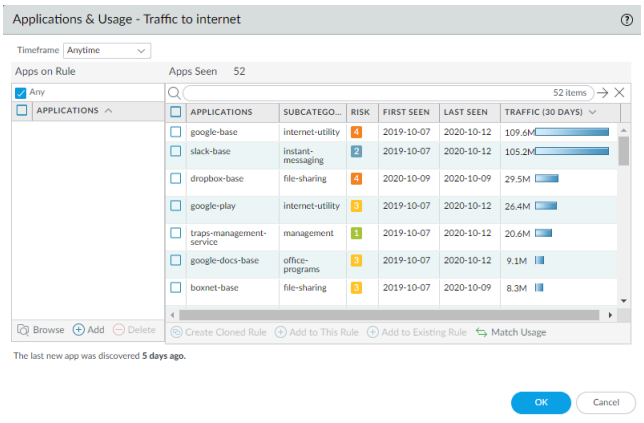
d'une règle, car les règles les plus vieilles qui n'ont pas récemment été modifiées peuvent également être plus stables.

- **Hit Count (Nombre de correspondances)** : affiche les règles qui ont été mises le plus souvent en correspondance au cours d'une période de temps sélectionnée. Vous pouvez exclure les règles pour lesquelles vous avez réinitialisé le nombre de correspondances et spécifier la période d'exclusion en jours. L'exclusion des règles dont le nombre de correspondances a récemment été réinitialisé empêche les malentendus quant aux règles qui présentent un nombre plus faible de correspondances que ce à quoi vous vous attendez, car vous n'êtes pas au cours de la réinitialisation du nombre de correspondances.

*Vous pouvez également utiliser le **Hit Count (Nombre de correspondances)** pour* Affichage de l'utilisation de la règle de politique *et permettre d'identifier et de supprimer les règles inutilisées afin de réduire les risques de sécurité et d'organiser votre base de règles.*

**STEP 3 |** Passez en revue les **Apps Seen (Applications vues)** sur les règles basées sur les ports, en commençant par les règles ayant la priorité absolue.

Sous **No Apps Specified (Aucune application spécifiée)**, cliquez sur **Compare (Comparer)** ou sur le chiffre qui figure dans **Apps Seen (Applications vues)** pour ouvrir **Applications & Usage (Applications et utilisation)**, qui indique les applications qui ont été mises en correspondance avec une règle basée sur les ports au cours d'une **Timeframe (Période de temps)** définie. Vous pouvez également consulter le **Risk (Risque)** que comporte chaque application, la date à laquelle elle a été **First Seen (Vue pour la première fois)**, la date à laquelle elle a été **Last Seen (Vue pour la dernière fois)** et la quantité de trafic constatée au cours des 30 derniers jours.




Vous pouvez vérifier les **Applications seen (Applications vues)** dans les règles basées sur les ports au cours des 7, 15 ou 30 derniers jours ou au cours de la durée de vie de la règle (**Anytime [N'importe quand]**). Lors de la migration des règles, **Anytime [N'importe quand]** fournit l'évaluation la plus exhaustive des applications qui ont été mises en correspondance avec la règle.

Vous pouvez chercher et filtrer les **Apps Seen (Applications vues)**. N'oubliez toutefois que vous devrez attendre au moins une heure pour la mise à jour des **Apps Seen (Applications vues)**. Vous pouvez également ordonner les **Apps Seen (Applications vues)** en cliquant sur les en-têtes de colonne. Par exemple, vous pouvez cliquer sur **Traffic (30 days) [Trafic (30 jours)]** pour

ramener les applications qui présentent le trafic le plus récent au haut de la liste ou cliquer sur **Subcategory (Sous-catégorie)** pour organiser les applications selon des sous-catégories.

*La granularité de la mesure des options **First Seen (Première apparition)** et **Last Seen (Dernière apparition)** est d'une journée. Ainsi, au cours de la journée où vous définissez une règle, des dates indiquées dans ces deux colonnes sont identiques. Le deuxième jour que le pare-feu voit du trafic sur une application, vous constaterez une différence de dates.*

**STEP 4 |** Clonez ou ajoutez des applications à la règle pour spécifier les applications que vous souhaitez autoriser sur la règle.

Sous **Applications & Usage (Applications et utilisation)**, convertissez une règle basée sur les ports en une règle basée sur les applications selon l'une des deux méthodes suivantes :

- **Cloner la règle** : préserve la règle basée sur les ports originale et positionne la règle basée sur les applications directement au-dessus de cette première dans la base de règles.
- **Ajouter des applications à la règle** : remplace la règle basée sur les ports originale par la nouvelle règle basée sur les applications et supprime la règle originale.

*Si vous disposez de règles basées sur les applications existantes et que vous souhaitez y faire migrer des applications à partir de règles basées sur les ports, vous pouvez Ajout d'applications à une règle existante au lieu de cloner une nouvelle règle ou de convertir la règle basée sur les ports en y ajoutant des applications.*

*Certaines applications apparaissent sur le réseau à certains intervalles, par exemple, lors d'événement trimestriels ou annuels. Il se peut que ces applications ne s'affichent pas à l'écran **Applications & Usage (Applications et utilisation)** si l'historique n'est pas suffisamment long pour en capturer la dernière activité.*

*Lorsque vous clonez une règle ou que vous ajoutez des applications à une règle, aucun autre changement n'est apporté à la règle originale. La configuration de la règle originale demeure inchangée, sauf pour les applications que vous avez ajoutées à la règle. Par exemple, si le service de la règle originale autorisait **Any (N'importe quelle)** application ou qu'il spécifiait un service particulier, vous devez modifier le service et le faire passer à **Application-Default (Par défaut de l'application)** pour restreindre les applications autorisées à leurs ports par défaut sur la nouvelle règle.*

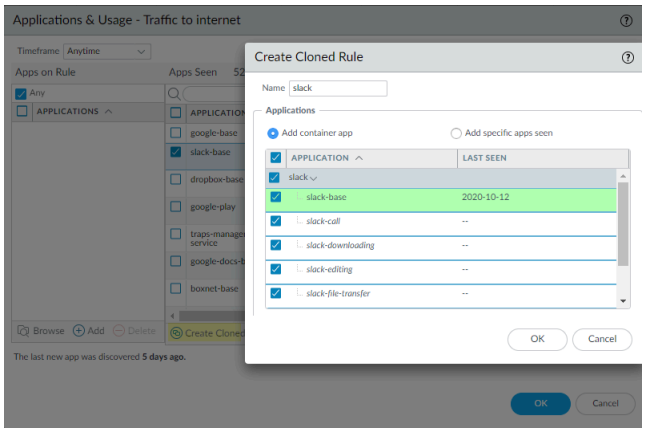
Le clonage est la méthode de migration des règles la plus sécuritaire, particulièrement lorsque **Applications & Usage (Applications et utilisation)** présente de nombreuses applications bien connues mises en correspondance avec la règle (la rubrique Cas d'utilisation de la migration du clonage de règles : Navigation Web et trafic SSL en présente un exemple). Le clonage préserve la règle basée sur les ports originale et la positionne sous la règle basée sur les applications clonée, ce qui élimine le risque de perte de disponibilité des applications, car le trafic qui ne correspond pas à la règle passe par la règle basée sur les ports. Lorsque le trafic provenant d'applications légitimes n'a pas été mis en correspondance avec la règle basée sur les ports pendant une

période de temps raisonnable, vous pouvez la supprimer pour terminer la migration de cette règle.

Pour **cloner** une règle basée sur les ports :

1. Sous **Apps Seen (Applications vues)**, cochez la case qui se trouve à côté de chaque application que vous souhaitez ajouter à la règle clonée. N'oubliez pas que la mise à jour des **Apps Seen (Applications vues)** prend au moins une heure.
2. Cliquez sur **Create Cloned Rule (Créer la règle clonée)**. Dans la boîte de dialogue **Create Cloned Rule (Créer la règle clonée)**, donnez un **Name (Nom)** à la règle clonée (« slack » dans le présent exemple) et ajoutez d'autres applications dans le même conteneur et dans les mêmes dépendances, s'il y a lieu. Par exemple, pour cloner une règle en sélectionnant l'application basée sur slack :




   Le texte en vert correspond à l'application devant être clonée. L'application de conteneur (**slack**) se trouve sur la ligne grisée. Les applications qui sont indiquées en ***italiques*** correspondent aux applications qui n'ont pas été vues dans la règle, mais qui se trouvent dans le même conteneur que l'application sélectionnée. Les applications individuelles qui ont été vues dans la règle utilisent une police normale. Toutes les applications sont incluses dans la règle de clonage par défaut (l'option **Add Container App [Ajouter l'application conteneur]**, qui ajoute toutes les applications du conteneur, est sélectionnée par défaut) afin d'empêcher l'interruption de la règle à l'avenir.
3. Si vous souhaitez autoriser toutes les applications du conteneur, laissez l'option **Add container app (Ajouter l'application conteneur)** sélectionnée. Cela permet également de créer une règle qui résistera à l'épreuve du temps, car, lorsqu'une application est ajoutée à l'application conteneur, elle est automatiquement ajoutée à la règle.

   Si vous souhaitez limiter l'accès à certaines des applications individuelles du conteneur, décochez la case qui figure à côté de chacune des applications individuelles auxquelles vous ne voulez pas que les utilisateurs accèdent. L'application conteneur est également décochée. Ainsi, si vous voulez ultérieurement autoriser de nouvelles applications du conteneur, vous avez à les ajouter individuellement.

   Si vous décochez l'application conteneur, toutes les applications sont décochées et vous sélectionnez manuellement les applications que vous voulez inclure dans la règle clonée.
4. Si les dépendances de l'application sont énumérées dans une case sous les Applications (il n'y en a aucune dans cet exemple), laissez-les cochées. Les applications que vous avez sélectionnées ont besoin de ces dépendances pour fonctionner. Les dépendances communes incluent **ssl** et **web-browsing**.

5. Cliquez sur **OK** pour ajouter la nouvelle règle basée sur les applications directement au-dessus de la règle basée sur les ports dans la base de règles.
6. **Commit (Validez)** la configuration.

Lorsque vous clonez une règle et **Commit (Valider)** la configuration, les applications que vous sélectionnez pour la règle clonée sont supprimées de la liste des **Apps Seen (Applications vues)** de la règle basée sur les ports d'origine. Par exemple, si une règle basée sur les ports comporte 16 **Apps Seen (Applications vues)** et que vous sélectionnez deux applications individuelles et une application dépendante pour la règle clonée, à l'issue du clonage, la règle basée sur les ports affiche 13 **Apps Seen (Applications vues)**, car les trois applications sélectionnées ont été supprimées de la règle basée sur les ports (16-3 = 13). La règle clonée présente les trois applications ajoutées sous **Apps on Rule (Applications d'une règle)**.

La création d'une règle clonée à l'aide d'une application de conteneur fonctionne un peu différemment. Par exemple, une règle basée sur les ports comporte 16 **Apps Seen (Applications vues)** et vous sélectionnez une application individuelle et une application conteneur pour la règle clonée. L'application conteneur comporte cinq applications individuelles et une application dépendante. À l'issue du clonage, la règle clonée présente sept **Apps on Rule (Applications d'une règle)** : l'application individuelle, les cinq applications individuelles de l'application conteneur et l'application dépendante de l'application conteneur. Cependant, dans la règle basée sur les ports d'origine, treize applications apparaissent sous **Apps Seen (Applications vues)**, car seule l'application individuelle, l'application conteneur et l'application dépendante de l'application conteneur sont supprimées de la règle basée sur les ports.

Contrairement au clonage, l'ajout d'applications à une règle basée sur les ports remplace la règle par la règle basée sur les applications qui en résulte. Il est plus simple d'ajouter des applications à une règle que de la cloner, mais c'est également plus risqué, car vous pourrez omettre par mégarde des applications qui doivent figurer dans la règle, et la règle basée sur les ports d'origine ne se trouve plus dans la base de règle pour attraper les omissions accidentelles. Cependant, lorsque vous ajoutez des applications à des règles basées sur les ports qui s'appliquent uniquement à quelques applications connues, la règle est rapidement migrée vers une règle basée sur les applications. Par exemple, dans le cas d'une règle basée sur les ports qui ne contrôle que le trafic vers le port TCP 22, la seule application légitime est SSH. Il est donc sécuritaire d'ajouter des applications à cette règle.

*L'ajout d'applications à l'aide de l'onglet **Application** de la règle de politique de sécurité ne modifie pas les **Apps Seen (Applications vues)** ou les **Apps on Rule (Applications d'une règle)**. Pour préserver l'exactitude des informations d'utilisation des applications, lors du remplacement des règles basées sur les ports par des règles basées sur les applications, ajoutez les applications en utilisant **Add to This Rule (Ajouter à cette règle)** ou **Match Usage (Faire correspondre l'utilisation)** (ou créez une règle clonée ou ajoutez des applications à une règle basée sur les applications existante) sous **Apps Seen (Applications vues)**.*

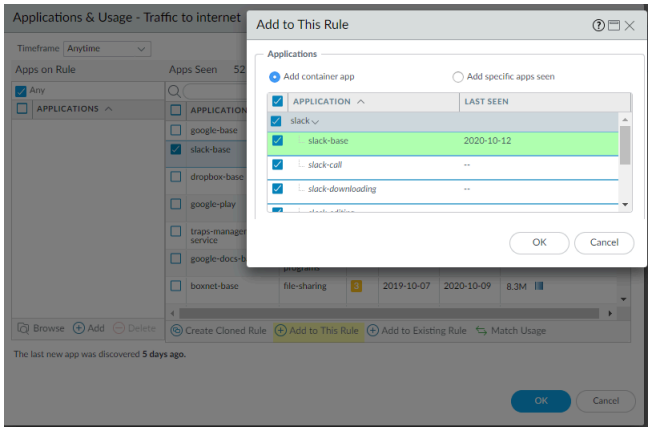
Il existe trois façons de remplacer une règle basée sur les ports par une règle basée sur les applications en ajoutant des applications (**Add to This Rule (Ajouter à cette règle)** et **Match**

**Usage (Faire correspondre l'utilisation)** sous **Apps Seen (applications vues)** et **Add (Ajouter)** sous **Apps on Rule (Applications d'une règle)**) :

- Ajoutez des applications sous **Add to This Rule (Ajouter à cette règle)**, sous **Apps Seen (applications vues)** (applications mises en correspondance avec la règle). N'oubliez pas que la mise à jour des **Apps Seen (Applications vues)** prend au moins une heure.

  1. Sélectionnez les applications parmi les **Apps Seen (Applications vues)** sur la règle.
  2. Cliquez sur **Add to This Rule (Ajouter à cette règle)**. Dans la boîte de dialogue **Add to This Rule (Ajouter à cette règle)**, ajoutez d'autres applications dans la même application conteneur et dans les mêmes dépendances, s'il y a lieu. Par exemple, pour ajouter une application basée sur slack à la règle :

     Tout comme la boîte de dialogue **Create Cloned Rule (Créer la règle clonée)**, le texte en vert qui s'affiche sous **Add to This Rule (Ajouter à cette règle)** correspond à l'application qui a été sélectionnée afin d'être ajoutée à la règle. L'application de conteneur (**slack**) se trouve sur la ligne grisée. Les applications qui sont indiquées en ***italiques*** correspondent aux applications qui n'ont pas été vues dans la règle, mais qui se trouvent dans le même conteneur que l'application sélectionnée. Les applications individuelles qui ont été vues dans la règle utilisent une police normale. Toutes les applications sont incluses dans la règle de clonage par défaut (l'option **Add Container App [Ajouter l'application conteneur]**, qui ajoute toutes les applications du conteneur, est sélectionnée par défaut) afin d'empêcher l'interruption de la règle à l'avenir.
  3. Si vous souhaitez autoriser toutes les applications du conteneur, laissez l'option **Add container app (Ajouter l'application conteneur)** sélectionnée. Cela permet également de créer une règle qui résistera à l'épreuve du temps, car, lorsqu'une application est ajoutée à l'application conteneur, elle est automatiquement ajoutée à la règle.

     Si vous souhaitez limiter l'accès à certaines des applications individuelles du conteneur, décochez la case qui figure à côté de chacune des applications individuelles auxquelles vous ne voulez pas que les utilisateurs accèdent. L'application conteneur est également décochée. Ainsi, si vous voulez ultérieurement autoriser de nouvelles applications du conteneur, vous avez à les ajouter individuellement.

     Si vous décochez l'application conteneur, toutes les applications sont décochées et vous sélectionnez manuellement les applications que vous voulez inclure dans la règle clonée.
  4. Si les dépendances de l'application sont énumérées dans une case sous les Applications (il n'y en a aucune dans cet exemple), laissez-les cochées. Les applications que vous avez sélectionnées ont besoin de ces dépendances pour fonctionner.

5. Cliquez sur **OK** pour remplacer la règle basée sur les ports par la nouvelle règle basée sur les applications.

   Lorsque vous **Add to This Rule (Ajoutez à cette règle)** et **Commit (Validez)** la configuration, les applications que vous n'avez pas ajoutées sont supprimées des **Apps Seen (Applications vues)**, car la nouvelle règle basée sur les applications ne les autorise plus. Par exemple, si une règle comporte 16 **Apps Seen (Applications vues)** et que vous **Add to This Rule (ajoutez à cette règle)** trois applications, la nouvelle règle qui en résulte n'affiche que ces trois applications ajoutées sous **Apps Seen (Applications vues)**.

   **Add to This Rule (Ajouter à cette règle)** avec une application de conteneur fonctionne un peu différemment. Par exemple, une règle basée sur les ports comporte 16 **Apps Seen (Applications vues)** et vous sélectionnez une application individuelle et une application conteneur à ajouter à la nouvelle règle. L'application conteneur comporte cinq applications individuelles et une application dépendante. À l'issue de l'ajout des applications à la règle, la nouvelle règle présente sept **Apps on Rule (Applications d'une règle)** : l'application individuelle, les cinq applications individuelles de l'application conteneur et l'application dépendante de l'application conteneur. Cependant, treize applications apparaissent sous **Apps Seen (Applications vues)**, car l'application individuelle, l'application conteneur et l'application dépendante de l'application conteneur sont supprimées de cette liste.

- Toutes les **Apps Seen (Applications vues)** dans la règle correspondent à la règle d'une seule fois, en un seul clic (**Match Usage (Faire correspondre l'utilisation)**).

  *Les règles basées sur les ports autorisent toutes les applications, les **Apps Seen (Applications vues)** peuvent donc comprendre des applications inutiles ou non sécuritaires. Utilisez **Match Usage (Faire correspondre l'utilisation)** pour convertir une règle uniquement lorsque la règle a vu un très faible nombre d'applications biens connues ayant des objectifs d'affaires légitimes. Le port TCP 22 en est un bon exemple. En effet, ce dernier ne devrait autoriser que le trafic SSH ; ainsi, si SSH est la seule application vue sur une règle basée sur les ports qui ouvre le port 22, vous pouvez activer **Match Usage (Faire correspondre l'utilisation)** en toute sécurité.*

  1. Sous **Apps Seen (Applications vues)**, cliquez sur **Match Usage (Faire correspondre l'utilisation)**. N'oubliez pas que la mise à jour des **Apps Seen (Applications vues)** prend au moins une heure. Toutes les applications sous **Apps Seen (Applications vues)** sont copiées vers **Apps on Rule (Applications d'une règle)**.
  2. Cliquez sur **OK** pour créer la nouvelle règle basée sur les applications et remplacer la règle basée sur les ports.

- Si vous savez quelles applications vous souhaitez ajouter à la règle, vous pouvez **Add (Ajouter)** des applications manuellement sous **Apps on Rule (Applications d'une règle)**. Cependant, cette méthode revient à utiliser l'onglet **Application** de la règle de politique de sécurité et ne modifie pas les **Apps Seen (Applications vues)** ou les **Apps on Rule (Applications d'une règle)**. Pour préserver l'exactitude des informations sur l'utilisation des applications, convertissez les règles en utilisant **Add to This Rule (Ajouter à cette règle)**, **Create Cloned Rule (Créer la règle clonée)** ou **Match Usage (Faire correspondre l'utilisation)** sous **Apps Seen (Applications vues)**.

  1. Sous **Apps on Rule (Applications d'une règle)**, **Add (Ajoutez)** (ou **Browse (Parcourez)**) et sélectionnez les applications à ajouter à la règle. Cela revient à ajouter les applications à l'onglet **Application**.

2. Cliquez sur **OK** pour ajouter les applications à la règle et pour remplacer la règle basée sur les ports par la nouvelle règle basée sur les applications.

   *Comme cette méthode est identique à l'ajout d'applications au moyen de l'onglet **Application**, la boîte de dialogue permettant l'ajout des dépendances d'applications ne s'affiche pas.*

**STEP 5 |** Définissez le **Service** de chaque règle basée sur des applications sur **application-default (Par défaut de l'application)**.

*Si, en raison des besoins d'affaires, vous devez autoriser des applications (par exemple, des applications personnalisées internes) sur des ports non standard entre des clients et des serveurs donnés, restreignez l'exception uniquement à l'application, aux sources et aux destinations requises. Envisagez de réécrire les applications personnalisées afin qu'elles utilisent leur port par défaut.*

**STEP 6 |** **Commit (Validez)** la configuration.

**STEP 7 |** Surveillez les règles.

- **Règles clonées :** Surveillez la règle basée sur les ports d'origine pour veiller à ce que la règle basée sur les applications mettent en correspondance le trafic souhaité. Si les applications que vous souhaitez autoriser correspondent à la règle basée sur les ports, ajoutez-les à la règle basée sur les applications ou clonez une autre règle basée sur les applications pour elles. Lorsque, depuis un certain temps, la règle basée sur les ports n'est mise en correspondance qu'avec des applications que vous ne voulez pas autoriser sur votre réseau, la règle clonée est robuste (elle attrape tout le trafic applicatif que vous souhaitez contrôler) et vous pouvez la supprimer en toute sécurité.
- **Règles comportant des applications ajoutées** : comme vous ne convertissez que des règles basées sur les ports qui comportent qu'un très faible nombre d'applications bien connues directement en des règles basées sur les applications, dans la plus des cas, la règle est solide dès le départ. Surveillez la règle convertie pour voir si le trafic attendu correspond à la règle. S'il y a moins de trafic que prévu, il se peut que la règle n'autorise pas toutes les applications nécessaires. S'il y a plus de trafic que prévu, il se peut que la règle autorise du trafic non souhaité. Soyez à l'écoute des commentaires des utilisateurs : si les utilisateurs n'arrivent pas à accéder aux applications dont ils ont besoin à des fins d'affaires, il se peut que la règle (ou une autre règle) soit trop stricte.

## Cas d'utilisation de la migration du clonage de règles : Navigation Web et trafic SSL

Une règle basée sur les ports qui autorise l'accès Web sur les ports TCP 80 (navigation Web HTTP) et 443 (SSL HTTPS) ne procure aucun contrôle sur les applications qui utilisent ces ports ouverts. Il existe de nombreuses applications Web. Une règle générale qui autorise le trafic Web autorise donc des milliers d'applications, dont de nombreuses applications que vous ne voulez pas autoriser sur votre réseau.

Ce cas d'utilisation illustre la migration d'une politique basée sur les ports qui autorise toutes les applications Web vers une politique basée sur les applications qui n'autorisent que les applications souhaitées. C'est donc dire que vous pouvez activer en toute sécurité les applications que vous

choisissez d'autoriser. Pour les règles qui sont associées à un grand nombre d'applications, il est plus sécuritaire de cloner la règle basée sur les ports, puis d'ajouter les applications à la règle, car cet ajout remplace la règle basée sur les ports. Ainsi, si, par mégarde, vous omettez d'ajouter une application essentielle, vous affecter la disponibilité de l'application. Et si vous **Match Usage (Faites correspondre l'utilisation)**, qui remplace également la règle basée sur les ports, vous autorisez toutes les applications que la règle a vues, ce qui pourrait s'avérer dangereux, particulièrement pour le trafic de navigation Web.

Le clonage de la règle conserve la règle basée sur les ports d'origine et positionne la règle basée sur les applications directement au-dessus de cette première dans la base de règles, ce qui vous permet de surveiller les règles. Le clonage vous permet également de diviser les règles qui voient beaucoup d'applications différentes (comme une règle de trafic Web basée sur les ports) en plusieurs règles basées sur les applications, ce qui vous permet de traiter différents groupes d'applications différemment. Lorsque vous êtes certain d'autoriser toutes les applications que vous devez autoriser dans la règle (ou les règles) clonée(s), vous pouvez supprimer la règle basée sur les ports.

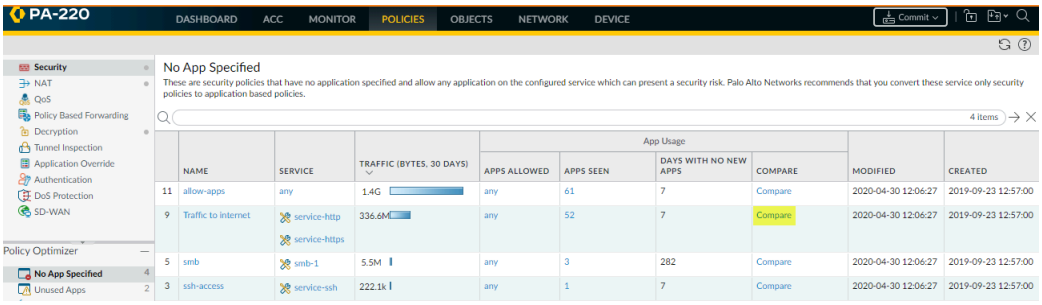
Cet exemple clone une règle de trafic web basée sur le port pour créer une règle basée sur l'application pour le trafic de partage de fichiers basé sur le web (un sous-ensemble du trafic d'application vu sur la règle basée sur le port).

*Cet exemple ne s'applique pas à l'utilisation de* New App Viewer (Nouvelle visionneuse d'applications) *pour cloner des applications App-ID Cloud Engine (ACE) (consultez la documentation* ACE *pour obtenir des exemples de procédure à prendre) ; ACE nécessite une licence* SaaS Security Inline.

**STEP 1 |** Rendez-vous à **Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer (Optimiseur de politique)** > **No App Specified (Aucune application spécifiée)** pour afficher les règles basées sur les ports.

**STEP 2 |** Cliquez sur **Compare (Comparer)** pour la règle que vous souhaitez migrer.

Dans cet exemple, la règle basée sur les ports qui autorise l'accès Web est nommée Trafic vers Internet.

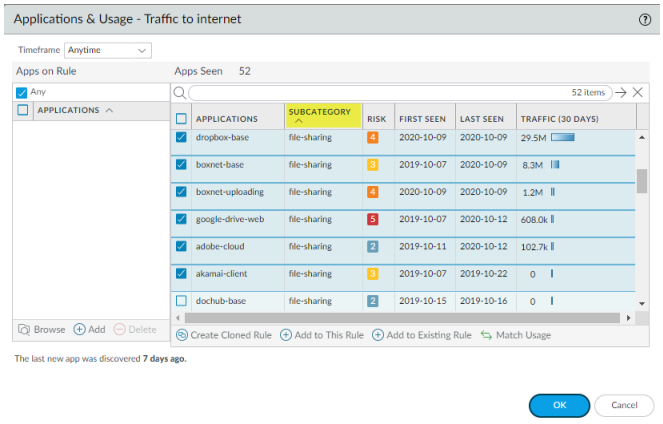


**STEP 3 |** Utilisez les options de tri pour passer en revue les **Apps Seen (Applications vues)** et sélectionner celles que vous voulez autoriser.

> *Le nombre de **Apps Seen (Applications vues)** est mis à jour environ aux heures. Ainsi, si vous ne voyez pas le nombre d'application attendu, effectuez une nouvelle vérification après environ une heure. Selon la charge du pare-feu, la mise à jour de ces champs pourrait prendre plus d'une heure.*

Par exemple, cliquez sur **Subcategory (Sous-catégorie)** pour trier les applications, faites défiler jusqu'à la sous-catégorie de partage de fichiers, puis sélectionnez les applications que vous souhaitez autoriser. Vous pouvez également filtrer (rechercher) les applications de partage de fichiers.

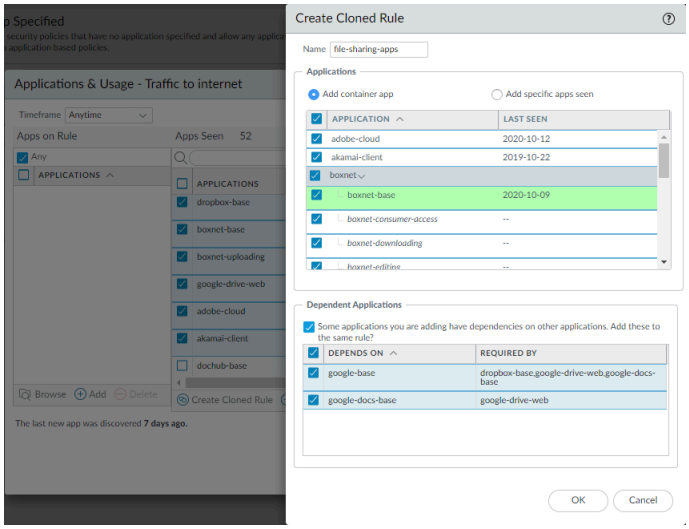



**STEP 4 |** Cliquez sur **Create Cloned Rule (Créer une règle clonée)** et **Name (Nommez)** la règle clonée (file-sharing-apps dans cet exemple).

**Create Cloned Rule (Créer la règle clonée)** montre les applications sélectionnées ombragées en vert, les applications conteneur ombragées en gris, les applications individuelles du conteneur qui n'ont pas été vues dans la règle en ***italique*** et les applications individuelles qui ont été vues

dans la règle dans une police normale. En faisant défiler les **Applications**, vous verrez toutes les applications conteneur et leurs applications individuelles.




**Create Cloned Rule (Créer la règle clonée)** montre également les applications dépendantes pour les applications sélectionnées. Dans cet exemple, certaines des applications sélectionnées nécessitent (**Required By**) l'exécution des applications google-base et google-docs-base.

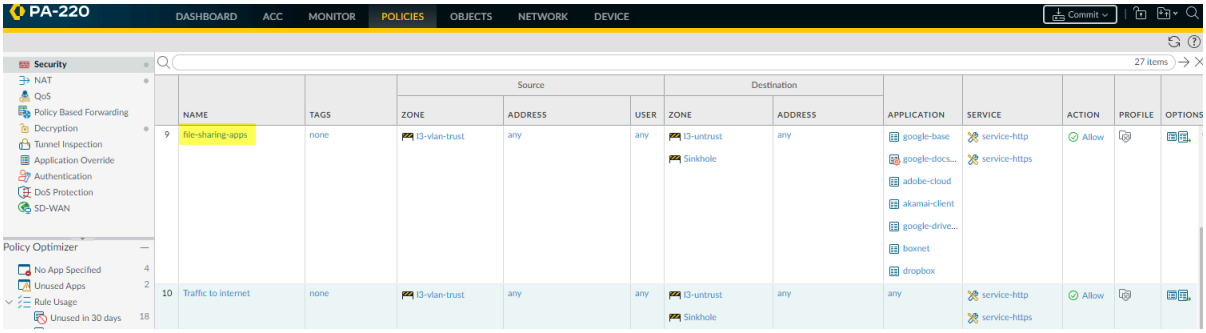
**STEP 5 |** Sélectionnez les applications à inclure dans la règle clonée.

Décochez la case correspondant aux applications que vous ne souhaitez pas inclure ; la case de l'application conteneur est aussi décochée. Si vous n'incluez pas l'application conteneur, lorsque de nouvelles applications sont ajoutées au conteneur, elles ne sont pas automatiquement ajoutées à la règle.

Si vous décochez l'application conteneur, toutes les applications individuelles du conteneur sont décochées et vous devez sélectionner manuellement les applications que vous voulez ajouter.

**STEP 6 |** Cliquez sur **OK** pour créer la règle clonée.

**STEP 7 |** Sous **Policies (Politiques)** > **Security (Sécurité)**, la règle clonée (file-sharing-apps) est insérée dans la base de règle au-dessus de la règle basée sur les ports d'origine (Trafic vers Internet).




**STEP 8 |** Cliquez sur le nom de la règle pour modifier la règle clonée, qui hérite des propriétés de la règle basée sur les ports d'origine.

**STEP 9 |** Dans l'onglet **Service/URL Category (Catégorie de service/d'URL)**, supprimez service-http et service-https sous **Service**.

Le **Service** passe alors à **application-default (Par défaut de l'application)**, qui empêche les applications d'utiliser les ports non standard et réduit davantage la surface d'attaque.

*Si, en raison des besoins d'affaires, vous devez autoriser des applications (par exemple, des applications personnalisées internes) sur des ports non standard entre des clients et des serveurs donnés, restreignez l'exception uniquement à l'application, aux sources et aux destinations requises. Envisagez de réécrire les applications personnalisées afin qu'elles utilisent leur port par défaut.*

**STEP 10 |** Aux onglets **Source**, **User (Utilisateur)** et **Destination**, renforcez la règle pour qu'elle s'applique uniquement aux bons utilisateurs uniquement dans les bons emplacements (zones, sous-réseaux).

Par exemple, vous pouvez décider de limiter l'activité de partage de fichiers sur le web aux seuls groupes d'utilisateurs qui ont des raisons professionnelles de partager des fichiers sur le web.

**STEP 11 |** Cliquez sur **OK**.

**STEP 12 |** **Commit (Validez)** la configuration.

**STEP 13 |** Répétez le processus pour d'autres catégories d'applications qui figurent dans la règle d'accès Web basée sur les ports jusqu'à ce que les règles basées sur les applications autorisent uniquement les applications que vous souhaitez autoriser sur votre réseau.

Lorsque le trafic que vous souhaitez autoriser cesse de correspondre à la règle basée sur les ports pendant une période de temps suffisamment longue pour que vous vous sentiez à l'aise que la règle basée sur les ports n'est plus nécessaire, vous pouvez supprimer la règle basée sur les ports de la base de règles.

## Ajout d'applications à une règle existante

Dans certains cas, il se peut que vous souhaitiez ajouter des applications apprises (vues) dans une règle basée sur les ports à une règle qui existe déjà. Par exemple, il se peut qu'un administrateur crée une règle basée sur les applications clonée pour les applications web d'entreprise générales à partir d'une règle basée sur les ports qui autorise l'accès à Internet (règle de port 80/443). Plus tard, l'administrateur constate que la règle d'accès à Internet basé sur le port règle a vu un plus grand nombre d'applications d'entreprise générales et veut ajouter une partie ou la totalité d'entre eux à la règle basée sur les applications clonée (le clonage d'une autre règle basée sur les applications pour le même type d'application créerait une règle inutile et compliquerait la base de règles).

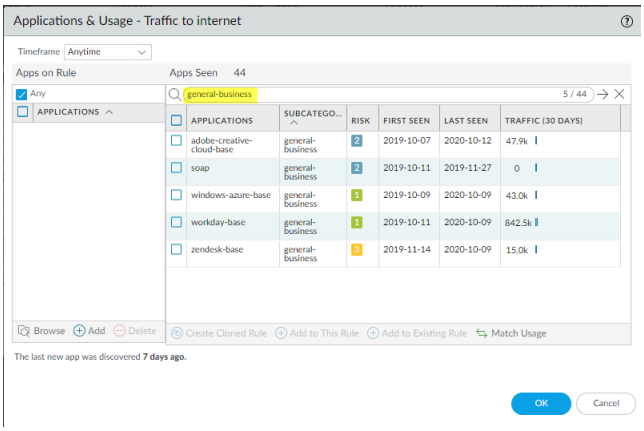
Cet exemple suppose qu'une règle de politique de sécurité basée sur les applications pour contrôler le trafic d'entreprise général existe déjà ou a été clonée à partir d'une règle d'accès à Internet basée sur le port, de manière similaire à Cas d'utilisation de la migration du clonage de règles : Navigation Web et trafic SSL. Dans cet exemple, nous avons cloné une règle basée sur les applications à partir de la règle d'accès à l'internet basée sur les ports et avons changé le service de la nouvelle règle en application par défaut pour empêcher les applications web d'utiliser des ports non standard.

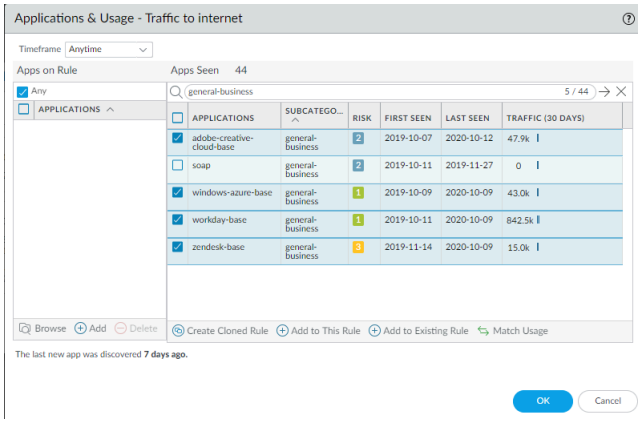
*En plus d'ajouter des applications à une règle basée sur les applications existantes, vous pouvez ajouter des applications à une règle basée sur les ports existants. Cela permet de convertir la règle basée sur le port en une règle basée sur l'application pour les applications que vous ajoutez à la règle. Si vous faites cela, rendez-vous à la règle et modifiez le Service sur application-default (par défaut de l'application) pour empêcher les applications d'utiliser des ports non standards (le Service configuré sur la règle peut également ne pas correspondre à l'application).*

*Cet exemple ne s'applique pas à l'utilisation de New App Viewer (nouvelle visionneuse d'applications) pour ajouter des applications App-ID Cloud Engine (ACE) à une règle existante (consultez la documentation ACE pour obtenir des exemples sur la façon de procéder) ; ACE nécessite une licence SaaS Security Inline.*

**STEP 1 |** Vous vérifiez la règle d'accès à l'internet basée sur le port et vous découvrez que la règle a vu des applications commerciales générales et que vous devez en autoriser certaines à des fins commerciales.

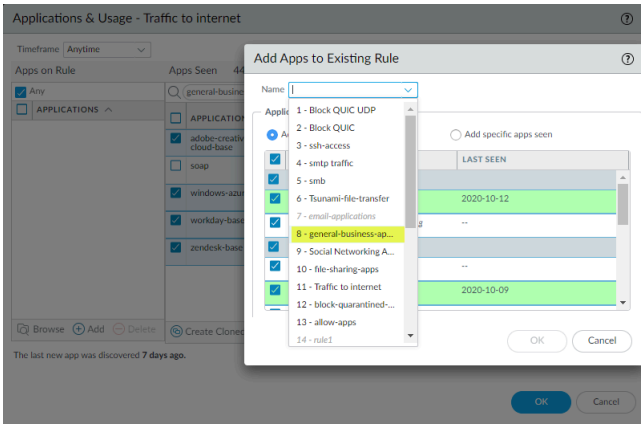



**STEP 2 |** Sélectionnez les applications d'entreprise générale que vous souhaitez ajouter à la règle existante.



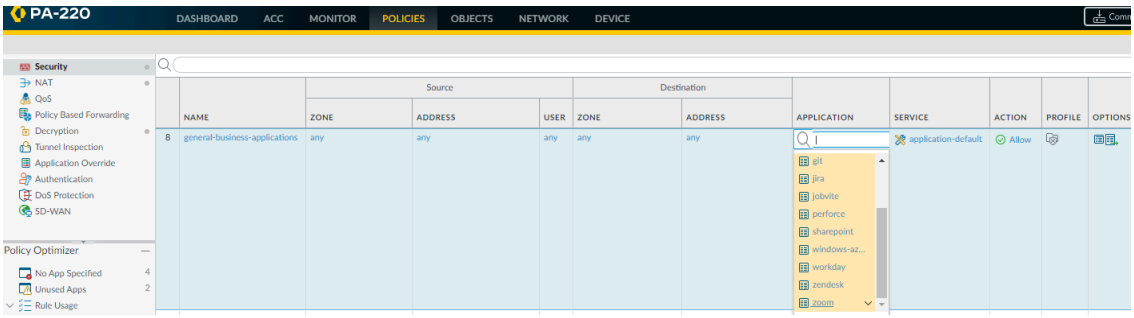
**STEP 3 |** Cliquez sur **Add to Existing Rule (Ajouter à la règle existante)** et sélectionnez le **Name (Nom)** de la règle à laquelle vous voulez ajouter les applications ; dans cet exemple, il s'agit de **general-business-apps (applications d'entreprise générale)**.




**STEP 4 |** Cliquez sur **OK** dans **Add Apps to Existing Rule (Ajouter les applications à la règle existante)** pour ajouter les applications sélectionnées à la règle **general-business-applications (applications d'entreprise générale)**.

**STEP 5 |** Cliquez sur **OK** dans **Applications & Usage (Applications et utilisation)**.

**STEP 6 |** La règle mise à jour contrôle désormais les applications d'origine sur la règle et les applications que vous venez d'ajouter.




# Identification des règles de politique de sécurité comportant des applications non utilisées

Si vous disposez de règles de politique de sécurité basées sur les applications qui autorisent un grand nombre d'applications, vous pouvez supprimer les applications inutilisées (applications jamais vues dans les règles) pour renforcer ces règles afin qu'elles n'autorisent que les applications réellement vues dans le trafic qui correspond à la règle. Il est recommandé d'identifier les applications non utilisées et de les supprimer de la politique de sécurité afin de renforcer votre position en matière de sécurité en réduisant la surface d'attaque.

**STEP 1 |** Identifiez les règles de politique de sécurité qui comportent des applications non utilisées.

**Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer (Optimisateur de politique)** > **Unused Apps (Applications inutilisées)** affiche toutes les règles basées sur des applications qui sont configurées avec des applications qui ne correspondent pas à (ont été vues sur) la règle. Cela signifie que ces règles autorisent des applications que vous ne pouvez pas utiliser dans votre

réseau (ou qu'une autre règle fait de l'ombre à la règle, de sorte que le trafic que vous pensez correspondre à la règle correspond à une règle antérieure dans la base de règles).

*Le nombre de **Apps Allowed (Applications autorisées)** et de **Apps Seen (Applications vues)** est mis à jour environ aux heures. Ainsi, si vous configurez des applications dans une règle et que vous ne voyez pas le nombre de **Apps Allowed (Applications autorisées)** attendus, effectuez une nouvelle vérification après environ une heure. Selon la charge du pare-feu, la mise à jour de ces champs pourrait prendre plus d'une heure.*

**STEP 2 |** Priorisez les règles qui comportent des applications non utilisées à modifier en premier.

**Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer (Optimiseur de politique)** > **Unused Apps (Applications inutilisées)** vous permet de trier les règles dans modifier leur ordre dans la base de règles et vous fournit d'autres informations qui vous aident à prioriser les règles à nettoyer selon les objectifs de votre entreprise et sa tolérance à l'égard des risques.

- La différence entre les **Apps Allowed (Applications autorisées)** (le nombre d'applications autorisées sur la liste d'autorisation) et les **Apps Seen (Applications vues)** (le nombre d'applications autorisées qui ont été vues sur la règle) correspond au nombre d'applications configurées sur chaque règle, mais pas encore vues sur la règle et indique dans quelle mesure la règle est surdimensionnée. Cliquez sur **Apps Allowed (Applications autorisées)** pour trier en fonction du nombre d'applications autorisés dans une règle et cliquez sur **Apps Seen (Applications vues)** pour trier en fonction du nombre d'applications réellement vues sur une règle.
- **Days with No New Apps (Journée sans nouvelles applications)** (cliquez pour trier) vous montre le nombre de jours depuis la dernière correspondance d'une nouvelle application avec la règle. Cette option indique la probabilité qu'une règle soit arrivée à maturité et qu'elle voit plus d'applications qui n'ont jamais été vues. Plus l'on compte de **Days with No New Apps (Journée sans nouvelles applications)**, moins il est probable que de nouvelles applications seront mises en correspondance avec la règle et plus il est probable que vous connaissiez toutes les applications que la règle autorise.
- Les dates de **Created (Création)** et de **Modified (Modification)** aident également à déterminer si une règle est suffisamment mature pour comprendre si des applications jamais vues sur la règle peuvent être vues ultérieurement ou si la règle a vu toutes les applications qui doivent correspondre à la règle. Plus de temps s'est écoulé depuis la **Modified (Modification)** d'une règle, plus il est probable que la règle soit mature. (Si les dates de **Created (Création)** et de **Modified (Modification)** sont identiques, c'est que la règle n'a pas encore été modifiée.)
- **Hit Count (Nombre de correspondances)** : affiche les règles qui ont été mises le plus souvent en correspondance au cours d'une période de temps sélectionnée. Vous pouvez exclure les règles pour lesquelles vous avez réinitialisé le nombre de correspondances et spécifier la période d'exclusion en jours. L'exclusion des règles dont le nombre de correspondances a récemment été réinitialisé empêche les malentendus quant aux règles qui présentent un nombre plus faible de correspondances que ce à quoi vous vous attendez, car vous n'êtes pas au cours de la réinitialisation du nombre de correspondances.

  *Vous pouvez également utiliser le **Hit Count (nombre de correspondances)** pour* Affichage de l'utilisation de la règle de politique.

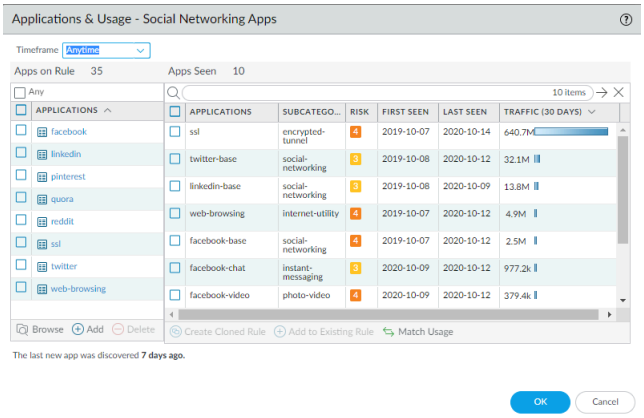
Vous pouvez également cliquer sur **Traffic (Bytes, 30 days) [Trafic (octets, 30 jours)]** pour trier en fonction du trafic qu'une règle a vu au cours des 30 derniers jours). Utilisez ces informations

pour prioriser les règles à convertir en premier. Par exemple, vous pouvez prioriser les règles qui présentent le plus grand écart entre les **Apps Allowed (Applications autorisées)** et les **Apps Seen (Applications vues)** et qui possèdent également le plus grand nombre de **Days with No New Apps (Journées sans nouvelles applications)**, car ces règles ont le plus grand nombre d'applications inutilisées et sont les plus matures.

**STEP 3 |** Passez en revue les **Apps Seen (Applications vues)** sur la règle.

Sous **Unused Apps (Applications inutilisées)**, cliquez sur **Compare (Comparer)** ou sur le chiffre indiqué dans la colonne **Apps Seen (Applications vues)** pour ouvrir **Applications & Usage (Applications et utilisation)**, qui présente les applications configurées dans la règle (**Apps on Rule [Applications d'une règle]**) et les **Apps Seen (Applications vues)** dans la règle.

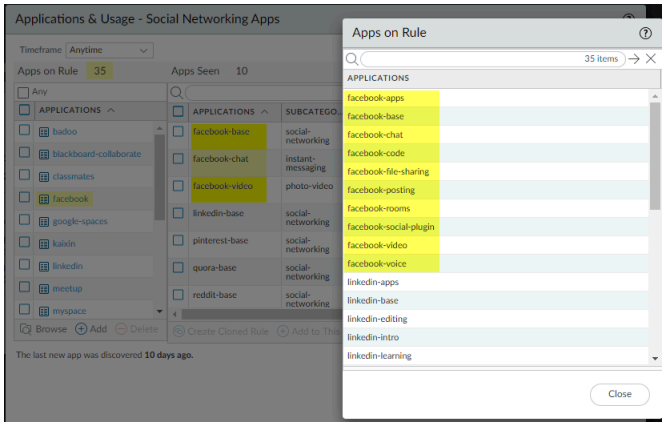



- Le chiffre indiqué à côté de **Apps Seen (Applications vues)** (10, dans l'exemple) est le nombre d'applications qui correspondent à la règle. N'oubliez pas que la mise à jour des **Apps Seen (Applications vues)** sur le pare-feu prend au moins une heure.
- Le chiffre indiqué à côté de **Apps on Rule (Applications d'une règle)** (35, dans cet exemple) correspond au nombre d'applications qui sont configurées dans la règle, qui est calculé en comptant chaque application d'une application conteneur (mais pas l'application conteneur elle-même—si vous configurez une application conteneur sur la règle, la règle autorise les applications individuelles de l'application conteneur). Comme la liste **Applications** n'affiche que les applications que vous configurez manuellement sur la règle, lorsque vous configurez une application conteneur sur une règle, **Applications** n'affiche que l'application conteneur et non toutes les applications individuelles du conteneur (sauf si vous configurez également manuellement les applications individuelles sur la règle). Pour cette raison, le nombre de **Apps on Rule (Applications d'une règle)** peut différer du nombre d'applications figurant dans la liste **Applications**.
- Cliquez sur le numéro qui est indiqué à côté de **Apps on Rule (Applications d'une règle)** pour voir toutes les applications individuelles de la règle.

  Cet exemple de règle a 10 **Apps Seen (Applications vues)** (applications qui correspondent à la règle) mais permet 35 **Apps on Rule (Applications d'une règle)**. L'application conteneur **facebook** est configurée sur la règle et la règle voit le trafic des applications individuelles facebook-base, facebook-chat, et facebook-video (**Apps Seen (Applications vues)**). Lorsque vous cliquez sur le numéro **Apps on Rule (Applications d'une règle)**, la boîte de dialogue **Apps**

**on Rule (Applications d'une règle)** affiche les demandes individuelles autorisées, mais pas l'application conteneur elle-même.




Vous ne pouvez ajouter ou supprimer d'applications de la boîte de dialogue contextuelle.

Comparez les **Apps Seen (Applications vues)** dans la règle avec les **Apps on Rule (Applications d'une règle)**. Si une application dans la règle n'est pas utilisée (vous ne voyez pas l'application ou vous ne voyez pas les applications dans un conteneur autorisé dans **Apps Seen (Applications vues)**), envisagez de retirer l'application de la règle pour réduire la surface d'attaque. Tenez compte des applications qui sont utilisées périodiquement, comme les événements trimestriels ou annuels, qui pourraient vous sembler inutilisées si vous n'examinez pas l'utilisation des applications sur une longue période de temps. **Timeframe (Période de temps)** vous permet de sélectionner la période de temps à appliquer aux **Apps Seen (Applications vues)** dans la règle. Sélectionnez **Anytime (En tout temps)** pour voir chaque application vue au cours de la durée de vie de la règle. Selon la date de **Created (Création)** ou de **Modified (Modification)** indiquée dans la boîte de dialogue **No App Specified (Aucune application spécifiée)** et la durée entre les événements périodiques, il se peut que la configuration de la règle est trop récente pour que vous puissiez voir toutes les applications utilisées périodiquement.

**STEP 4 |** Supprimez les applications inutilisées de la règle.

**Delete (Supprimez)** (ou **Add [Ajoutez]**) des applications sous **Apps on Rule (Applications d'une règle)** pour supprimer (ou ajouter) des applications manuellement, ou **Match Usage (Faites correspondre l'utilisation)** pour ajouter les **Apps Seen (Applications vues)** dans la règle et supprimer les applications pour lesquelles aucun trafic de correspondance a été vu dans la règle, d'un seul clic.

Pour supprimer manuellement les applications d'une règle, sélectionnez les applications dans **Apps on Rule (Applications d'une règle)**, puis **Delete (Supprimer)**. Assurez-vous que les applications ne sont pas requises pour les événements périodiques avant de les supprimer de la

règle. (Vous pouvez également ajouter ou supprimer des applications dans l'onglet **Application** de la règle de politique de sécurité.)

**Match Usage (Faire correspondre l'utilisation)** fait passer les **Apps Seen (Applications vues)** dans la règle à **Apps on Rule (Applications d'une règle)** et supprime toute les applications inutilisées de la règle.

*Vous pouvez cloner des règles sous **Policies (Politiques) > Security (Sécurité)** et sous **No App Specified (Aucune application spécifiée)** pour* Migration des règles de sécurité basées sur le port vers des règles de politique de sécurité basées sur App-ID*. Vous ne pouvez cloner de règle sous **Unused Apps (Applications inutilisées)**.*

**STEP 5 |** **Commit (Validez)** la configuration.

**STEP 6 |** Surveillez les règles mises à jour et soyez à l'écoute des commentaires des utilisateurs pour vous assurer que les règles mises à jour autorisent les applications que vous souhaitez autoriser et qu'elles ne bloquent pas, par mégarde, les applications utilisées périodiquement.

*Le nombre de **Apps Allowed (Applications autorisées)** et de **Apps Seen (Applications vues)** est mis à jour environ aux heures. Après que vous avez supprimé toutes les applications inutilisées d'une règle, la règle demeure présente sous **Policies (Politiques) > Security (Sécurité) > Policy Optimzer (Optimiseur de politique) > Unused Apps (Applications inutilisées)** jusqu'à ce que le pare-feu mette l'affichage à jour. Lorsque le pare-feu met l'affichage à jour et que le nombre de **Apps Allowed (Applications autorisées)** est identique au nombre de **Apps Seen (Applications vues)**, la règle ne s'affiche plus à l'écran **Unused Apps (Applications inutilisées)**. Cependant, selon la charge du pare-feu, la mise à jour de ces champs pourrait prendre plus d'une heure.*

## Haute disponibilité pour les statistiques d'utilisation des applications

Lorsque vous configurez deux pare-feu en tant que paire High Availability (haute disponibilité - HA), les statistiques d'utilisation des applications sont locales au pare-feu qui génère les journaux de trafic pour l'application. L'endroit où vous pouvez afficher les statistiques d'utilisation des applcations dépend également de la configuration HA :

- **Active/Passive** : le périphérique actif génère les statistiques d'utilisation des applications. Si un périphérique passif n'a vu aucun trafic utilisateur, seul le périphérique actif affiche les statistiques d'utilisation des applications. Si un périphérique passif a vu du trafic, le périphérique passif affiche uniquement les statistiques d'utilisation des applications du trafic qu'il a vu.

  Lors d'un basculement, les statistiques d'utilisation des applications se fondent uniquement sur les journaux du trafic générés sur le périphérique nouvellement actif (le périphérique qui était passif avant le basculement).
- **Active/Active** : le périphérique propriétaire d'une session génère les journaux du trafic pour cette session. Les statistiques d'utilisation des applications d'une session ne sont disponibles que sur le périphérique propriétaire de la session. Si un périphérique actif est propriétaire d'une session, l'autre périphérique actif n'affiche pas les statistiques d'utilisation des applications.

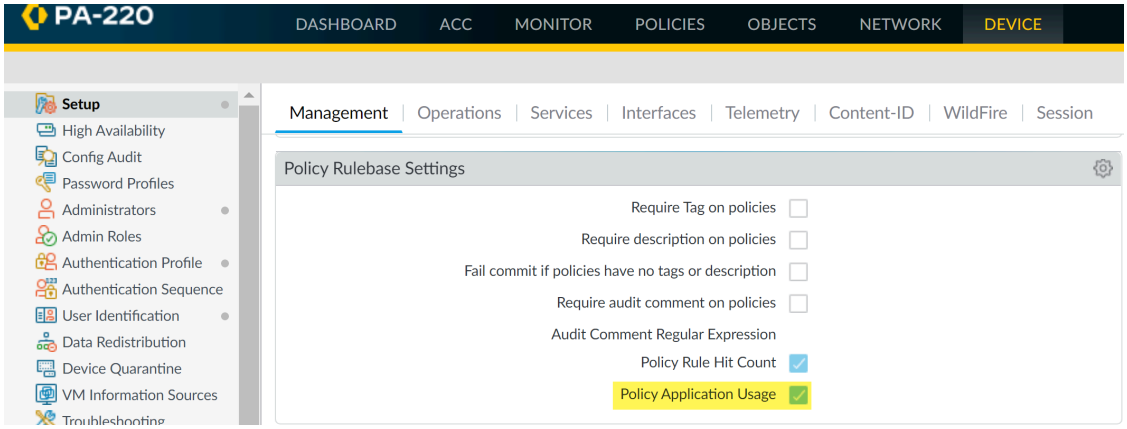
 

# Désactivation de l'optimiseur de politique

L'optimiseur de politique est activé par défaut. L'optimiseur de politique procure de nombreuses capacités qui peuvent faciliter la Migration des règles de sécurité basées sur le port vers des règles de politique de sécurité basées sur App-ID et l'Identification des règles de politique de sécurité comportant des applications non utilisées et supprimer les applications inutilisées des règles. Cependant, si vous souhaitez désactiver cette fonctionnalité, vous pouvez le faire.

**STEP 1 |** Rendez-vous à **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **Policy Rulebase Settings (Paramètres de la base de règles de politique)**.

**STEP 2 |** Cochez la case **Policy Application Usage (Utilisation de l'application de la politique)** pour activer la fonctionnalité et décochez cette case pour la désactiver.



# App-ID Cloud Engine

L'App-ID Cloud Engine (ACE) est un nouveau service qui permet au pare-feu ou à Panorama de télécharger des App-ID à partir du cloud pour les applications qui n'ont pas d'App-ID prédéfinis spécifiques de l'équipe de contenu de Palo Alto Networks. Ce sont les applications que le pare-feu identifie comme trafic ssl, de navigation Web, inconnu-tcp ou inconnu-udp. Utilisez les ID d'application ACE dans les règles de politique de sécurité pour obtenir une visibilité et contrôler ces applications et utilisez Policy Optimizer (optimiseur de politique) pour ajouter et gérer des applications dans la Politique de sécurité. Vous ne pouvez pas utiliser les ID d'application ACE dans d'autres types de règles de politique. ACE :

- Augmente considérablement le nombre d'App-ID connus pour identifier et contrôler les applications. Au fur et à mesure que ACE définit de nouveaux App-ID pour les applications, ils deviennent disponibles sur le pare-feu.
- Accélère la disponibilité et la livraison de nouveaux App-ID au pare-feu.
- Accélère et peut automatiser l'ajout d'applications à la Politique de sécurité grâce à l'utilisation de Filtres d'application dans les Règles de politique de sécurité.
- Augmente considérablement la visibilité des applications précédemment identifiées comme SSL, navigation Web, inconnue-tcp ou inconnue-udp.

*ACE nécessite un abonnement* SaaS Security Inline*. Chaque appareil qui utilise ACE doit avoir un certificat de périphérique valide installé.*

*Toutes les plates-formes matérielles qui prennent en charge PAN-OS 10.1 ou une version ultérieure prennent en charge ACE et toutes les appareils sur lesquelles vous souhaitez utiliser ACE nécessitent PAN-OS 10.1 ou une version ultérieure. Panorama ne peut pas transmettre et valider des politiques ou des objets basés sur ACE sur des pare-feu sur lesquels aucune licence SaaS Security Inline n'est installée ou sur des pare-feu qui exécutent une version antérieure de PAN-OS à 10.1.*

*ACE est pris en charge dans les régions GCP des États-Unis, de l'APAC et de l'UE. La région est sélectionnée automatiquement en fonction de votre région CDL.*

*Vérifiez que le pare-feu utilise le bon FQDN Content Cloud (* ***Device (Périphérique)*** *>* ***Setup (Configuration)*** *>* ***Content-ID (ID de contenu)*** *>* ***Content Cloud Setting (Paramètre du Cloud de contenu)****) pour votre région et modifiez le FQDN si nécessaire :*

- *États-Unis—****hawkeye.services-edge.paltoaltonetworks.com***
- *UE—****eu.hawkeye.services-edge.paltoaltonetworks.com***
- *APAC—****apac.hawkeye.services-edge.paltoaltonetworks.com***

*Les données ACE, y compris les charges utiles de trafic, sont envoyées aux serveurs de la région sélectionnée. Si vous spécifiez un FQDN Content Cloud qui se trouve en dehors de votre région (par exemple, si vous êtes dans la région de l'UE mais que vous spécifiez le FQDN de la région APAC), vous pouvez enfreindre les réglementations légales et de confidentialité de votre pays ou de votre organisation.*

App-ID prédéfini avec contenu fourni fournit de nouvelles applications une fois par mois et vous devez analyser les nouveaux App-ID avant de les installer pour comprendre les modifications qu'ils peuvent apporter aux règles de politique de sécurité. La cadence mensuelle et le besoin d'analyse ralentissent l'adoption de nouveaux identifiants d'application dans la politique. Bien que Palo Alto Networks continue de fournir de nouveaux identifiants d'application via des mises à jour de contenu mensuelles que vous devez examiner, ACE améliore l'adoption de nouveaux identifiants d'application en fournissant des identifiants d'application à la demande pour les applications initialement identifiées comme l'un des quatre types suivants :

- **ssl** : le trafic SSL crypté est de loin le type de trafic réseau le plus courant, la plupart des experts affirmant qu'il dépasse 90 % du trafic total. Si vous ne déchiffrez pas ou ne pouvez pas déchiffrer ce trafic, le pare-feu ne peut souvent l'identifier qu'en tant que SSL au lieu de l'application sous-jacente réelle.
- **web-browsing (navigation Web)** : le pare-feu ne peut pas identifier spécifiquement le trafic de navigation Web non crypté, car il existe tellement d'applications que l'App-ID fourni par le contenu ne peut pas suivre le volume toujours croissant.

- **unknown-tcp** et **unknown-udp** : ce trafic peut être des applications internes ou personnalisées ou des applications externes inconnues. Il est important d'identifier ce trafic par son App-ID spécifique afin que vous puissiez prendre des décisions d'accès intelligentes et créer des Règles de politique de sécurité appropriées pour contrôler et inspecter le trafic.

ACE fournit une identification spécifique de ces applications, ce qui vous permet de les comprendre et de les contrôler de manière appropriée dans la politique.

*Les ID d'application ACE n'identifient pas d'autres types d'applications publiques et n'identifient pas les applications privées et personnalisées. Le catalogue ACE App-ID ne contient pas d'App-ID prédéfinis fournis par le contenu. Les App-ID fournis par le contenu arrivent toujours chaque mois dans les mises à jour de contenu.*

Lorsque le pare-feu rencontre du trafic SSL, de navigation Web, inconnu-tcp ou inconnu-udp, le pare-feu envoie la charge utile à ACE pour analyse. S'il existe un App-ID correspondant dans la base de données ACE, ACE renvoie l'App-ID au pare-feu demandeur. Si ACE n'a pas d'ID d'application correspondant pour le trafic, ACE envoie la charge utile au moteur Machine Learning (ML). Le moteur ML analyse la charge utile et développe le nouvel App-ID en collaboration avec l'équipe de contenu humain et supprime le trafic qui n'est pas lié aux applications. Une fois le développement terminé, le moteur ML télécharge le nouvel App-ID dans la base de données ACE, et le pare-feu demandeur (et tout autre pare-feu) peut télécharger l'App-ID et l'utiliser dans la politique de sécurité.

*Étant donné que la récupération d'une application d'ACE pour laquelle il dispose d'un App-ID peut prendre plusieurs minutes et plus si un nouvel App-ID doit être développé, la détection des applications cloud n'est pas en ligne sur le pare-feu. Le pare-feu n'attend pas de verdict pour traiter le trafic de l'application. Le pare-feu traite le trafic en tant que ssl, navigation Web, unknown-tcp ou unknown-udp jusqu'à ce qu'il reçoive un App-ID d'ACE, puis continue à traiter le trafic de cette manière jusqu'à ce que vous receviez le nouvel App-ID et l'utilisiez dans la Politique de sécurité.*

*Si vous rétrogradez un pare-feu ou Panorama après l'activation d'ACE et que les ID d'application cloud ACE sont toujours utilisés dans les règles de politique de sécurité ou les groupes d'applications, la rétrogradation échoue. La raison de l'échec répertorie les objets que vous devez supprimer de la configuration afin de rétrograder. Supprimez ces objets de la configuration et* ***Commit (validez)*** *la configuration, puis la rétrogradation réussira.*



# Se préparer au déploiement d'App-ID Cloud Engine

Plusieurs tâches d'intégration doivent être effectuées avant que le pare-feu puisse utiliser App-ID Cloud Engine (ACE). Vous pouvez déployer ACE sur des pare-feu autonomes ou utiliser Panorama pour déployer ACE sur des pare-feu gérés.

Avant qu'un pare-feu puisse utiliser ACE pour fournir des APP-ID spécifiques pour le trafic précédemment identifié comme ssl, navigation Web, trafic tcp inconnu et trafic udp inconnu, l'administrateur PAN-OS et l'administrateur de sécurité SaaS doivent travailler ensemble pour :

- Installez un certificat de périphérique valide sur chaque appareil qui utilisera ACE, y compris les appareils Panorama qui gèrent les pare-feu ACE. (Administrateur PAN-OS.)
- Activez SaaS Security Inline sur chaque pare-feu qui utilisera ACE. Panorama ne nécessite pas de licence. (Administrateur de sécurité SaaS.)
- Configurez un itinéraire de service pour la communication entre le pare-feu et ACE. (Administrateur PAN-OS.)
- Activez ACE sur les appareils Panorama qui gèrent les pare-feux qui utiliseront ACE. (Administrateur PAN-OS.)

  ***Sur les pare-feu, ACE est activé par défaut après l'activation de SaaS Security Inline.***

- Créez une règle de stratégie de sécurité qui autorise le trafic ACE. (Administrateur PAN-OS.)
- Configurez le transfert de journal du pare-feu vers le cortex Data Lake (CDL). (Administrateur PAN-OS.)

***À l'étape appropriée de la procédure suivante, l'administrateur PAN-OS doit informer l'administrateur SaaS Security que le déploiement est prêt pour l'activation SaaS Security Inline. Après avoir activé SaaS Security Inline, l'administrateur SaaS Security Inline doit informer l'administrateur PAN-OS que le déploiement est prêt à se terminer sur les périphériques PAN-OS. La communication entre les administrateurs est essentielle pour parvenir à un déploiement en douceur.***

Exigences :

- Les pare-feu autonomes, les appareils Panorama et les pare-feux gérés doivent exécuter PAN-OS 10.1 ou version ultérieure.
- Tous les pare-feux ACE doivent avoir acheté une licence SaaS Security Inline. Panorama ne nécessite pas de licence pour gérer les pare-feux ACE ou pousser les configurations ACE vers les pare-feux gérés.

- Tous les appareils ACE doivent pouvoir se connecter à la région GCP des États-Unis, de l'APAC ou de l'UE, en fonction de votre emplacement (la région est sélectionnée automatiquement en fonction de votre région CDL).

  Vérifiez que le pare-feu utilise le nom de domaine complet Content Cloud (**Device (périphérique)** > **Setup (configuration)** > **Content-ID (ID de contenu)** > **Content Cloud Setting (Paramètre de Content Cloud)**) correct pour votre région et modifiez le nom de domaine complet si nécessaire :

  - États-Unis—**hawkeye.services-edge.paltoaltonetworks.com**
  - UE—**eu.hawkeye.services-edge.paltoaltonetworks.com**
  - APAC—**apac.hawkeye.services-edge.paltoaltonetworks.com**

  Les données ACE, y compris les charges utiles de trafic, sont envoyées aux serveurs de la région sélectionnée. Si vous spécifiez un FQDN Content Cloud qui se trouve en dehors de votre région (par exemple, si vous êtes dans la région de l'UE mais que vous spécifiez le FQDN de la région APAC), vous pouvez enfreindre les réglementations légales et de confidentialité de votre pays ou de votre organisation.

L'administrateur PAN-OS effectue les deux premières étapes de la procédure, puis les transmet à l'administrateur SaaS Security Inline pour activation (Étape 3). Après l'activation, l'administrateur SaaS Security Inline remet le reste de la procédure à l'administrateur PAN-OS pour qu'il l'effectue sur les périphériques PAN-OS.

**STEP 1 |** Mettez le pare-feu et Panorama (si vous l'utilisez) en ligne. (Administrateur PAN-OS.)

**STEP 2 |** Install a Device Certifcate (Installez un Device Certifcate) sur des pare-feu individuels afin qu'ils puissent utiliser des services cloud ou utiliser Panorama pour Install the Device Certificate for Managed Firewalls (installer le certificat de périphérique pour les pare-feu gérés). (Administrateur PAN-OS.)

*Passez l'étape suivante à l'administrateur de la sécurité SaaS.*

**STEP 3 |** Activate SaaS Security Inline (Activez SaaS Security Inline) sur chaque pare-feu qui utilisera ACE. L'activation active ACE sur les pare-feux. (Administrateur de sécurité SaaS.)

*Panorama ne nécessite pas de licence SaaS Security Inline pour gérer les pare-feux qui utilisent ACE. Seuls les pare-feux gérés ont besoin de licences, que vous devez récupérer manuellement comme indiqué à l'étape suivante.*

*Transmettez le reste des étapes à l'administrateur PAN-OS.*

**STEP 4 |** Récupérez la licence SaaS Security Inline sur chaque pare-feu (Panorama n'a pas besoin de licence) et vérifiez qu'elle est activée. (Administrateur PAN-OS.)

L'activation de l'administrateur Saas de la sécurité configure les licences pour le pare-feu, de sorte que vous n'avez pas besoin d'accéder au portail de support client ou d'obtenir des codes d'authentification.

1. Accédez à **Device (périphérique)** > **Licenses (Licences)** > **License Management (Gestion des licences)**et sélectionnez **Retrieve license keys from license server (Récupérer les clés de licence du serveur de licences)** pour récupérer la licence.
2. Vérifiez **Device (périphérique)** > **Licenses (Licences)** pour vous assurer que la licence SaaS Security Inline est active.

**STEP 5 |** Configurez un itinéraire de service de services de données (dataplane) afin que le pare-feu puisse communiquer avec App-ID Cloud Engine. (Administrateur PAN-OS.)

*Vous pouvez transmettre cette configuration vers des pare-feux gérés à partir de Panorama. Panorama et les pare-feux gérés doivent exécuter PAN-OS 10.1 ou version ultérieure.*

Par défaut, le pare-feu utilise l'interface de gestion comme interface source pour l'itinéraire du service des services de données, mais il est recommandé de configurer une interface de plan de données qui a une connectivité aux services cloud en tant que**Source Interface (interface source)** et **Source Address (adresse source)** pour les services de données, comme indiqué plus loin dans cette étape.

Le problème sur les pare-feu est que si un proxy explicite est configuré sur l'interface de gestion et que vous l'utilisez pour l'itinéraire du service de services de données, l'interface de gestion ne peut se connecter qu'au service Knowledge Cloud (KCS), qui gère l'application cloud et les signatures. Lorsqu'un proxy explicite est configuré sur l'interface de gestion, il ne peut pas se connecter au service DCS (Detection Cloud Service), qui vérifie la charge utile de l'application par rapport aux ID d'application ACE existants et fournit des verdicts. KCS et DCS sont des services dans le cloud ACE. Si un proxy explicite est configuré sur l'interface de gestion, vous ne pouvez pas l'utiliser pour l'itinéraire du service de services de données pour ACE, car il ne peut pas se connecter à tous les services. Dans ce cas, vous devez utiliser une interface de plan de données sur le pare-feu pour vous connecter aux services de données.

*Panorama utilise le port de gestion par défaut pour se connecter au KCS et ne se connecte pas au DCS.*

Pour configurer l'itinéraire de service sur une interface de plan de données au lieu d'utiliser l'interface de gestion par défaut :

1. Sélectionnez **Device (périphérique)** > **Setup (configuration)** > **Services** puis dans **Service Features (Fonctionnalités des services)**, sélectionnez **Service Route Configuration (Configuration de l'itinéraire de service)**.
2. **Customize (Personnalisez)** un Itinéraire de service.
3. Sélectionnez le protocole **IPv4**.
4. Cliquez sur **Data Services (Services de données)** dans la colonne Service pour ouvrir la boîte de dialogue **Service Route Source (Source d'itinéraire de service)**.

5. Sélectionnez une **Source interface (interface source)** et une **Source Address (adresse source)** (il ne peut pas s'agir de l'interface de gestion).

   L'interface de la source doit avoir une connectivité internet. La bonne pratique consiste à utiliser une interface de plan de données qui dispose d'une connectivité aux services cloud. ConsultezConfigure Interfaces (Configurer les interfaces) et Create an Address Object (Créer un objet d'adresse) pour plus d'informations sur la création d'interfaces et d'adresses sources.
6. Cliquez sur **OK** pour définir l'interface source et l'adresse.
7. Cliquez sur **OK** pour enregistrer la configuration de l'itinéraire de service.
8. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et ajoutez une Security policy rule (règle de politique de sécurité)qui autorise le trafic de l'interface source que vous avez spécifiée précédemment dans cette procédure vers les adresses FQDN des services KCS et DCS, qui sont **`kcs.ace.tpcloud.paloaltonetworks`** (service KCS pour toutes les régions) et **`hawkeye.services-edge.paloaltonetworks.com`** (service DCS de la région États-Unis), **`eu.hawkeye.services-edge.paloaltonetworks.com`** (service DCS de la région UE) ou **`apac.hawkeye.services-edge.paloaltonetworks.com`** (service DCS de la région APAC).

   Ajoutez et autorisez également les deux nom de domaine complets suivants dans une règle de politique de sécurité nouvelle ou existante : **`ocsp.paloaltonetworks.com`** et **`crl.paloaltonetworks.com`** pour la vérification des certificats.

   Enfin, ajoutez ou modifiez une règle de politique de sécurité pour autoriser le trafic ACE en autorisant les trois applications suivantes : **`paloalto-ace`**, **`paloalto-ace-kcs`**, et **`paloalto-dlp-service`**.

**STEP 6 |** Assurez-vous que hawkeye.services-edge.paloaltonetworks.com et kcs.ace.tpcloud.paloaltonetworks sont accessibles sur les pare-feux et que kcs.ace.tpcloud.paloaltonetworks est accessible sur les périphériques Panorama. (Administrateur PAN-OS.)

Exécutez la commande opérationnelle **`admin@fw1> show cloud-appid connection-to-cloud`**. La sortie vous informe si la connexion fonctionne et si la licence est installée.

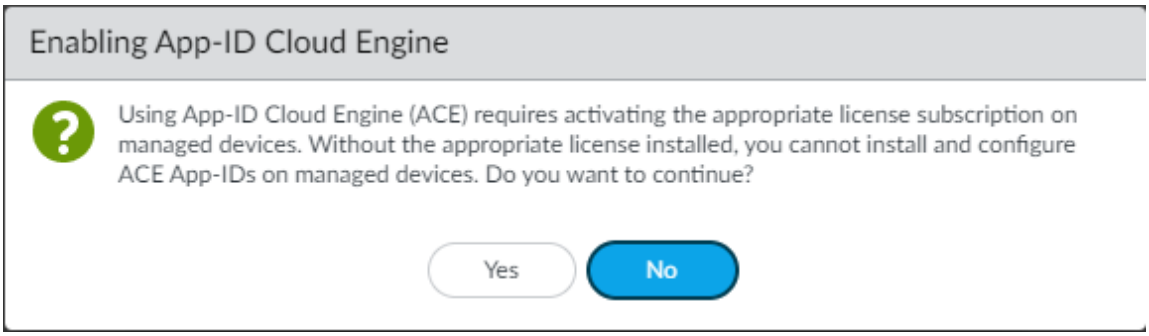
 

**STEP 7 |** (Panorama only (Panorama uniquement)) Activez ACE sur tout appareil Panorama qui gère les pare-feux compatibles ACE. (Administrateur PAN-OS.)

ACE est désactivé par défaut sur Panorama.

*Si vous transférez les configurations ACE vers des groupes gérés qui n'ont pas de pare-feux compatibles ACE (certains ou tous les pare-feux du groupe n'ont pas ACE activé), le transfert échoue.*

1. Accédez à **Paramètres** > **Setup (Configuration)** > **ACE** > **Settings (Paramètres)**.
2. Cliquez sur Modifier (⚙), puis désélectionnez **Disable App-ID Cloud Engine (Désactiver App-ID Cloud Engine).**
3. Cliquez sur **OK**.
4. La boîte de dialogue **Enable App-ID Cloud Engine (Activer App-ID Cloud Engine)** s'affiche.




Cliquez sur **Yes (Oui)** pour activer ACE.

5. **Commit (Validez)** la modification.

**STEP 8 |** Attendez le téléchargement du catalogue App-ID. (Administrateur PAN-OS.)

Il existe moins de quatre mille App-ID fournis par le contenu. Après avoir téléchargé le catalogue ACE, vous voyez plusieurs milliers d'autres applications sur le pare-feu et pouvez confirmer en cochant **Objects (Objets)** > **Applications** ou en utilisant la commande CLI opérationnelle `show cloud-appid cloud-app-data application all (afficher l'application cloud-appid cloud-appid cloud-app-data tous)` pour voir les nouveaux ID d'application.

**STEP 9 |** (Panorama only (Panorama uniquement)) Transférer la configuration souhaitée vers le(s) pare-feu géré(s). (Administrateur PAN-OS.)

**STEP 10 |** Configure Log Forwarding (Configurez le transfert de journal) vers Cortex Data Lake (CDL) et activez le transfert de journal avec le profil de transfert de journal correct dans les règles de politique de sécurité. (Administrateur PAN-OS.)

*Une SaaS Security Inline connection (connexion SaaS Security Inline) à CDL est requise pour la visibilité SaaS et pour prendre en charge la SaaS App-ID Policy Recommendation (recommandation de politique SaaS App-ID). Au minimum, vous devez transférer les journaux de trafic et les journaux d'URL vers CDL pour que SaaS Security Inline fonctionne correctement.*

# Activer ou désactiver App-ID Cloud Engine

App-ID Cloud Engine (ACE) est désactivé par défaut sur Panorama et activé par défaut sur les pare-feu lorsque la licence SaaS Security Inline est installée. Vous devez activer ACE sur les appareils Panorama qui gèrent les pare-feu compatibles ACE.

Pour activer ou désactiver ACE :

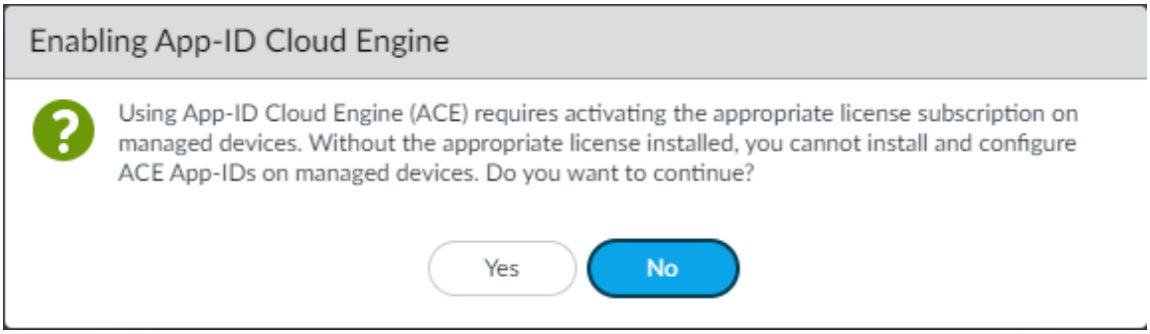
**STEP 1 |** Accédez à **Device (Périphérique)** > **Setup (Configuration)** > **ACE** > **Settings (Paramètres)**sur le pare-feu ou**Panorama** > **Setup (Configuration)** > **ACE** > **Settings (Paramètres)** sur Panorama.

**STEP 2 |** Cliquez sur Modifier (⚙), puis désactivez**Disable App-ID Cloud Engine (Désactiver App-ID Cloud Engine)** pour activer ACE ou sélectionnez **Disable App-ID Cloud Engine (Désactiver App-ID Cloud Engine)** pour désactiver ACE.

ACE est désactivé par défaut.

**STEP 3 |** Cliquez sur **OK**.

**STEP 4 |** (Only if enabling ACE (Uniquement si vous activez ACE) ) Si vous activez ACE, la boîte de dialogue **Enable App-ID Cloud Engine (Activer App-ID Cloud Engine)** s'affiche.




Si la licence SaaS Security Inline est installée sur le pare-feu ou les pare-feu gérés par Panorama, cliquez sur **Yes (Oui)** pour activer ACE.

**STEP 5 |** **Commit (Validez)** la modification.

# Traitement et utilisation d'App-ID Cloud Engine

Lorsque le pare-feu télécharge les App-ID App-ID Cloud Engine (ACE), il est important de comprendre comment le pare-feu gère ces App-ID et comment le pare-feu gère les App-ID ACE lorsqu'il existe également des App-ID prédéfinis basés sur le contenu pour le mêmes applications. L'équipe de contenu de Palo Alto Networks développe des App-ID prédéfinis basés sur le contenu et les met à jour avec des App-ID modifiés et nouveaux via des application content updates (mises à jour de contenu d'application) (un contrat de support valide est requis pour les mises à jour).

ACE nécessite une licence SaaS Security Inline. Les pare-feu qui ne prennent pas en charge ACE ont uniquement des App-ID prédéfinis basés sur le contenu. Le catalogue ACE App-ID ne contient pas d'App-ID basés sur le contenu.

*Vous ne pouvez utiliser les ID d'application ACE que dans les règles de politique de sécurité. Vous ne pouvez pas utiliser les ID d'application ACE dans tout autre type de règle de politique.*

- Lorsque le pare-feu se connecte pour la première fois au moteur cloud App-ID, le pare-feu télécharge un catalogue des App-ID ACE disponibles et vous pouvez utiliser ces App-ID dans la Politique de sécurité. Il ne télécharge pas les signatures complètes. Le catalogue vous permet d'utiliser les ID d'application ACE dans la Politique de sécurité même si les applications n'ont jamais été vues sur le pare-feu. ACE envoie régulièrement les mises à jour du catalogue aux pare-feux afin que les pare-feux aient accès aux derniers ID d'application ACE.

  Si une application arrive au pare-feu identifié comme SSL, navigation Web, tcp inconnu ou udp inconnu et que le pare-feu n'a pas sa signature, le pare-feu envoie la charge utile à ACE. Si ACE a un App-ID pour le trafic, ACE renvoie les signatures complètes au pare-feu. Si le trafic ne correspond à aucune signature ACE, ACE envoie la charge utile au moteur Machine Learning (ML). Le moteur ML analyse la charge utile et développe le nouvel App-ID en collaboration avec l'équipe de contenu humain et supprime le trafic qui n'est pas lié aux applications. Le moteur ML envoie le nouvel App-ID à ACE et les pare-feu demandeurs peuvent le télécharger et l'utiliser dans la Politique de sécurité.

  ***Étant donné que la récupération d'une application d'ACE pour laquelle il dispose d'un App-ID peut prendre plusieurs minutes et plus si un nouvel App-ID doit être développé, la détection des applications cloud n'est pas en ligne sur le pare-feu. Le pare-feu n'attend pas de verdict pour traiter le trafic de l'application. Le pare-feu traite le trafic en tant que ssl, navigation Web, unknown-tcp ou unknown-udp jusqu'à ce qu'il reçoive un App-ID d'ACE, puis continue à traiter le trafic de cette manière jusqu'à ce que vous receviez le nouvel App-ID et l'utilisiez dans la Politique de sécurité.***

- Lorsqu'un pare-feu demande un App-ID d'ACE, le pare-feu ne retient pas le trafic, il continue à traiter le trafic comme d'habitude jusqu'à ce qu'il reçoive un App-ID d'ACE.
- Le pare-feu gère les App-ID cloud téléchargés depuis ACE différemment qu'il ne gère les App-ID fournis par le contenu. Vous n'avez pas besoin d'examiner comment les nouveaux ID d'application ACE affectent la Politique de sécurité avant qu'ils ne soient installés sur le pare-feu, car le pare-feu utilise les ID d'application ACE conformément à la Politique de sécurité existante. Vos règles de Politique de sécurité existantes contrôlent les nouveaux ID d'application ACE jusqu'à ce que vous utilisiez explicitement les ID d'application ACE dans la Politique de sécurité. Par exemple :

  1. Une application est identifiée uniquement comme « ssl » et vous avez une règle de Politique de sécurité qui autorise le trafic SSL, donc la règle SSL autorise cette application.
  2. Le pare-feu voit l'application SSL et envoie la charge utile à ACE.
  3. ACE identifie l'application réelle. Si l'application existe dans la base de données ACE, ACE envoie cet App-ID au pare-feu. S'il s'agit d'une nouvelle application pour laquelle ACE n'a pas d'ID d'application, ACE transfère la charge utile au moteur de ML. Le pare-feu ne reçoit pas l'App-ID jusqu'à ce que le ML Engine et l'équipe de contenu humain attribuent un App-ID et l'envoient à ACE.
  4. La règle qui autorise le trafic SSL autorise toujours l'application nouvellement identifiée, même si son App-ID n'est plus « ssl ». (Cependant, si vous utilisez le nouveau ACE App-ID dans la Politique de sécurité, cette Politique contrôle le trafic. De même, le trafic précédemment identifié comme navigation Web, tcp inconnu et udp inconnu continue d'obéir aux règles

de politique de sécurité qui contrôlent ces types de trafic jusqu'à ce que vous utilisiez les ID d'application ACE dans la Politique de sécurité.)

> ***Contrairement aux App-ID ACE, si l'App-ID était un App-ID prédéfini et fourni par le contenu, la règle qui autorise le trafic SSL ne correspondrait plus à l'application. Le pare-feu le bloquerait si aucune règle de Politique de sécurité ne le permet explicitement.***

L'exception à ce comportement est si une autre règle de Politique de sécurité spécifie l'App-ID donné au trafic par ACE. La règle de politique de sécurité avec l'App-ID spécifique est prioritaire sur la règle avec l'App-ID ssl moins spécifique. Si la règle qui spécifie l'App-ID réel est une règle de blocage, l'application est bloquée même s'il existe une règle qui autorise le trafic SSL. La règle avec l'App-ID le plus spécifique (granulaire) est celle sur laquelle le pare-feu agit.

> ***Dans cet exemple, si vous ajoutez l'ID d'application cloud pour l'application précédemment identifiée comme « ssl » à une règle existante ou clonée, soit directement, soit à l'aide d'un filtre d'application ou d'un groupe d'applications, cette règle contrôle l'application. La règle « ssl » ne contrôle plus l'application car l'application est spécifiquement identifiée dans une autre règle.***

Si vous n'ajoutez pas explicitement de nouveaux ID d'application ACE aux règles de politique de sécurité, le pare-feu continue de les contrôler avec les mêmes règles qui contrôlaient ces applications avant qu'elles n'aient des ID d'application ACE et qu'elles soient identifiées comme ssl, navigation Web, inconnue- tcp ou trafic inconnu-udp. Par exemple, si le pare-feu voit une application identifiée comme inconnue-tcp, puis reçoit un identifiant d'application ACE pour le trafic, mais que vous n'utilisez pas cet identifiant d'application ACE dans une Règle de politique de sécurité, le pare-feu contrôle toujours ce trafic. en utilisant la règle qui contrôle le trafic tcp inconnu : si vous bloquez le trafic tcp inconnu, alors le trafic est bloqué, et si vous autorisez le trafic tcp inconnu, le trafic est autorisé.

- Le pare-feu met en cache certaines informations afin que le pare-feu puisse vérifier le cache et éviter d'envoyer à plusieurs reprises des données au cloud et de demander des verdicts. Si le pare-feu attend un verdict d'ACE, le pare-feu ne transmet pas deux fois les mêmes données d'application.
- Une application de conteneur particulière et ses applications fonctionnelles sont soit tous des App-ID basés sur le cloud, soit tous des App-ID basés sur le contenu. Une méthode de livraison App-ID définit une application de conteneur et toutes ses applications fonctionnelles.
- Si les noms App-ID personnalisés basés sur le cloud, fournis par le contenu et définis par l'utilisateur se chevauchent, l'ordre de priorité est :

  1. **Custom App-IDs (App-ID personnalisés)** : ces App-ID ont priorité sur tous les autres App-ID et si le pare-feu tente de télécharger une application ACE avec le même App-ID, la validation

échoue car deux applications sur le même pare-feu ne peuvent pas avoir la même App-ID. IDENTIFIANT.

Dans ce cas, vous pouvez renommer l'application personnalisée ou, si l'application personnalisée est la même que l'application ACE, vous pouvez supprimer l'application personnalisée et utiliser l'application ACE.

2. **Content-based, predefined App-IDs (App-ID prédéfinis et basés sur le contenu)** : ces App-ID ont la priorité sur les définitions d'App-ID du cloud ACE.
3. **ACE cloud App-IDs (ID d'application cloud ACE)** : les ID d'application personnalisés et basés sur le contenu ont priorité sur les définitions d'ID d'application ACE.

- Si un App-ID correspond à une application de conteneur, le pare-feu télécharge l'App-ID de l'application de conteneur et toutes ses applications fonctionnelles. Par exemple, si le pare-feu récupère l'application de conteneur facebook, il récupère également facebook-base, facebook-chat, facebook-post, etc.
- Lorsque vous effectuez l'une des actions suivantes sur un ID d'application ACE, vous affectez la façon dont la Politique de sécurité gère cet ID d'application ACE, car le pare-feu prendra des mesures en fonction de l'ID d'application ACE spécifique au lieu de se fonder sur le précédent SSL, Web -browsing, unknown-tcp ou unknown-udp App-ID :
  - Créez des Application Filters (Filtres d'application) pour automatiser l'ajout d'ID d'application ACE à la Politique de sécurité.

    ***Utilisez les Filtres d'application pour automatiser l'ajout d'ID d'application ACE aux Règles de politique de sécurité. Lorsqu'un nouvel App-ID correspond à un Filtre d'application, le pare-feu l'ajoute automatiquement au filtre. Lorsque vous utilisez ce Filtre d'application dans une Règle de stratégie de sécurité, la règle contrôle le trafic d'application pour les nouveaux ID d'application qui ont été automatiquement ajoutés au filtre. En d'autres termes, les filtres d'application sont votre « bouton facile » pour sécuriser automatiquement les identifiants d'application ACE afin d'obtenir une visibilité et un contrôle maximum des applications avec un minimum d'effort.***
  - Ajoutez les App-ID aux Application Groups (groupes d'applications).
  - Utilisez Policy Optimizer (optimiseur de politique) pour ajouter les App-ID à une règle clonée ou à une règle existante, ou à un Filtre d'application ou un Groupe d'applications existant. Vous pouvez utiliser l'Optimiseur de politique pour créer de nouveaux Filtres d'application et Groupes d'applications directement à partir de l'outil Optimiseur de politique. Utilisez les sorting and filtering tools (outils de tri et de filtrage) de l'Optimiseur de politique pour hiérarchiser les règles sur lesquelles travailler et pour évaluer le nombre d'ID d'application ACE correspondant à ces règles.
  - Ajoutez un App-ID ACE directement à une règle de politique de sécurité nouvelle ou existante.

  Lorsque vous ajoutez un App-ID cloud à une règle de politique de sécurité directement ou à l'aide d'un Filtre d'application ou d'un Groupe d'applications, cette règle contrôle l'application. Jusqu'à ce que vous effectuiez l'une de ces actions pour contrôler les App-ID fournis par le cloud, le pare-feu utilise les règles de politique de sécurité SSL, navigation Web, unknown-tcp ou unknown-udp existantes pour contrôler les applications ACE.
- Lorsque vous créez des Filtres d'application, excluez ssl et la navigation Web des filtres. Ensemble, ssl et la navigation Web correspondent à toutes les applications cloud basées sur un navigateur,

de sorte qu'un filtre d'application qui inclut ssl et la navigation Web correspond à toutes les applications cloud basées sur un navigateur.

- Haute disponibilité active/passive :
  - Le pare-feu actif synchronise le catalogue ACE avec le pare-feu passif afin qu'ils aient des catalogues identiques.
  - Le pare-feu passif n'initie pas de connexions à ACE jusqu'à ce qu'il devienne le pare-feu actif.
- Haute disponibilité active/active : Chaque périphérique récupère les catalogues et les signatures séparément, de sorte que les catalogues et les signatures ne sont pas synchronisés. Cependant, les validations échouent si le catalogue est désynchronisé sur les pairs et si les ID d'application ACE sont référencés dans les Règles de politique de sécurité. Si les catalogues des pare-feux HA homologues ne sont pas synchronisés, attendez quelques minutes que les mises à jour atteignent les périphériques et redeviennent synchronisées.
- Un échec Panorama commit all/push vers les pare-feux gérés se produit si :
  - Les pare-feu gérés n'ont pas de licence SaaS Security Inline valide, ils n'ont donc pas le catalogue ACE. Dans ce cas, supprimez les objets ACE de la configuration transmise et réessayez.
  - La connexion entre un pare-feu géré et ACE tombe en panne et la configuration transmise inclut des applications qui ne figurent pas dans le catalogue ACE sur le pare-feu. Dans ce cas, vérifiez la connexion au cloud ACE et rétablissez la connexion si nécessaire pour que le firewall puisse mettre à jour son catalogue.

    La commande CLI opérationnelle **`show cloud-appid connection-to-cloud`** fournit l'état de la connexion cloud et l'URL du serveur cloud ACE.
  - Le catalogue ACE sur Panorama et le catalogue ACE sur les pare-feu gérés sont désynchronisés, ce qui entraîne des configurations transmises qui incluent des applications ACE qui ne figurent pas dans le catalogue du pare-feu. Si la connexion entre le pare-feu et ACE est établie, le catalogue obsolète sera mis à jour automatiquement dans les prochaines minutes et résoudra le problème. (Attendez cinq minutes et réessayez.)

    ***Vous pouvez également utiliser la commande CLI `debug cloud-appid cloud-manual-pull check-cloud-app-data` pour mettre à jour le catalogue manuellement.***
- Certains profils de Sécurité tels que les profils de Blocage de fichiers, Antivirus, WildFire et DLP peuvent spécifier des applications dans le cadre du profil. Seuls les App-ID fournis par le contenu sont pris en charge dans les profils de Sécurité. Les identifiants d'application ACE ne sont pas pris en charge dans les profils de Sécurité. Les ID d'application ACE sont destinés à être utilisés dans les Règles de politique de sécurité uniquement.

- Étant donné que les ID d'application ACE sont pris en charge uniquement pour la stratégie de sécurité, ils ne sont pas pris en charge dans les règles de stratégie Application Override, Policy-Based Forwarding (PBF), QoS ou SD-WAN.

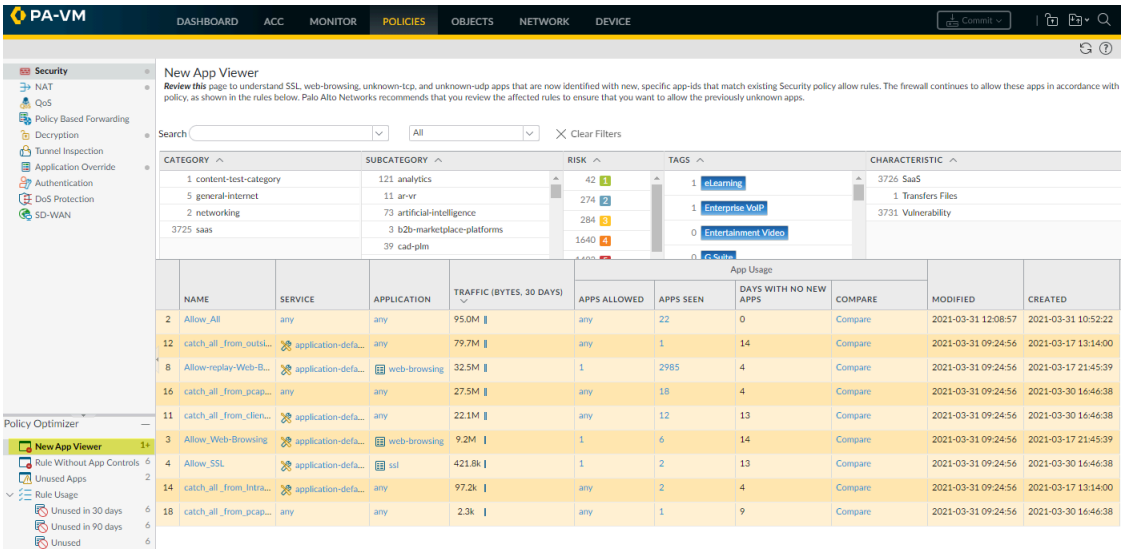
  *Vous ne pouvez pas voir les ID d'application ACE dans la configuration de la règle Application Override ou PBF. Cependant, les ID d'application ACE sont visibles (pouvant être sélectionnés) dans la configuration des règles de politique QoS et SD-WAN et peuvent être présents dans les Groupes d'applications ou les Filtres d'application appliqués à une règle. Si vous utilisez des identifiants d'application ACE dans ces règles, la politique ne contrôle pas le trafic d'application et il n'y a aucun effet sur le trafic d'application - les règles ne s'appliquent pas au trafic d'identifiant d'application ACE même si des identifiants d'application ACE ont été ajoutés à la règle.*

# Nouvelle visionneuse d'applications (Optimiseur de politique)

Policy Optimizer (optimiseur de politique) **New App Viewer (Nouvelle visionneuse d'applications)** vous montre les règles de politique de sécurité qui correspondent aux ID d'applications cloud téléchargées à partir d'ACE. Vous pouvez utiliser l'Optimiseur de politique pour gérer les applications nouvellement identifiées et les ajouter à des règles clonées ou à des règles existantes. Sélectionnez **Policies (politiques)** > **Security (Sécurité)** pour exposer la **New App Viewer (nouvelle visionneuse d'applications)** dans la partie **Policy Optimizer (Optimiseur de politique)** de l'interface, puis sélectionnez **New App Viewer (Nouvelle visionneuse d'applications)**.

La partie supérieure de l'écran est similaire à **Objects (Objets)** > **Application Filters (Filtres d'application)**. Il fonctionne de la même manière et filtre les règles de politique de sécurité affichées dans la partie inférieure de l'écran. Vous pouvez filtrer les règles qui autorisent les applications par catégorie, sous-catégorie, etc. Les seules catégories et sous-catégories disponibles pour le filtrage sont celles qui correspondent aux nouvelles applications sur les règles répertoriées dans la moitié inférieure de l'écran, de sorte que vous ne perdez pas votre temps à filtrer les applications qui ne sont pas là.

Lorsque vous filtrez les règles, seules les règles qui incluent les applications filtrées sont affichées dans la partie inférieure de l'écran. Les règles qui n'ont pas vu les applications dans le filtre sont supprimées de la liste. (Vous pouvez tous les voir à nouveau en supprimant le filtre.)



Cliquez sur le numéro dans la colonne **Apps seen (Applications vues)** pour ouvrir la boîte de dialogue **Applications & Usage (Applications et utilisation)** afin de modifier la façon dont le pare-feu gère les applications basées sur le cloud dans la politique de sécurité. Ajoutez des ID d'application ACE aux règles de politique de sécurité à l'aide d'un Filtre d'application, d'un Groupe d'applications, d'un Optimiseur de politique ou en ajoutant directement une ID d'application ACE à une règle. Jusqu'à ce que vous preniez l'une de ces mesures pour contrôler les App-IDs fournis par le cloud, le pare-feu continue de voir le trafic sous forme de trafic ssl, navigation Web, unknown-tcp ou unknown-udp et utilise les règles de politique de sécurité ssl, web-browsing, unknown-tcp ou unknown-udp existantes pour contrôler les applications.

## Ajouter des applications à un filtre d'applications avec l'optimiseur de politique

Ajoutez des ID d'application à partir du moteur cloud App-ID (ACE et/ou des ID d'application fournis par le contenu) à des filtres d'application nouveaux ou existants pour automatiser la façon dont vous contrôlez les ID d'application cloud dans la stratégie de sécurité. Lorsque de nouvelles ID d'application ACE correspondent à un filtre d'application, le pare-feu les ajoute automatiquement au filtre. Lorsque vous utilisez le filtre d'application dans une règle de stratégie de sécurité, la règle contrôle automatiquement les nouvelles ID d'application ACE lorsqu'ils arrivent au pare-feu et sont ajoutés au filtre.

*ACE fournit des identifiants d'application pour les applications précédemment identifiées comme SSL, navigation Web,unknown-tcp ou unknown-udp.*

L'utilisation des filtres d'application est une bonne pratique car ils :

- Améliorez votre posture de sécurité. Les filtres d'application automatisent l'ajout de nouveaux APP-ID ACE aux règles de stratégie de sécurité que vous concevez spécifiquement pour gérer un type particulier de trafic d'application, au lieu de faire correspondre le trafic à des règles ssl plus générales, de navigation Web, de unknown-tcp, ou unknown-udp.
- Gagner du temps. Les administrateurs de pare-feu peuvent configurer les filtres d'application pour gérer différents types de trafic afin que l'ajout de nouvelles ID ACE à la politique soit automatique et ne nécessite aucun effort supplémentaire de la part de l'administrateur.

*Lorsque vous créez des Filtres d'application, excluez ssl et la navigation Web des filtres. Ensemble, ssl et la navigation Web correspondent à toutes les applications cloud basées sur un navigateur, de sorte qu'un filtre d'application qui inclut ssl et la navigation Web correspond à toutes les applications cloud basées sur un navigateur.*

Utilisez Policy Optimizer (Optimiseur de politique) pour ajouter des ID d'application ACE aux filtres d'application et pour appliquer les filtres aux règles clonées ou existantes et contrôler les ID d'application ACE dans la politique de sécurité.

**STEP 1 |** Accédez à **Policies (Politiques)** > **Security** et ensuite sélectionnez **Policy Optimizer (Optimiseur de politique)** > **New App Viewer (Nouvelle visionneuse d'applications)**.

Si le pare-feu a identifié le trafic avec des ID d'application ACE, un numéro s'affiche en regard de **New App Viewer (Nouvelle visionneuse d'application)** dans la fenêtre de navigation de gauche. L'écran affiche les règles de stratégie de sécurité qui correspondent aux ID d'application cloud.

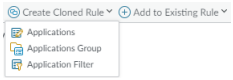
 

**STEP 2 |** Cliquez sur le nombre dans **Apps seen (Applications vues)** pour une règle de stratégie de sécurité pour voir les applications fournies par le cloud qui correspondent à la règle dans la boîte de dialogue **Applications & Usage (Applications et utilisation)**.

**STEP 3 |** Sélectionnez les applications que vous souhaitez ajouter à un filtre d'application existant ou nouveau.

Vous pouvez sort and filter (trier et filtrer) les applications dans **Apps Seen (Applications vues)** par sous-catégorie, risque, volume de trafic vu au cours des 30 derniers jours, ou quand l'application a été vue pour la première ou la dernière fois.

**STEP 4 |** Sélectionnez **Application Filter (Filtre d'application)** dans **Create Cloned Rule (Créer une règle clonée)** ou **Add to Existing Rule (Ajouter à une règle)**, existante, selon la façon dont vous souhaitez gérer les applications.




*Le nombre maximal d'applications que vous pouvez cloner à l'aide de **Create Cloned Rule (Créer une règle clonée)** est de 1 000 applications. S'il y a plus de 1 000 applications que vous souhaitez déplacer vers une règle différente, utilisez plutôt **Add to Existing Rule (Ajouter à la règle existante)**. Si vous souhaitez déplacer les applications vers une nouvelle règle, créez simplement la règle d'abord (**Policies (Politiques)** > **Security (Sécurité)**), puis utilisez l'optimiseur de politique pour les ajouter à cette règle.*

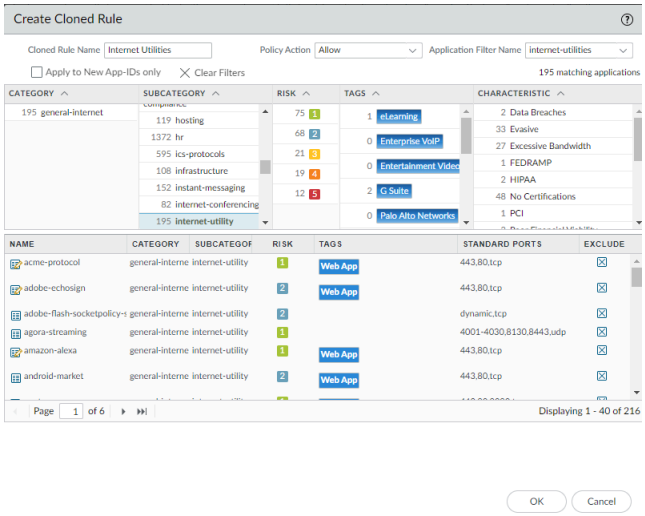
**STEP 5 |** Sélectionnez ou créez le Filtre d'application pour la règle clonée ou existante. La Creating an Application Filter (création d'un filtre d'application) à l'aide de l'Optimiseur de stratégie est presque exactement la même que l'utilisation de **Objects (Objets)** > **Application Filters (filtres d'application** pour créer un filtre d'application : vous utilisez les mêmes outils et options de filtrage.

**Create Cloned Rule (Créer la règle clonée)** :

1. Tapez le **Cloned Rule Name (Nom de la règle clonée)** (le nom de la règle clonée, qui apparaîtra dans la base de règles de politique de sécurité immédiatement au-dessus de la règle d'origine).
2. Sélectionnez **Policy Action (action de politique)** (Autoriser ou Refuser).
3. Sélectionnez le **Application Filter Name (nom du filtre d'application)** dans le menu ou tapez le nom d'un nouveau filtre d'application.
4. Indiquez si le filtre doit **Apply to New App-IDs only (s'appliquer uniquement aux nouvelles ID d'application)** ou s'il doit s'appliquer à toutes les ID d'application.
5. Utilisez les valeurs Catégorie, Sous-catégorie, Risque, Balises et Caractéristique pour filtrer les types d'applications que vous souhaitez ajouter au filtre d'application. Le pare-feu ajoute

automatiquement de nouvelles applications qui répondent aux critères de filtre au filtre d'application.



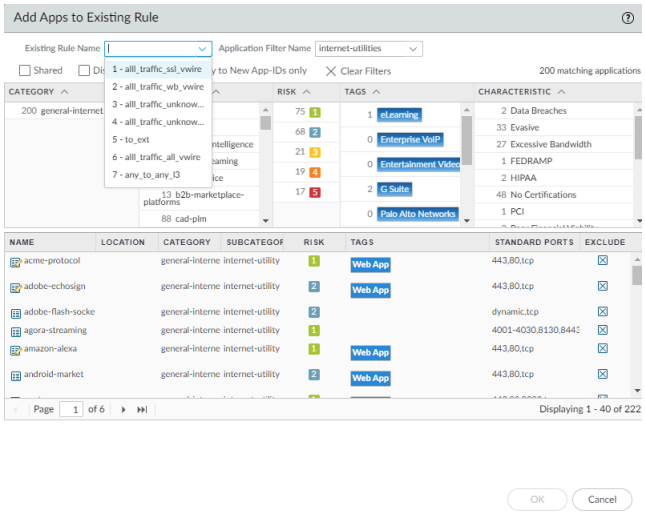

6. Cliquez sur **OK** pour ajouter les applications au filtre d'application nouveau ou existant. Le pare-feu inclut les applications que vous avez sélectionnées en Step 3 (étape 3) du filtre d'application.
7. **Validez** les modifications.

**Add to Existing Rule (Ajouter à la règle existante)** :

1. Sélectionnez le **Existing Rule Name** nom de la règle existante) pour ajouter les applications sélectionnées à une règle existante dans un filtre d'application.
2. Sélectionnez le **Application Filter Name (nom du filtre d'application)** dans le menu ou tapez le nom d'un nouveau filtre d'application.
3. Indiquez si le filtre d'application est **Shared (partagé)**, si vous souhaitez **Disable override (désactiver le remplacement)** des caractéristiques d'application pour le filtre et si le filtre doit **Apply to New App-IDs only (s'appliquer uniquement aux nouveaux ID d'application)** ou s'il doit s'appliquer à tous les ID d'application.
4. Utilisez les valeurs Catégorie, Sous-catégorie, Risque, Balises et Caractéristique pour filtrer les types d'applications que vous souhaitez ajouter au filtre d'application. Le pare-feu ajoute

automatiquement de nouvelles applications qui répondent aux critères de filtre au filtre d'application.




5. Cliquez sur **OK** pour ajouter les applications au filtre d'application nouveau ou existant. Le pare-feu inclut les applications que vous avez sélectionnées en Step 3 (étape 3) du filtre d'application.
6. **Validez** les modifications.

# Ajouter des applications à un groupe d'applications avec l'optimiseur de politique

Ajoutez des ID d'application à partir du moteur cloud App-ID (ACE et/ou des ID d'application fournis par le contenu) à des groupes d'applications nouveaux ou existants et utilisez les règles de stratégie Groupes d'applications dans Sécurité pour contrôler les ID d'application cloud dans la stratégie de sécurité.

*ACE fournit des identifiants d'application pour les applications précédemment identifiées comme SSL, navigation Web,unknown-tcp ou unknown-udp.*

Utilisez Policy Optimizer (Optimiseur de politique) pour ajouter des ID de groupes d'applications ACE aux groupes d'application et pour appliquer les filtres aux règles clonées ou existantes et contrôler les ID d'application ACE dans la politique de sécurité.

**STEP 1 |** Allez dans **Policies (Politiques)** > **Security (Sécurité)** puis sélectionnez **Policy Optimizer (Optimiseur de politique)** > **New App Viewer (nouvelle visionneuse d'applications)**.

Si le pare-feu ou Panorama a téléchargé des identifiants d'application ACE, un nombre s'affiche à côté de **New App Viewer (nouvelle visionneuse d'applications)** dans la fenêtre de navigation de gauche. L'écran affiche les règles de politique de sécurité qui correspondent aux App-ID cloud téléchargés.

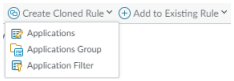
**STEP 2 |** Cliquez sur le nombre dans **Apps seen (Applications vues)** pour une règle de stratégie de sécurité pour voir les applications fournies par le cloud qui correspondent à la règle dans la boîte de dialogue **Applications & Usage (Applications et utilisation)**.

**STEP 3 |** Sélectionnez les applications que vous souhaitez ajouter à un groupe d'applications existant ou nouveau.

Vous pouvez sort and filter (trier et filtrer) les applications dans **Apps Seen (Applications vues)** par sous-catégorie, risque, volume de trafic vu au cours des 30 derniers jours, ou quand l'application a été vue pour la première ou la dernière fois.

**STEP 4 |** Sélectionnez **Application Group (Groupe d'applications)** dans **Create Cloned Rule (Créer une règle clonée)** ou **Add to Existing Rule (Ajouter à une règle)**, existante, selon la façon dont vous souhaitez gérer les applications.




*Le nombre maximal d'applications que vous pouvez cloner à l'aide de **Create Cloned Rule (Créer une règle clonée)** est de 1 000 applications. S'il y a plus de 1 000 applications que vous souhaitez déplacer vers une règle différente, utilisez plutôt **Add to Existing Rule (Ajouter à la règle existante)**. Si vous souhaitez déplacer les applications vers une nouvelle règle, créez simplement la règle d'abord (**Policies (Politiques)** > **Security (Sécurité)**), puis utilisez l'optimiseur de politique pour les ajouter à cette règle.*

**STEP 5 |** Sélectionnez ou créez le groupe d'applications pour la règle clonée ou existante. Creating Application Groups (création de groupes d'applications) à l'aide de l'Optimiseur de politique est similaire à l'utilisation de **Objects (Objets)** > **Application Groups** groupes d'applications d'objets pour créer un groupe d'applications.

**Create Cloned Rule (Créer la règle clonée)** :

1. Tapez le **Cloned Rule Name (Nom de la règle clonée)** (le nom de la règle clonée, qui apparaîtra dans la base de règles de politique de sécurité immédiatement au-dessus de la règle d'origine).
2. Sélectionnez **Policy Action (action de politique)** (Autoriser ou Refuser).
3. Dans **(Add to Application Group (Ajouter au groupe d'applications)**, sélectionnez le groupe d'applications auquel vous souhaitez ajouter les applications que vous avez sélectionnées dans 3.
4. Choisissez **Add container app (ajouter une application conteneur)** (par défaut) ou uniquement d'ajouter des **Add specific apps seen (applications spécifiques vues)**.

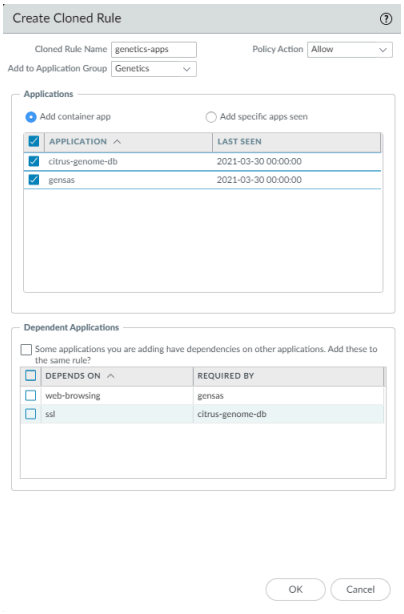
   Lorsque vous ajoutez l'application de conteneur, vous ajoutez également toutes les applications fonctionnelles dans ce conteneur, y compris les applications fonctionnelles qui n'ont pas encore été vues sur le pare-feu. Par exemple, si vous ajoutez l'application de conteneur « facebook », cela ajoute également facebook-base, facebook-chat, facebook-posting, etc., ainsi que toutes les futures applications ajoutées au conteneur. L'application conteneur et ses applications fonctionnelles sont soumises à la règle de stratégie de sécurité à laquelle vous ajoutez le groupe d'applications. La sélection de l'application de conteneur assure essentiellement la pérennité et automatise la sécurité des applications du conteneur afin que vous n'ayez pas à ajouter manuellement de nouvelles applications dans ce conteneur à votre Politique de sécurité.

   L'ajout uniquement des applications spécifiques vues signifie que seules les applications que vous avez sélectionnées sont ajoutées au groupe d'applications. Si de nouvelles applications

dans la même application conteneur arrivent au pare-feu, le Groupe d'applications ne les contrôle pas et vous devez décider manuellement comment gérer les nouvelles applications.

5. Dans certains cas, les applications que vous souhaitez placer dans un groupe d'applications nécessitent (dépendent de) d'autres applications pour fonctionner. Dans ces cas, la boîte de dialogue **Create Cloned Rule (Créer une règle clonée)** comprend des **Dependent Applications (applications dépendantes)**, dans lesquelles vous pouvez choisir d'ajouter ou non ces applications à la règle clonée. Ajoutez les applications dépendantes à la règle pour vous assurer que les applications sélectionnées fonctionnent correctement.



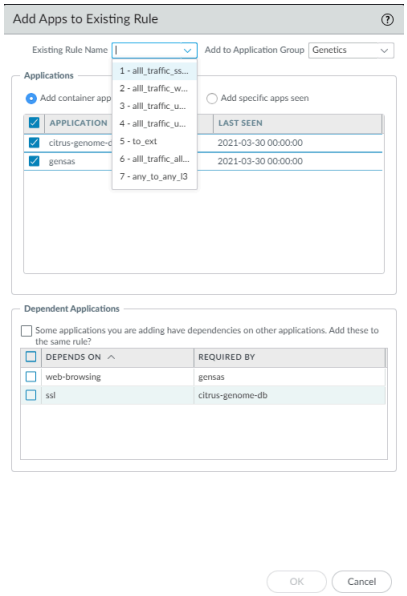

6. Cliquez sur **OK** pour ajouter les applications au Groupe d'applications nouveau ou existant.
7. **Validez** les modifications.

**Add Apps to Existing Rule (Ajouter des applications à une règle existante)** :

1. Sélectionnez le **Existing Rule Name** nom de la règle existante) pour ajouter les applications sélectionnées à une règle existante dans un Groupe d'application.
2. Sélectionnez le groupe d'applications dans **Add to Application Group (Ajouter au groupe d'applications)** ou tapez le nom d'un nouveau groupe d'applications.
3. Comme pour le clonage de la règle, vous pouvez choisir **Add container app (ajouter une application conteneur)** ou **Add specific apps seen (ajouter des applications spécifiques vues)**. L'ajout de l'application de conteneur ajoute toutes les applications fonctionnelles dans le conteneur et toutes les futures applications ajoutées à ce conteneur. L'ajout uniquement des applications spécifiques ajoute uniquement les applications sélectionnées spécifiques.
4. Comme pour le clonage de la règle, dans certains cas, les applications que vous souhaitez placer dans un groupe d'applications nécessitent (dépendent de) d'autres applications pour fonctionner. Dans ces cas, la boîte de dialogue **Add Apps to Existing Rule (Ajouter des applications à la règle existante)** comprend des **Dependent Applications (applications dépendantes)**, dans lesquelles vous pouvez choisir d'ajouter ou non ces applications à la règle

clonée. Ajoutez les applications dépendantes à la règle pour vous assurer que les applications sélectionnées fonctionnent correctement.




5. Cliquez sur **OK** pour ajouter les applications au Groupe d'applications nouveau ou existant.
6. **Validez** les modifications.

# Ajouter des applications directement à une règle avec l'optimiseur de politique

Vous pouvez ajouter des App-ID App-ID Cloud Engine (ACE et/ou App-ID fournis par le contenu) directement à une règle clonée ou existante avec Policy Optimizer (optimiseur de politique). Cependant, envisagez d'utiliser des Application Filters (filtres d'application) pour automatiser l'ajout d'ID d'application ACE à la stratégie de sécurité lorsqu'ils arrivent au pare-feu au lieu de les ajouter manuellement.

*ACE fournit des identifiants d'application pour les applications précédemment identifiées comme SSL, navigation Web,unknown-tcp ou unknown-udp.*

**STEP 1 |** Allez dans **Policies (Politiques)** > **Security (Sécurité)** puis sélectionnez **Policy Optimizer (Optimiseur de politique)** > **New App Viewer (nouvelle visionneuse d'applications)**.

Si le pare-feu ou Panorama a téléchargé des identifiants d'application ACE, un nombre s'affiche à côté de **New App Viewer (nouvelle visionneuse d'applications)** dans la fenêtre de navigation de gauche. L'écran affiche les règles de politique de sécurité qui correspondent aux App-ID cloud téléchargés.

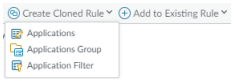
**STEP 2 |** Cliquez sur le nombre dans **Apps seen (Applications vues)** pour une règle de stratégie de sécurité pour voir les applications fournies par le cloud qui correspondent à la règle dans la boîte de dialogue **Applications & Usage (Applications et utilisation)**.

**STEP 3 |** Sélectionnez les applications que vous souhaitez ajouter à une règle de stratégie de sécurité existante ou clonée.

Vous pouvez sort and filter (trier et filtrer) les applications dans **Apps Seen (Applications vues)** par sous-catégorie, risque, volume de trafic vu au cours des 30 derniers jours, ou quand l'application a été vue pour la première ou la dernière fois.

**STEP 4 |** Sélectionnez **Applications** dans **Create Cloned Rule (Créer une règle clonée)** ou **Add to Existing Rule (Ajouter à une règle existante)**, selon la manière dont vous souhaitez gérer les applications.




*Le nombre maximal d'applications que vous pouvez cloner à l'aide de **Create Cloned Rule (Créer une règle clonée)** est de 1 000 applications. S'il y a plus de 1 000 applications que vous souhaitez déplacer vers une règle différente, utilisez plutôt **Add to Existing Rule (Ajouter à la règle existante)**. Si vous souhaitez déplacer les applications vers une nouvelle règle, créez simplement la règle d'abord (**Policies (Politiques)** > **Security (Sécurité)**), puis utilisez l'optimiseur de politique pour les ajouter à cette règle.*

**STEP 5 |** Ajoutez les applications sélectionnées à une règle clonée ou à une règle existante.

**Create Cloned Rule (Créer la règle clonée)** :

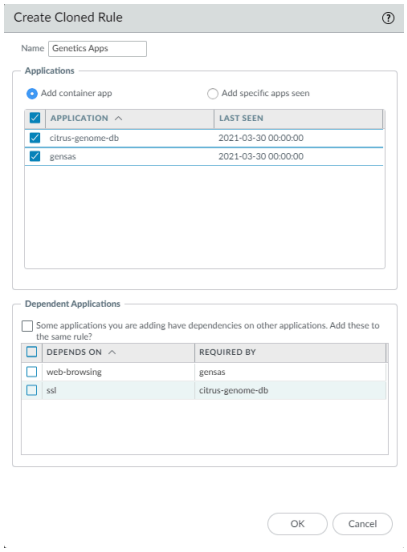
1. Saisissez le **Name (Nom)** (le nom de la règle clonée, qui apparaîtra dans la base de règles de la politique de sécurité immédiatement au-dessus de la règle d'origine). La règle clonée a la même action (autoriser ou refuser) que la règle d'origine.
2. Choisissez **Add container app (ajouter une application conteneur)** (par défaut) ou uniquement d'ajouter des **Add specific apps seen (applications spécifiques vues)**.

   Lorsque vous ajoutez l'application de conteneur, vous ajoutez également toutes les applications fonctionnelles dans ce conteneur, y compris les applications fonctionnelles qui n'ont pas encore été vues sur le pare-feu. Par exemple, si vous ajoutez l'application de conteneur « facebook », cela ajoute également facebook-base, facebook-chat, facebook-posting, etc., ainsi que toutes les futures applications ajoutées au conteneur. Le conteneur et ses applications fonctionnelles sont soumis à la règle de stratégie de sécurité que vous clonez. La sélection de l'application de conteneur assure essentiellement la pérennité et automatise la sécurité des applications du conteneur afin que vous n'ayez pas à ajouter manuellement de nouvelles applications dans ce conteneur à votre Politique de sécurité.

   L'ajout uniquement des applications spécifiques vues signifie que seules les applications que vous avez sélectionnées sont ajoutées à la règle clonée. Si de nouvelles applications dans la même application de conteneur arrivent au pare-feu, la règle clonée ne les contrôle pas et vous devez décider manuellement comment gérer les nouvelles applications.
3. Dans certains cas, les applications que vous souhaitez ajouter à une règle nécessitent (en dépendent) d'autres applications pour fonctionner. Dans ces cas, la boîte de dialogue **Create Cloned Rule (Créer une règle clonée)** comprend des **Dependent Applications (applications dépendantes)**, dans lesquelles vous pouvez choisir d'ajouter ou non ces applications à la règle

clonée. Ajoutez les applications dépendantes à la règle pour vous assurer que les applications sélectionnées fonctionnent correctement.



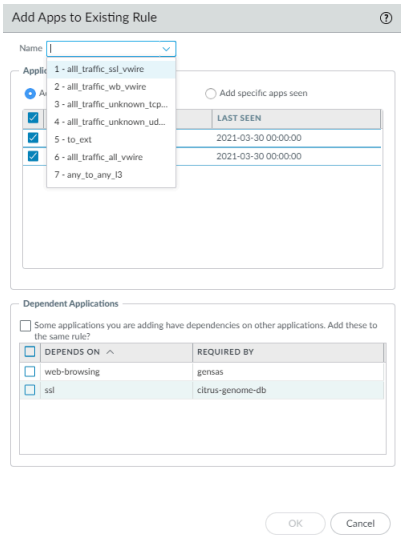

4. Cliquez sur **OK** pour ajouter les applications à la règle clonée.
5. **Validez** les modifications.

**Add Apps to Existing Rule (Ajouter des applications à une règle existante)** :

1. Sélectionnez le **Name (Nom)** de la règle existante à laquelle vous souhaitez ajouter les applications sélectionnées.
2. Comme pour le clonage de la règle pour ajouter des applications, vous pouvez choisir **Add container app (ajouter une application conteneur)** ou **Add specific apps seen (ajouter des applications spécifiques vues)**. L'ajout de l'application de conteneur ajoute toutes les applications fonctionnelles dans le conteneur et toutes les futures applications ajoutées à ce conteneur. L'ajout uniquement des applications spécifiques ajoute uniquement les applications sélectionnées spécifiques.
3. Comme pour le clonage de la règle, dans certains cas, les applications que vous souhaitez ajouter à une règle nécessitent (dépendent d') d'autres applications pour fonctionner. Dans ces cas, la boîte de dialogue **Add Apps to Existing Rule (Ajouter des applications à la règle existante)** comprend des **Dependent Applications (applications dépendantes)**, dans lesquelles vous pouvez choisir d'ajouter ou non ces applications à la règle clonée. Ajoutez

les applications dépendantes à la règle pour vous assurer que les applications sélectionnées fonctionnent correctement.




4. Cliquez sur **OK** pour ajouter les applications à la règle existante.
5. **Validez** les modifications.

# Remplacement d'un pare-feu RMA (ACE)

Pour restaurer la configuration d'un pare-feu géré lorsqu'il existe une autorisation de retour de marchandise (RMA), la procédure consiste à :

- Passer en revue Before Starting RMA Firewall Replacement (Avant de commencer le remplacement d'un pare-feu RMA).
- Dans Panorama, remplacez le numéro de série de l'ancien pare-feu par le numéro de série du nouveau pare-feu.
- Dans l'interface de ligne de commande du pare-feu, vérifiez que le pare-feu est en ligne et connecté au service Knowledge afin que le pare-feu puisse télécharger le catalogue d'applications cloud :

  1. Accédez à la CLI du pare-feu.
  2. En mode opérationnel, vérifiez la connexion App-ID cloud :

     ```
     admin@vm1> show cloud-appid connection-to-cloud (admin@vm1>
     afficher la connexion cloud-appid au cloud)
     ```

     Si le pare-feu est connecté au cloud, la commande show renvoie :

     ```
     ACE Cloud server: kcs.ace.tpcloud.paloaltonetworks.com:443Cloud
     connection: connected (Serveur ACE Cloud :
     kcs.ace.tpcloud.paloaltonetworks.com:443Sa connexion cloud :
     connecté)
     ```

     Des informations sur la connexion s'affichent également. Si le pare-feu n'est pas connecté au cloud, vérifiez si les services DNS fonctionnent et vérifiez tout autre problème de connectivité lié au réseau.

- Une fois le pare-feu connecté au cloud App-ID, Restore the Firewall Configuration after Replacement (restaurez la configuration du pare-feu après le remplacement).

## Impact de l'expiration de la licence ou de la désactivation d'ACE

Si vous activez App-ID Cloud Engine (ACE) sur un pare-feu, téléchargez des ID d'application ACE sur le pare-feu, puis utilisez ces ID d'application dans des objets tels que les filtres d'application et dans les règles de stratégie de sécurité, vous devez comprendre ce qui se passe si la licence SaaS Security Inline expire ou si vous disable ACE (désactivez ACE). La désactivation d'ACE et l'expiration de la licence SaaS Security Inline affectent toutes deux les ID d'application ACE téléchargés, le catalogue d'ID d'application ACE, les règles de politique de sécurité qui contrôlent les ID d'application ACE et les objets qui incluent des ID d'application ACE. L'effet est le même, sauf indication contraire :

- Les APP-IDs ACE restent sur le pare-feu, mais le pare-feu cesse d'appliquer les APP-ID ACE dans la politique de sécurité.

  Les règles de politique de sécurité qui contrôlent les ID d'application ACE ne contrôlent plus les ID d'application ACE même s'ils sont visibles dans la règle. Le trafic qui était contrôlé par des règles ssl, de navigation Web, unknown-tcp ou unknown-udp avant l'activation d'ACE sur le pare-feu est à nouveau contrôlé par ces règles jusqu'à ce que vous mettiez à jour et activiez la licence SaaS Security Inline et/ou réactivez ACE ou modifiez ces règles.
- L'application des règles de politique de sécurité basées sur les IED d'application ACE s'arrête dans les 4 à 6 heures suivant l'expiration de la licence (sur la base d'une minuterie qui vérifie périodiquement l'état de la licence).

  L'application des règles de politique de sécurité basées sur les AI d'application ACE s'arrête immédiatement après la validation de l'ACE désactivant sur le pare-feu.

  ***La désactivation d'ACE arrête l'application des règles de politique de sécurité basées sur les APP-ID ACE dès que vous validez la modification, même si la licence SaaS Security Inline est toujours valide et active.***
- Le catalogue des ID d'application ACE reste sur le pare-feu et sur Panorama, mais le moteur cloud ne met plus à jour le catalogue.
- La connexion du pare-feu à ACE ne fonctionne plus. Si vous réactivez ACE ou renouvelez la licence SaaS Security Inline, le téléchargement de toutes les mises à jour du catalogue peut prendre un certain temps.
- Si la licence SaaS Security Inline expire, le service ACE cesse de fonctionner dans les 4 à 6 heures.

  ***Panorama ne nécessite pas de licence SaaS Security Inline, il n'y a donc pas de licence pour expirer sur Panorama. Toutefois, lorsque la licence expire sur les pare-feu gérés, les transferts de configuration vers ces pare-feu à partir de Panorama échouent s'ils contiennent des configurations ACE dans la politique de sécurité ou dans les groupes d'applications.***
- Les objets tels que les filtres d'application et les groupes d'applications ne sont pas modifiés, mais les ID d'application ACE que vous avez placés dans ces objets ne sont plus appliqués même si les ID d'application ACE sont toujours visibles.
- Si vous utilisez la recommandation de politique SaaS, le pare-feu ne peut plus extraire les recommandations de stratégie SaaS, de sorte que l'administrateur SaaS ne peut pas envoyer de nouvelles recommandations de politique au pare-feu. Les recommandations de politique qui

ont été téléchargées avant l'expiration de la licence restent dans la configuration, mais elles ne sont pas appliquées (même comportement que les politiques de sécurité configurées avec les INFORMATIONS d'application ACE lorsque la licence expire ou que ACE est désactivé).

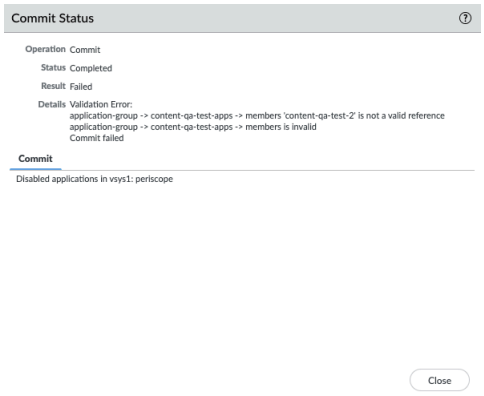
## Échec de la validation en raison de la restauration du contenu cloud

Bien que cela soit extrêmement improbable, il est possible que les ID d'application ACE doivent être annulés (restaurés) en raison de mauvaises métadonnées ou de problèmes avec les applications. Si ACE doit rétablir les App-ID et que vous avez utilisé ces App-ID dans une règle de politique de sécurité (directement ou dans un groupe d'applications), les actions de validation échouent jusqu'à ce que ces applications soient supprimées des règles de politique de sécurité et des objets.

S'il devient nécessaire de restaurer les App-ID, ACE rétablit tous les derniers App-ID, signatures, métadonnées, catégories, sous-catégories et balises du catalogue ACE. La suppression des App-ID du catalogue les supprime du pare-feu, c'est pourquoi l'action de validation échoue lorsque les App-ID sont utilisés dans la politique de sécurité.

***Si vous n'avez pas utilisé les applications que ACE a dû restaurer dans la stratégie de sécurité, il n'y a aucun impact sur la configuration et les actions de validation réussissent.***

Lorsque vous essayez de valider une configuration après une restauration de contenu ACE, le message d'échec de validation répertorie les applications que ACE a annulées, comme dans cet exemple de **Validation Error (erreur de validation)** :




Pour résoudre le problème, vous devez supprimer les applications répertoriées des Règles de stratégie de sécurité, qu'elles aient été ajoutées directement à une règle ou qu'elles aient été ajoutées à l'aide d'un Groupe d'applications. Si l'application est utilisée dans un Groupe d'applications, supprimez-la du Groupe d'applications.

Dans cet exemple, `content-qa-test-2` est l'application annulée, qui est référencée dans le groupe d'applications `content-qa-test-apps`. Une fois que vous avez supprimé `content-qa-test-2` du Groupe d'applications, les actions de validation réussissent.

## Résoudre les problèmes liés à App-ID Cloud Engine

Cette rubrique fournit des informations générales de dépannage pour App-ID Cloud Engine (ACE).

- Pour vérifier si un appareil dispose d'une licence SaaS Security Inline valide, exécutez la commande CLI opérationnelle **`show cloud-appid connection-to-cloud`**. En cas de problème, la commande renvoie le message suivant :

  **`Erreur ACE : Échec de la vérification de la licence. Vérifiez si la licence SaaS est installée et si la connexion activeCloud : échec`**

  De plus, la sortie indique l'heure de la dernière connexion réussie, par exemple : **`Dernière connexion gRPC réussie : 2021-05-20 16:00:00 -0800 PDT`**

  Si la licence est installée et que la connexion à ACE est bonne, la commande renvoie l'URL de la connexion au serveur cloud ACE et l'état **`Cloud connection: connected (Connexion cloud : connecté)`**, ainsi que les statistiques de connexion et l'état du certificat de l'appareil, y compris les dates de validité du certificat.
- Panorama Valider tous/transférer aux pare-feux gérés échoue. Vérifiez si l'une des conditions suivantes existe et réparez-les :
  - Les pare-feux gérés disposent-ils d'une licence SaaS Security Inline valide ? Si ce n'est pas le cas, ils n'ont pas le catalogue ACE et l'opération valider tous/gtransférer échoue. Selon que vous souhaitez que des pare-feux gérés gèrent les ID d'application ACE, supprimez les objets ACE de la configuration transférée et réessayez ou installez des licences SaaS Security Inline valides sur les pare-feux gérés, attendez que le catalogue soit téléchargé.

    *Il existe moins de quatre mille App-ID fournis par le contenu. Après avoir téléchargé le catalogue ACE, vous voyez plusieurs milliers d'autres applications sur le pare-feu et pouvez confirmer en cochant **Objects (Objets)** > **Applications** ou en utilisant la commande CLI opérationnelle `show cloud-appid cloud-app-data application all`pour voir les nouveaux ID d'application.*
  - La connexion entre un pare-feu géré et ACE a-t-elle été panne ? Vérifiez la connexion au cloud ACE et restaurez la connexion si nécessaire.

    La commande CLI opérationnelle **`show cloud-appid connection-to-cloud`** fournit l'état de la connexion cloud et l'URL du serveur cloud ACE.
  - Le catalogue ACE sur Panorama et le catalogue ACE sur les pare-feu gérés sont désynchronisés, ce qui entraîne des configurations transmises qui incluent des applications ACE qui ne figurent pas dans le catalogue du pare-feu. Si la connexion entre le pare-feu et ACE est établie, le catalogue obsolète sera mis à jour automatiquement dans les prochaines minutes et résoudra le problème. (Attendez cinq minutes et réessayez.)

    *Vous pouvez également exécuter la commande CLI opérationnelle `debug cloud-appid cloud-manual-pull check-cloud-app-data` pour mettre à jour le catalogue manuellement.*
  - Les pare-feux exécutent-ils tous PAN-OS 10.1 ou version ultérieure ? (La promotion de configurations qui référencent des applications et des objets ACE à des pare-feu exécutant des versions antérieures à PAN-10 10.1 n'est pas autorisée.)
- Dans une paire HA (active/active ou active/passive) qui a une configuration ACE, si vous exécutez la commande opérationnelle **`show session all (afficher toutes les sessions)`** ou **`show session id (afficher l'id de la session) <id>`**,la sortie pour les applications ACE peut afficher le numéro d'ID d'application global au lieu du nom de l'application. Le pare-feu affiche uniquement le nom de l'application si son plan de données contient les

données de l'application cloud. Si ce n'est pas le cas, le pare-feu affiche le numéro de l'ID d'application global de l'application à la place.

- Pour réinitialiser la connexion à ACE (la connexion gRPC), exécutez la commande CLI opérationnelle **debug cloud-appid reset connection-to-cloud**.
- Affichez les applications ACE téléchargées sur l'appareil avec la commande CLI opérationnelle **show cloud-appid cloud-app-data application**. Vous pouvez afficher toutes les applications téléchargées ou des applications individuelles par ID d'application ou nom d'application.
- Affichez les demandes en attente pour les ID d'application ACE avec la commande CLI opérationnelle **show cloud-appid signature-dp pending-request**. La sortie inclut le nombre de fois que le pare-feu a envoyé la demande à ACE (**tries (essais)**). Après onze essais, l'opération d'envoi est épuisée.
- La commande CLI opérationnelle **show cloud-appid** propose des options plus utiles :

```
admin@PAN-ACE-VM-1> show cloud-appid ?
> app-objects-in-policy         Show application-filter/application-
groups referred in policy
> app-to-filtergroup-mapping    Show application to matched filter
 and groups
> application                   Show Application info for UI
> application-filter            Show cloud apps in application-
filters
> application-group             Show cloud apps in application-
groups
> cloud-app-data                Show cloud application, container
 and metadata
> connection-to-cloud           Show gRPC connection status to cloud
 application server
> ha-info                       Show statistics of cloud application
 high availability
> overlap-appid                 Show duplicated applications in
 predefined content
> signature-dp                  Show cloud signatures and
 applications used on DP
> task                          Show task on management-plane
> transaction                   Show cloud application transaction
> version                       Show Cloud-AppID version
```

- Pour afficher les compteurs globaux pour ACE, exécutez la commande CLI opérationnelle **show counter global filter value all category cad** (**cad** signifie « cloud app-identification »).
- Pour afficher les statistiques des octets et des paquets reçus et envoyés vers/depuis la mémoire partagée et vers/depuis le client de sécurité pour des services tels que ACE, DLP et IoT, exécutez la commande opérationnelle **show ctd-agent statistics**.
- Si vous remarquez une différence entre le nombre d'applications qui correspondent à un filtre d'application lorsque vous regardez dans l'interface utilisateur et lorsque vous regardez dans l'interface de ligne de commande, c'est en raison de la façon dont le pare-feu compte les

applications correspondantes dans les interfaces utilisateur par rapport à l'interface de ligne de commande :

- Lorsque vous examinez un filtre d'application dans **Objects (Objets)** > **Application Filters (Filtres d'application)**, le pare-feu affiche toutes les applications correspondantes dans le catalogue ACE, que le pare-feu ait ou non vu ces applications et téléchargé leurs ID d'application, et le nombre de personnes inclut toutes ces applications.
- Lorsque vous examinez un filtre d'application dans l'interface de ligne de commande avec la commande opérationnelle `show cloud-appid application-filter,` le pare-feu affiche uniquement le nombre d'applications correspondantes pour lesquelles le pare-feu a téléchargé des ID d'application ACE.

Pour cette raison, l'interface utilisateur peut afficher plus d'applications correspondantes que l'interface de ligne de commande pour le même filtre d'application.

***La même chose s'applique aux Groupes d'applications lorsque vous les regardez dans l'interface utilisateur par rapport à l'interface de ligne de commande.***

- Les APP-ID ACE sont pris en charge uniquement pour la politique de sécurité. Les APP-ID ACE ne sont pris en charge pour aucun autre type de politique.

  Toutefois, lorsque vous configurez la politique QoS ou SD-WAN, les ID d'application ACE sont visibles (peuvent être sélectionnés) et peuvent être présents dans les groupes d'applications ou les filtres d'application appliqués à la règle, mais leur ajout à la politique QoS ou SD-WAN n'a aucun effet sur le trafic de l'application. (Les politiques QoS et SD-WAN ne contrôlent pas le trafic des applications.)

# Recommandation de politique d'ID d'application SaaS

La prolifération rapide des applications SaaS rend difficile l'attribution d'identifiants d'application spécifiques à toutes, la visibilité sur ces applications et leur contrôle. Les règles de politique de sécurité qui autorisent SSL, la navigation Web ou « toute » application peuvent autoriser des applications SaaS non autorisées qui peuvent introduire des risques de sécurité pour votre réseau. Pour obtenir une visibilité sur ces applications et les contrôler sur le pare-feu, les administrateurs de sécurité SaaS peuvent recommander des règles de politique de sécurité avec des identifiants d'application SaaS spécifiques fournis par App-ID Cloud Engine (ACE) aux administrateurs de pare-feu PAN-OS. Les administrateurs PAN-OS peuvent importer ces règles sur les pare-feu disposant d'un abonnement SaaS Security Inline.

*La recommandation de politique SaaS nécessite un abonnement* SaaS Security Inline*. Chaque appareil qui utilise le moteur de recommandation de stratégie SaaS doit* generate and install (générer et installer) *un certificat d'appareil valide ou* use Panorama (utiliser Panorama) *pour générer et installer un certificat d'appareil valide.*

*Une* SaaS Security Inline connection (connexion SaaS Security Inline) *à Cortex Data Lake (*CDL*) est requise pour la visibilité SaaS.* Configure Log Forwarding (Configurez le transfert de journal) *vers CDL et activez le transfert de journal avec le profil de transfert de journal approprié dans les règles de politique de sécurité. Au minimum, vous devez transférer les journaux de trafic et les journaux d'URL vers CDL pour que SaaS Security Inline fonctionne correctement.*

*Toutes les plates-formes matérielles qui prennent en charge PAN-OS 10.1 ou version ultérieure prennent en charge la recommandation de politique SaaS et tous les appareils sur lesquels vous souhaitez utiliser la recommandation de politique SaaS nécessitent PAN-OS 10.1 ou version ultérieure. Panorama ne peut pas transférer et valider les recommandations de politique SaaS sur des pare-feux sur lesquels aucune licence SaaS Security Inline n'est installée ou sur des pare-feux qui exécutent une version antérieure de PAN-OS à 10.1.*

- Le *SaaS Security Administrator's Guide (Guide de l'administrateur de sécurité SaaS)* décrit la procédure de l'administrateur de sécurité SaaS pour créer des recommandations de règles de politique de sécurité, puis les transmettre au pare-feu.
- Le *PAN-OS Administrator's Guide (Guide de l'administrateur PAN-OS)* décrit comment l'administrateur PAN-OS importe et gère les recommandations de stratégie de l'administrateur de sécurité SaaS.

L'administrateur de sécurité SaaS crée la nouvelle règle, ajoute des applications, des utilisateurs et des groupes à la règle et définit l'action de la règle. L'action de la règle peut être autorisée ou bloquée ; aucune autre action n'est autorisée pour les règles transférées. L'administrateur de sécurité SaaS transmet ensuite la règle aux appareils appropriés et la règle apparaît dans l'interface du pare-feu (**Device (Périphérique)** > **Policy Recommendation (Recommandation de politique)** > **SaaS**).

L'administrateur PAN-OS évalue la règle recommandée et décide de l'implémenter sur le pare-feu. Si l'administrateur PAN-OS choisit d'implémenter la règle, l'administrateur l'importe sur

le pare-feu et sélectionne où placer la règle de politique dans la base de règles du pare-feu. Lorsqu'un administrateur PAN-OS importe une recommandation de politique, le pare-feu crée automatiquement les profils HIP, les balises et les groupes d'applications requis (l'administrateur PAN-OS n'a pas à le faire manuellement).

*Si l'administrateur de sécurité SaaS envoie des profils de sécurité avec la recommandation de politique et que ces profils n'existent pas sur le pare-feu, l'importation du pare-feu échoue. Si les profils existent déjà sur le pare-feu, l'importation réussit.*

Si l'administrateur de sécurité SaaS met à jour une recommandation de règle de politique, l'administrateur PAN-OS voit la mise à jour et l'importe dans le pare-feu. Si l'administrateur de sécurité SaaS supprime une recommandation de règle de politique, l'administrateur PAN-OS voit l'action et supprime la règle de la base de règles de la politique de sécurité du pare-feu.

*Si la licence SaaS Security Inline expire, le pare-feu n'extrait plus les recommandations de politique SaaS, de sorte que vous ne voyez aucune nouvelle recommandation. Cependant, les règles de politique de sécurité que vous avez déjà importées continuent de fonctionner.*

*Si vous désactivez ACE, le pare-feu ne reçoit plus de nouvelles signatures d'application cloud et App-ID et le pare-feu ne peut pas importer les recommandations de politique SaaS basées sur les nouveaux App-ID ACE.*

Le ACE deployment process (processus de déploiement ACE) (connexion au cloud, installation des certificats d'appareil, activation de la licence sur le portail de sécurité SaaS et transmission à Panorama et aux pare-feu, etc.) configure également la recommandation de politique SaaS.

*Mettez à jour toutes les appareils avec les dernières* content updates (mises à jour du contenu) *des menaces.*

Les ajouts d'interface utilisateur pour cette nouvelle fonctionnalité incluent :

- **Device (Périphérique)** > **Policy Recommendation (Recommandation de politique)** > **SaaS** affiche les recommandations de politique des administrateurs SaaS et permet aux administrateurs de pare-feu d'importer, de mettre à jour, de supprimer et de contrôler les politiques SaaS recommandées. L'affichage de la page inclut les Groupes d'applications configurés par l'administrateur SaaS pour la politique.
- ACE deployment process (accès à l'interface basé sur les rôles) (**Device (Périphérique)** > **Admin Roles Rôles d'administrateur**) dispose d'une nouvelle option dans l'onglet **Web UI** pour les autorisations de recommandation de politique SaaS : **Device (Périphérique)** > **Policy Recommandation (Recommandation de politique)** > **SaaS**.
- Les recommandations de politique SaaS sont automatiquement balisées **SaaSSecurityRecommended**, qui s'affiche dans la colonne **Tags (Balises)** de l'interface.

Vous pouvez importer et mettre à jour les recommandations de politique SaaS poussées par les administrateurs SaaS et supprimer les recommandations de politique SaaS que l'administrateur SaaS a supprimées.

- Recommandation de politique d'importation SaaS
- Importer la recommandation de stratégie SaaS mise à jour
- Supprimer la recommandation de stratégie SaaS supprimée

# Recommandation de politique d'importation SaaS

Lorsqu'un administrateur de sécurité SaaS envoie des recommandations de règles de politique de sécurité à un pare-feu PAN-OS, l'administrateur de pare-feu PAN-OS peut importer ces règles sur le pare-feu pour obtenir une visibilité et un contrôle des applications dans la recommandation de politique.

Consultez le ***SaaS Security Administrator's Guide (Guide de l'administrateur de sécurité SaaS)*** pour les recommandations de politique et les procédures push de l'administrateur SaaS. Cette procédure montre aux administrateurs PAN-OS comment importer des recommandations de politique.

*Si l'administrateur de sécurité SaaS envoie des profils de sécurité avec la recommandation de politique et que ces profils n'existent pas sur le pare-feu, l'importation du pare-feu échoue. Si les profils existent déjà sur le pare-feu, l'importation réussit.*

**STEP 1 |** **Device (périphérique)** > **Policy Recommendation (recommandation de politique)** > **SaaS** sur le pare-feu et **Panorama** > **Policy Recommendation (Recommandation de politique)** > **SaaS** sur Panorama affichent toutes les recommandations de politique SaaS transmises par l'administrateur SaaS. Poussez les recommandations de politique de Panorama vers les pare-feu gérés.

**STEP 2 |** Actualiser ( ) **Device (périphérique)** > **Policy Recommendation (Recommandation de politique)** > **SaaS** (ou **Panorama** > **Policy Recommendation (Recommandation de politique)** > **SaaS**) pour vous assurer que les recommandations de politique SaaS sont à jour.

*Chaque fois que vous transférez des recommandations de politique de Panorama vers des pare-feux gérés, actualisez ( ) la page sur les pare-feux pour vous assurer que les recommandations sont à jour.*

Les recommandations de politique récemment transmises s'affichent en haut de l'écran. **Active Recommandations (Recommandations actives)** affiche la valeur **active** et **(Nouvelles mises à jour disponibles)** affiche la valeur **Yes (Oui)**.

**STEP 3 |** Sélectionnez une nouvelle recommandation de politique.

Vous importez une recommandation de politique à la fois. La colonne **Applications** affiche un groupe d'applications pour chaque recommandation de politique. Cliquez sur le nom du groupe pour voir les applications de ce groupe.

La colonne **Device (périphérique)** affiche l'appareil source que l'administrateur SaaS a configuré pour la règle. Le terme « SaaS » précède l'appareil source. Le périphérique source peut être :

- MCD—Périphérique conforme géré
- MNCD—Périphérique non conforme géré
- UMCD—Périphérique conforme non géré
- UMNCD—Périphérique non conforme non géré

Par exemple, **SaaS - MCD** indique un périphérique source géré et conforme.

**STEP 4 |** **Import Policy Rule (Importer la règle de politique)**.

Dans la boîte de dialogue **Import Policy Rule (Importer une règle de stratégie)** :

- **Name (Nom)** : nommez la règle importée en utilisant un nom qui décrit l'intention de la règle.

  *Si vous spécifiez un nom de règle qui existe déjà dans la base de Règles de la politique de sécurité, la règle importée écrase la règle existante.*

- **After Rule (Après la règle)** : sélectionnez la règle après laquelle placer la règle SaaS importée. Pensez à la base de règles du pare-feu et à la manière dont la nouvelle règle peut affecter les règles existantes. Si vous ne sélectionnez pas de règle (**No Rule Selection(Aucune sélection de règle)**), la règle est placée en haut de la base de règles de la politique de sécurité. Dans certains cas, ce n'est pas là que vous voulez placer la règle. Par exemple, vous pouvez souhaiter que certaines règles de blocage particulières soient toujours au sommet de la base de règles, comme le blocage du protocole QUIC. Soyez conscient de l'intention de la règle importée et veillez à ne pas masquer les règles existantes.

La **Description** provient de la description saisie lors de la création de la règle par l'administrateur SaaS. Vous pouvez le modifier ou le laisser tel quel.

*Le processus d'importation crée automatiquement un Groupe d'applications pour les applications de la recommandation de politique. Le nom du Groupe d'applications est dérivé du nom que l'administrateur de sécurité SaaS a donné à la règle. Le pare-feu crée également automatiquement tous les profils et balises HIP que l'administrateur SaaS a appliqués à la règle.*

**STEP 5 |** Cliquez sur **OK** pour importer la règle et l'ajouter à la base de règles de la politique de sécurité à la position sélectionnée dans **After Rule (Après la règle)**.

**STEP 6 |** Lorsque vous voyez le message d'état « Vous avez mis à jour avec succès vos règles de politique de sécurité », cliquez sur **OK**.

La colonne **Location (Emplacement)** affiche désormais l'emplacement de la règle (vsys) sur le pare-feu, qui correspond au vsy auquel l'administrateur SaaS a transmis la règle.

**STEP 7 |** Confirmez que la règle de politique importée se trouve dans la base de règles de politique de sécurité (**Security (Sécurité)** > **Policies (Politiques)**) à l'emplacement spécifié et que le pare-feu a créé les objets associés.

Par exemple, vérifiez la règle de politique de sécurité pour :

- Le **Source Device (périphérique source)** de la règle est renseigné et affiche le périphérique source de la règle dans l'onglet **Source**.
- Le groupe d'applications remplit l'onglet **Application** de la règle.
- Les profils associés sont attachés à la règle (onglet **Actions**).

Vérifiez également que :

- **Objects (Objets)** > **Applications Group (Groupe d'applications)** affiche le Groupe d'applications importé.
- Les **Objects (objets)** > **GlobalProtect** > **HIP Objects (objets HIP)** et les **Objects (Objets)** > **GlobalProtect** > **HIP Profiles (Profils HIP)** affichent les informations HIP transmises par l'administrateur de sécurité SaaS avec la règle.

# Importer la recommandation de stratégie SaaS mise à jour

Lorsqu'un administrateur de sécurité SaaS envoie des recommandations de règles de stratégie de sécurité à un pare-feu PAN-OS (ou Panorama), l'administrateur PAN-OS peut importer ces règles pour obtenir une visibilité et un contrôle des applications dans la recommandation de stratégie. Cependant, si l'administrateur SaaS met à jour la règle, par exemple en ajoutant ou en supprimant des applications, la règle doit également être mise à jour sur le pare-feu.

*Si l'administrateur de sécurité SaaS envoie des groupes d'applications, des profils HIP ou des balises nouveaux ou mis à jour, le pare-feu crée ou met automatiquement à jour ces objets. Si l'administrateur de sécurité SaaS envoie des profils de sécurité avec la mise à jour des recommandations de politique et que ces profils n'existent pas sur le pare-feu, l'importation du pare-feu échoue. Si les profils existent déjà sur le pare-feu, l'importation réussit.*

**STEP 1 |** Actualiser ( ) **Device (périphérique)** > **Policy Recommendation (Recommandation de politique)** > **SaaS** (ou **Panorama** > **Policy Recommendation (Recommandation de politique)** > **SaaS**) pour vous assurer que vous voyez toutes les dernières recommandations de politique SaaS que l'administrateur Saas a transmises au pare-feu.

**STEP 2 |** Vérifiez **New Updates Available (Nouvelles mises à jour disponibles)**.

Si la valeur de la colonne **New Updates Available (Nouvelles mises à jour disponibles)** est **No (Non)**, aucune mise à jour de la règle n'est effectuée. Si la valeur est **Yes (Oui)**, alors l'administrateur SaaS a transmis une mise à jour de la règle vers le pare-feu. De plus, **Active Recommendations (Recommendations actives)**affiche la valeur **active**.

**STEP 3 |** Cliquez sur le nom du groupe d'applications dans la colonne **Applications** pour afficher la liste mise à jour des applications contrôlées par la règle.

**STEP 4 |** Sélectionnez une recommandation de stratégie à mettre à jour.

Vous ne mettez à jour qu'une seule recommandation de politique à la fois.

**STEP 5 |** Cliquez sur **Import Policy Rule (Importer une règle de politique)** pour importer la stratégie (s'il n'y a pas de mise à jour de la règle, cette option est grisée et vous ne pouvez pas la sélectionner).

La boîte de dialogue **Import Policy Rule (Importer une règle de politique)** s'affiche. Le **Name (nom)** est déjà renseigné et ne peut pas être modifié car la règle a déjà été importée. **After Rule (après la règle)** ne peut pas non plus être modifié dans la boîte de dialogue, mais si vous souhaitez modifier l'emplacement de la règle dans la base de règles de la politique de sécurité, vous pouvez le faire sur **Policies (Politiques)** > **Security (Sécurité)**de la même manière que vous modifiez la position de n'importe quelle Règle de politique de sécurité. Vous pouvez modifier la **Description** ou la laisser telle quelle.

**STEP 6 |** Cliquez sur **OK**.

**STEP 7 |** Cliquez sur **Yes (Oui)** dans **Confirm Change (Confirmer la modification)** pour importer la règle mise à jour (ou cliquez sur **No (Non)** si vous ne souhaitez pas importer la règle modifiée).

Le pare-feu modifie automatiquement le Groupe d'applications, les profils HIP et les balises associées à la règle.

# Supprimer la recommandation de stratégie SaaS supprimée

Lorsqu'un administrateur de sécurité SaaS envoie des recommandations de règles de stratégie de sécurité à un appareil PAN-OS, l'administrateur PAN-OS peut importer ces règles pour gagner en visibilité et en contrôle sur les applications de la recommandation de stratégie. Toutefois, si l'administrateur de la sécurité SaaS supprime la règle, vous devez également supprimer cette règle de l'appareil PAN-OS.

Lorsqu'un administrateur de sécurité SaaS supprime une règle, la colonne **Active Recommendation (Recommandation active)** affiche la valeur **removed (supprimée)** (pour les règles valides, la valeur est **active**).

**STEP 1 |** Sélectionnez une règle que l'administrateur de sécurité SaaS a **removed (supprimée)** (vous ne pouvez sélectionner qu'une seule règle à supprimer à la fois).

*L'option **Import Policy Rule (Importer la règle de politique)** est grisée car la règle ne peut plus être importée.*

**STEP 2 |** Cliquez sur **Remove Recommendation Mapping (Supprimer le mappage des recommandations)**.

Cela supprime le mappage local de la règle de stratégie de sécurité sur le pare-feu. Par exemple, les mappages vers les emplacements, les utilisateurs et la règle sont supprimés. La boîte de dialogue **Remove Recommendation Mapping (Supprimer le mappage de recommandations)** vous indique l'emplacement de la règle afin que vous sachiez d'où la règle est supprimée.

**STEP 3 |** Cliquez sur **OK**.

**STEP 4 |** Dans la boîte de dialogue Confirmer la **modification,** cliquez sur **Oui** pour supprimer la règle de la base de données de recommandations de politique.

*Cette action supprime uniquement la règle de la liste des règles de recommandation de politique. Il ne supprime PAS la règle de la base de règles de politique de sécurité. Vous devez supprimer manuellement la règle de la base de règles.*

**STEP 5 |** Une boîte de dialogue **Status (État)** s'affiche pour confirmer que le mappage des recommandations de politique a été supprimé, mais vous devez toujours supprimer la règle de la base de règles de politique de sécurité.

**STEP 6 |** Accédez à **Policies (Politiques)** > **Security (Sécurité)** et supprimez la règle de la base de règles de politique de sécurité.

# >Passerelles au niveau de l'application

>Le pare-feu Palo Alto Networks ne classe pas le trafic par port et protocole ; il identifie plutôt l'application en se basant sur ses propriétés uniques et les caractéristiques de ses transactions à l'aide de la technologie App-ID. Certaines applications nécessitent, toutefois, le pare-feu pour ouvrir des***>pinholes*** dynamiques pour établir la connexion, déterminer les paramètres pour la session et négocier les ports qui seront utilisés pour le transfert de données ; ces applications utilisent les données utiles de la couche application pour communiquer les ports TCP ou UDP dynamiques sur lesquels l'application ouvre les connexions de données. Pour ce type d'applications, le pare-feu se sert d'Application Level Gateway (passerelle au niveau de l'application - ALG) et ouvre un pinhole pour une durée limitée et exclusivement pour transférer des données ou contrôler le trafic. Le pare-feu exécute aussi une réécriture NAT de la charge utile, le cas échéant.

- *>L'ALG pour H.323 (H.225 et H.248) n'est pas prise en charge en mode d'acheminement par contrôle d'accès.*
- *>Lorsque le pare-feu se sert d'ALG pour le Session Initiation Protocol (protocole d'initiation de session ; SIP), il effectue par défaut une réécriture NAT de la charge utile et ouvre des pinholes dynamiques pour les ports multimédia. Dans certains cas, en fonction des applications SIP utilisées dans votre environnement, les terminaux SIP sont dotés d'une intelligence NAT intégrée dans les systèmes de leurs clients. Dans ces cas, vous pourriez avoir besoin de désactiver la fonctionnalité ALG SIP pour empêcher le pare-feu de modifier les sessions de signalisation. Lorsque la fonctionnalité ALG SIP est désactivée, si le système App-ID détermine qu'il s'agit d'une session SIP, la charge utile ne sera pas traduite et les pinholes dynamiques ne seront pas ouverts. Reportez-vous à la section* >Désactivation de l'Application-Level Gateway (passerelle au niveau de l'application - ALG) du protocole SIP.

*>Lorsque vous utilisez les NAT Dynamic IP and Port (adresse IP et port dynamiques ; DIPP), le décodeur ALG du pare-feu Palo Alto Networks a besoin d'une combinaison d'adresse IP et de port (adresse d'envoi et port d'envoi) sous les en-têtes SIP (champs Contact et Via) pour arriver à traduire les en-têtes mentionnés et à ouvrir les sessions prévues en fonction de ceux-ci.*

>Le tableau suivant énumère les ALG pour IPv4, NAT, IPv6, NPTv6 et NAT64 et indique d'un crochet si l'ALG prend en charge chacun des protocoles (comme SIP).

>

| >App-ID | >IPv4 | >NAT | >IPv6 | >NPTv6 | >NAT64 |
|---|---|---|---|---|---|
| >SIP | ✓ > | ✓ > | ✓ > | >— | >— |
| >SCCP | ✓ > | ✓ > | ✓ > | >— | >— |
| >MGCP | ✓ > | ✓ > | >— | >— | >— |

| >App-ID | >IPv4 | >NAT | >IPv6 | >NPTv6 | >NAT64 |
|---|---|---|---|---|---|
| >FTP | ✓ | ✓ | ✓ | ✓ | >— |
| >RTSP | ✓ | ✓ | ✓ | ✓ | >— |
| >MySQL | ✓ | ✓ | >— | >— | >— |
| >Oracle/ SQLNet/ TNS | ✓ | ✓ | ✓ | ✓ | >— |
| >RPC | ✓ | ✓ | >— | >— | >— |
| >RSH | ✓ | ✓ | >— | >— | >— |
| >UNIStim | ✓ | ✓ | >— | >— | >— |
| >H.225 | ✓ | ✓ | >— | >— | >— |
| >H.248 | ✓ | ✓ | >— | >— | >— |

# Désactivation de l'Application-Level Gateway (passerelle au niveau de l'application ; ALG) du protocole SIP

Le pare-feu Palo Alto Networks utilise l'Application-Level Gateway (passerelle au niveau de l'application - ALG) du protocole Session Initiation Protocol (SIP) pour ouvrir des pinholes dynamiques au sein du pare-feu sur lequel la réécriture NAT est activée. Toutefois, certaines applications, telles que VoIP, sont dotées d'une intelligence NAT intégrée dans l'application du client. Dans ces cas, l'ALG SIP sur le pare-feu peut perturber les sessions de signalisation et provoquer l'arrêt du fonctionnement de l'application du client.

Pour résoudre ce problème, définissez une politique de contrôle prioritaire sur l'application pour le protocole SIP, mais cette approche désactive la fonctionnalité App-ID et de détection des menaces. Il est plutôt recommandé de désactiver l'ALG SIP, ce qui ne désactive pas App-ID ou la détection des menaces.

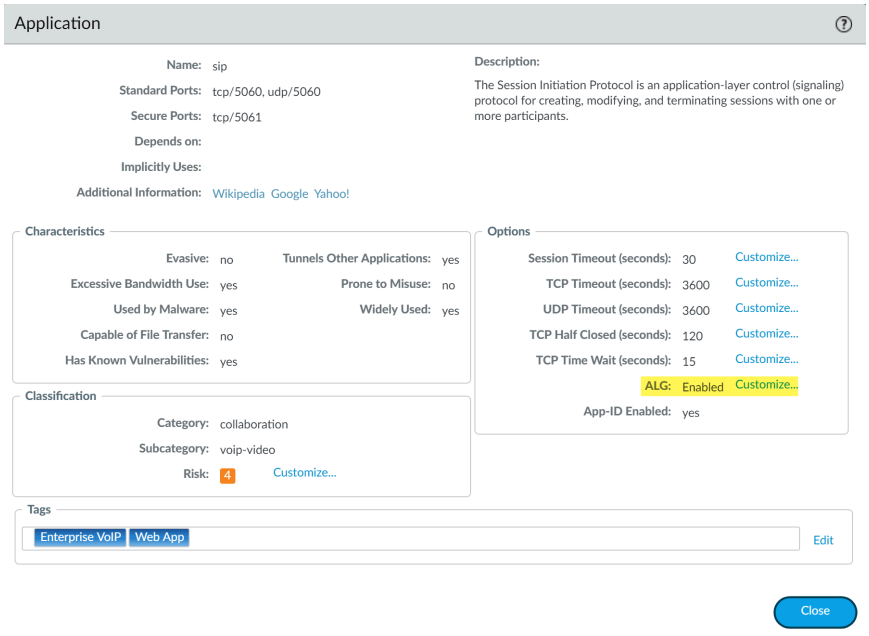
La procédure suivante décrit comment désactiver l'ALG SIP.

**STEP 1 |** Sélectionnez **Objects (Objets)** > **Applications (Applications)**.

**STEP 2 |** Sélectionnez l'application **sip (sip)**.

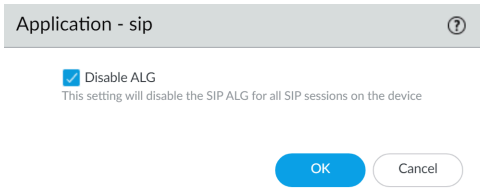
Vous pouvez saisir **sip** dans le champ **Search (Chercher)** pour permettre de trouver l'application SIP.

**STEP 3 |** Sélectionnez **Customize... (Personnaliser..).** pour **ALG (ALG)** dans la section Options (Options) de la boîte de dialogue Application (Application).



**STEP 4 |** Cochez la case **Disable ALG (Désactiver ALG)** dans la boîte de dialogue Application - SIP (Application - SIP) et cliquez sur **OK (OK)**.




**STEP 5 |** **Close (Fermez)** la boîte de dialogue Application (Application) et **Commit (Validez)** vos modifications.

# Utilisation d'en-têtes HTTP pour gérer l'accès aux applications SaaS

L'utilisation non approuvée des applications SaaS peut être un moyen pour vos utilisateurs de transmettre des informations de nature délicate à l'extérieur de votre réseau, généralement en accédant à une version cliente d'une application. Cependant, si vous devez autoriser l'accès à la version entreprise de ces applications à des personnes ou des organisations données, vous ne pouvez pas bloquer l'application SaaS complètement.

Vous pouvez utiliser des en-têtes HTTP personnalisés pour refuser les comptes de consommateurs SaaS tout en autorisant un compte d'entreprise spécifique. De nombreuses applications SaaS autorisent ou refusent l'accès aux applications selon les informations contenues dans les en-têtes HTTP spécifiques. Vous pouvez procéder à la Création d'entrées d'insertion d'en-têtes HTTP au moyen des types prédéfinis pour gérer l'accès aux applications SaaS populaires, comme Google G Suite et Microsoft Office 365. Palo Alto Networks® utilise les mises à jour de contenu pour maintenir des ensembles de règles prédéfinies spécifiques à ces applications ainsi que pour ajouter de nouveaux ensembles de règles prédéfinies.

Vous pouvez également procéder à la Création d'entrées d'insertion d'en-têtes HTTP personnalisées si vous voulez gérer l'accès à une application SaaS (qui utilise les en-têtes HTTP pour restreindre l'accès au service) pour laquelle Palo Alto Networks n'a pas fourni d'ensemble de règles prédéfinies.

Sachez que les applications SaaS commerciales utilisent toujours SSL ; le déchiffrement est donc toujours nécessaire pour procéder à l'insertion d'en-têtes HTTP. Vous pouvez configurer le pare-feu pour qu'il déchiffre le trafic en utilisant le déchiffrement de proxy de transfert SSL si le trafic n'est pas déjà déchiffré par un pare-feu en amont.

***Vous n'avez pas besoin d'une licence de filtrage des URL pour utiliser cette fonctionnalité.***

Pour comprendre comment utiliser les en-têtes HTTP pour gérer les applications SaaS, reportez-vous aux sections suivantes :

- Comprendre les en-têtes SaaS personnalisés
- Domaines utilisés par les types d'applications SaaS prédéfinis
- Création d'entrées d'insertion d'en-têtes HTTP au moyen des types prédéfinis
- Création d'entrées d'insertion d'en-têtes HTTP personnalisées

## Comprendre les en-têtes SaaS personnalisés

Avant de commencer, assurez-vous de comprendre les en-têtes HTTP personnalisés que vous utiliserez avec l'application SaaS que vous gérez. Vous devez comprendre ce que vous pouvez accomplir en utilisant ces en-têtes ainsi que les informations que vous devez spécifier pour atteindre vos objectifs.

Sachez que les applications SaaS qui utilisent des en-têtes personnalisés ne les utilisent pas toujours pour contrôler l'accès à ces types de comptes. Par exemple, Palo Alto Networks® offre un soutien prédéfini pour les en-têtes personnalisés de YouTube qui déterminent si les utilisateurs du réseau peuvent accéder au contenu restreint.

Vous devriez également lire la documentation propre à l'application SaaS à laquelle vous souhaitez contrôler l'accès afin de comprendre les en-têtes que vous devez utiliser pour cette application.

*Les limitations suivantes s'appliquent à l'insertion des en-têtes HTTP:*

- *Nombre de caractères maximum du nom de l'en-tête: 100.*
- *Nombre de caractères maximum de la valeur de l'en-tête: 512*

*Veuillez faire attention au fait que certaines applications SaaS peuvent définir des noms d'en-têtes personnalisés, ou assigner des valeurs à leurs en-têtes personnalisés, qui peuvent excéder ces limites. Ces situations devraient être rares, mais si une application SaaS excède une de ces limitations du nombre de caractères, alors votre pare-feu de nouvelle génération peut ne pas réussir à accéder à cette application SaaS*

La table suivante énumère les en-têtes que vous pouvez utiliser pour les applications SaaS pour lesquelles Palo Alto Networks fournir un soutien prédéfini ; chaque en-tête comprend également un lien vers plus d'informations propres à cet en-tête.

| Application | En-têtes | Pour plus d'informations |
|---|---|---|
| **Dropbox** | `X-Dropbox-allowed-Team-Ids` | www.dropbox.com/help/business/network-control<br><br>Vous pouvez autoriser l'accès aux comptes Dropbox d'entreprise. La valeur de l'en-tête correspond à l'ID de l'équipe responsable du compte d'entreprise, que vous pouvez obtenir dans la section relative au contrôle du réseau de la console d'administration de Dropbox. Vous devez également activer cette fonctionnalité à partir du même emplacement.<br><br>Pour obtenir des précisions sur la gestion de cet en-tête ainsi que sur l'activation de vos clients Dropbox pour déchiffrer leur trafic, communiquez avec votre représentant Dropbox. |
| **Google G Suite** | `X-GooGApps-Allowed-Domains` | support.google.com/a/answer/1668854?hl=en<br><br>Vous pouvez autoriser l'accès à des comptes Google spécifiques à partir de votre domaine. Les valeurs que vous donnez à cet en-tête sont votre domaine et vos sous-domaines.<br><br>Pour réussir à insérer des en-têtes pour les applications Google, vous devez également : |

| Application | En-têtes | Pour plus d'informations |
|---|---|---|
| | | 1. Créez un profil de décryptage SSL qui comprend les catégories et les URL suivantes :<br>• business-and-economy<br>• computer-and-internet-info<br>• content-delivery-networks<br>• internet-communications-and-telephony<br>• low-risk<br>• online-storage-and-backup<br>• search-engine<br>• web-based-email<br>• drive.google.com<br>• *.google.com<br>• *.googleusercontent.com<br>• *.gstatic.com<br>2. L'insertion d'en-tête HTTP n'est actuellement pas prise en charge pour HTTP/2. Pour insérer des en-têtes, réduisez les connexions HTTP/2 à HTTP/1.1 en utilisant la fonction **Strip ALPN (Enlever l'ALPN)** dans le profil de décryptage approprié. Pour plus d'informations, reportez-vous à la section Inspection d'App-ID et HTTP/2.<br>3. Create rules (Créez des règles) pour bloquer l'App-ID Quick UDP Internet Connections (QUIC) et placez-les en tête de votre politique de sécurité car le pare-feu ne prend pas en charge l'insertion d'en-tête pour ce protocole. Lorsque vous le faites, l'application revient à l'utilisation de HTTP/2 sur TLS, que le pare-feu gère à l'étape précédente. |
| **Microsoft Office 365** | `Restrict-Access-To-Tenants`<br>`Restrict-Access-Context` | docs.microsoft.com/en-us/azure/active-directory/active-directory-tenant-restrictions<br>Vous fournissez à `Restrict-Access-To-Tenants` une liste des locataires auxquels vous voulez autoriser vos utilisateurs à accéder. Vous pouvez utiliser n'importe quel domaine inscrit auprès d'un locataire pour identifier le locataire dans cette liste. |

| Application | En-têtes | Pour plus d'informations |
|---|---|---|
| | | Vous fournissez à `Restrict-Access-Context` l'ID de répertoire qui définit la restriction du locataire. Vous pouvez trouver votre ID de répertoire dans le portail Azure. Ouvrez une session en tant qu'administrateur, sélectionnez **Azure Active Directory (Répertoire actif d'Azure)**, puis sélectionnez **Properties (Propriétés)**. |
| **YouTube** | `YouTube-Restrict` | support.google.com/a/answer/6214622?hl=en<br>Vous fournissez à cet en-tête les informations concernant le type de vidéos que vous voulez que vos utilisateurs puissent visionner. Vous pouvez préciser un paramètre **Strict** ou **Moderate (Modéré)**. Consultez support.google.com/a/answer/6212415 pour plus de détails sur ces différents paramètres. |

## Domaines utilisés par les types d'applications SaaS prédéfinis

Les applications SaaS utilisent HTTPS. De ce fait, pour insérer des en-têtes personnalisés dans ce trafic, ils doivent être déchiffrés. Si vous utilisez le déchiffrement de transfert de proxy disponible sur le pare-feu pour déchiffrer les en-têtes personnalisés, vous devez identifier le trafic HTTPS spécifique que vous voulez déchiffrer en identifiant les domaines associés au trafic. Le tableau suivant identifie les domaines pertinents pour chaque application SaaS pour laquelle Alto Networks® a fourni des règles prédéfinies.

| Application | Domaines |
|---|---|
| **Dropbox** | `*.dropbox.com` |
| **G Suite** | `*.google.com`<br>`gmail.com` |
| **Microsoft Office 365** | `login.microsoftonline.com`<br>`login.microsoft.com`<br>`login.windows.net` |
| **YouTube** | `www.youtube.com`<br>`m.youtube.com`<br>`youtubei.googleapis.com`<br>`youtube.googleapis.com` |

| Application | Domaines |
|---|---|
| | `www.youtube-nocookie.com` |

## Création d'entrées d'insertion d'en-têtes HTTP au moyen des types prédéfinis

**STEP 1 |** Si aucun périphérique branché en amont ne déchiffre le trafic HTTPS, configurez le déchiffrement en utilisant la configuration du proxy de transfert SSL.

> *Si vous configurez le déchiffrement SSL pour Dropbox, vous devez alors également configurer vos clients Dropbox pour autoriser le trafic SSL. Ces procédures sont spécifiques et privées à Dropbox. Pour obtenir ces procédures, contactez votre représentant Dropbox.*

1. **Add (Ajoutez)** une catégorie d'URL personnalisée pour l'application SaaS que vous gérez (**Objects (Objets)** > **Custom Objects (Objets personnalisés)** > **URL Category (Catégorie d'URL)**).
2. Précisez un **Name (Nom)** à donner à la catégorie.
3. **Add (Ajoutez)** les domaines spécifiques à l'application Saas que vous gérez ou pour lesquels vous voulez insérer le nom d'utilisateur et le domaine dans les en-têtes. Reportez-vous à la section Domaines utilisés par les types d'applications SaaS prédéfinis pour obtenir une liste de tous les domaines que vous utilisez pour chacune des applications SaaS prédéfinies. Reportez-vous à la section Insertion du nom d'utilisateur dans les en-têtes HTTP pour obtenir de plus amples renseignements sur la configuration du pare-feu pour inclure le nom d'utilisateur et le domaine dans les en-têtes HTTP.

   Chaque nom de domaine peut comporter un maximum de 254 caractères et vous pouvez identifier un maximum de 50 domaines pour chaque entrée. La liste de domaines prend en charge les caractères spéciaux (par exemple, **`*.exemple.com`**). Il est recommandé de ne pas emboîter de caractères spéciaux (par exemple, **`*.*.*`**) et de ne pas faire se chevaucher des domaines au sein du même profil d'URL.
4. Pour la gestion des applications SaaS, procédez à la Création d'une règle de politique de décryptage et, en suivant cette procédure, configurez ce qui suit :
   - À l'onglet **Service/URL Category (Service / Catégorie d'URL)**, **Add (Ajoutez)** la **URL Category (Catégorie d'URL)** que vous avez créée à l'étape précédente.
   - à l'onglet **Options**, assurez-vous que l'**Action** est définie sur **Decrypt (Décrypter)** et que le **Type** est défini sur **SSL Forward Proxy (Proxy de transfert SSL)**.

**STEP 2 |** Modifiez ou ajoutez un profil de filtrage des URL.

**STEP 3 |** Sélectionnez **HTTP Header Insertion (Insertion de l'en-tête HTTP)** dans la boîte de dialogue **URL Filtering Profile (Profil de filtrage des URL)**.

**STEP 4 |** **Add (Ajoutez)** une entrée.

1. Donnez un **Name (Nom)** (100 caractères maximum) à cette entrée.
2. Sélectionnez **Type** de rôle prédéfini.

   Les listes **Domains (Domaines)** et **Headers (En-têtes)** apparaissent alors.
3. Pour chaque **Header (En-tête)**, saisissez une **Value (Valeur)**.
4. (Facultatif) Sélectionnez **Log (Journal)** pour activer la journalisation des activités d'insertion pour les en-têtes.

   Le trafic autorisé n'est pas journalisé, les insertions d'en-têtes ne sont donc pas journalisées pour le trafic autorisé.
5. Cliquez sur **OK** pour enregistrer vos modifications.

**STEP 5 |** **Add (Ajoutez)**ou modifiez une règle de Security Policy (Politique de sécurité) (**Policies [Politiques]** > **Security [Sécurité]**) pour inclure l'insertion d'en-têtes HTTP .

- Pour la gestion d'applications SaaS, autorisez les utilisateurs à accéder à l'application SaaS pour laquelle vous configurez la règle d'insertion d'en-têtes.
- Pour inclure le nom d'utilisateur et le domaine dans les en-têtes HTTP, appliquez le profil de filtrage des URL à la règle de politique de sécurité du trafic HTTP ou HTTPS.

  1. Choisissez le profil de filtrage des URL (**Actions** > **URL Filtering (Filtrage des URL)**) que vous avez modifié ou créé à l'étape 2.
  2. Cliquez sur **OK** pour enregistrer, puis **Commit (Validez)** vos modifications.

**STEP 6 |** Vérifiez que le pare-feu a bien inséré l'en-tête.

- Pour la gestion des applications SaaS, à partir d'un terminal, confirmez que l'accès à l'application SaaS fonctionne de la manière attendue.

  **1.** Essayez d'accéder à un compte ou à du contenu auquel vous devriez pouvoir accéder. Si vous ne pouvez accéder au compte ou au contenu SaaS, c'est que la configuration ne fonctionne pas.

  **2.** Essayez d'accéder à un compte ou à du contenu qui devrait être bloqué. Si vous pouvez accéder au compte ou au contenu SaaS, c'est que la configuration ne fonctionne pas.

  **3.** Si les deux étapes précédentes fonctionnent comme prévu, vous pouvez alors Afficher les journaux (si vous avez configuré la journalisation à l'étape 4.4). Vous devriez voir l'activité d'insertion des en-têtes HTTP consignée.

# Création d'entrées d'insertion d'en-têtes HTTP personnalisées

**STEP 1 |** Si aucun périphérique branché en amont ne déchiffre le trafic HTTPS, configurez Decryption (Décryptage) en utilisant Configure SSL Forward Proxy (Configurer le proxy de transfert SSL) Decryption (Décryptage).

1. **Add (Ajoutez)** une catégorie d'URL personnalisée pour l'application SaaS que vous gérez (**Objects (Objets)** > **Custom Objects (Objets personnalisés)** > **URL Category (Catégorie d'URL)**).
2. Précisez un **Name (Nom)** à donner à la catégorie.
3. **Add (Ajoutez)** les domaines propres à l'application SaaS que vous gérez.
4. Procédez à la Création d'une règle de politique de décryptage et, en suivant cette procédure, configurez ce qui suit :
   - À l'onglet **Service/URL Category (Service / Catégorie d'URL)**, **Add (Ajoutez)** la **URL Category (Catégorie d'URL)** que vous avez créée à l'étape précédente.
   - à l'onglet **Options**, assurez-vous que l'**Action** est définie sur **Decrypt (Décrypter)** et que le **Type** est défini sur **SSL Forward Proxy (Proxy de transfert SSL)**.

**STEP 2 |** Modifiez ou créez un profil de filtrage des URL.

**STEP 3 |** Sélectionnez **HTTP Header Insertion (Insertion de l'en-tête HTTP)** dans la boîte de dialogue **URL Filtering Profile (Profil de filtrage des URL)**.

**STEP 4 |** **Add (Ajoutez)** une entrée.

1. Précisez un **Name (Nom)** pour cette entrée.
2. Comme **Type (Type)**, sélectionnez **Custom (Personnalisé)**.
3. **Add (Ajoutez)** des domaines à la liste des **Domains (Domaines)**.

   Vous pouvez ajouter un maximum de 50 domaines et chaque nom de domaine peut comporter un maximum de 256 caractères ; les caractères génériques sont pris en charge (par exemple, *.exemple.com).

   *L'insertion d'un en-tête HTTP se produit lorsqu'un domaine de cette liste correspond au domaine de l'en-tête Hôte de la requête HTTP.*
4. **Add (Ajoutez)** les en-têtes à la liste des **Headers (En-têtes)**.

   Vous pouvez ajouter un maximum de 5 en-têtes et chaque en-tête peut comporter un maximum de 100 caractères, mais ne peut contenir d'espaces.
5. Pour chaque **Value (Valeur)** d'en-tête.
6. (Facultatif) Sélectionnez **Log (Journal)** pour activer la journalisation des activités d'insertion pour les en-têtes.
7. Cliquez sur **OK** pour enregistrer vos modifications.

**STEP 5 |** **Add (Ajoutez)** ou modifiez une règle de politiques de sécurité (**Policies (Politiques)** > **Security (Sécurité)**)Security Policy (Politique de sécurité) qui autorise les utilisateurs à accéder à l'application SaaS pour laquelle vous configurez cette règle d'insertion d'en-têtes.

1. Choisissez le profil de filtrage des URL (**Actions** > **URL Filtering (Filtrage des URL)**) que vous avez modifié ou créé à l'étape 2.
2. Cliquez sur **OK** pour enregistrer, puis **Commit (Validez)** vos modifications.

**STEP 6 |** Vérifiez que l'accès à l'application SaaS fonctionne comme vous le souhaitez. À partir d'un point de terminaison connecté à votre réseau :

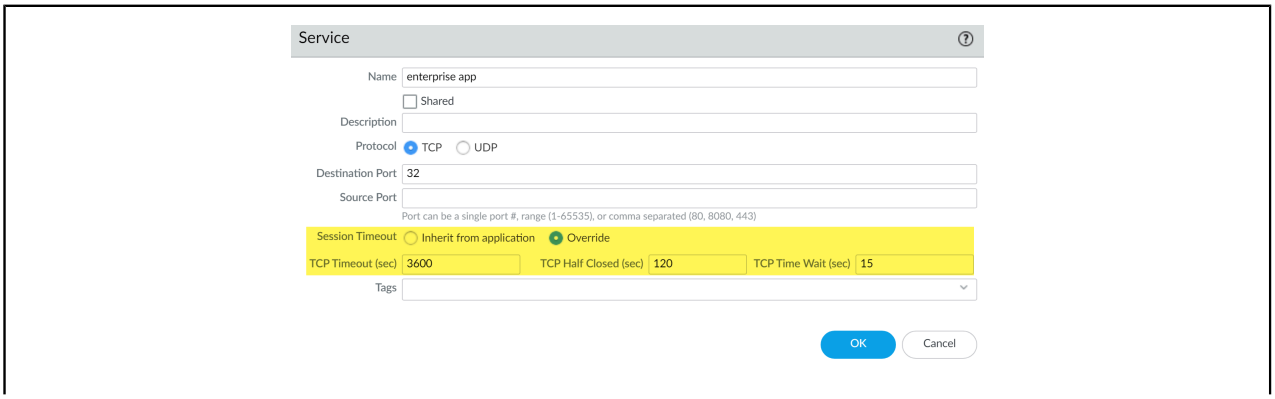
1. Essayez d'accéder à un compte ou à du contenu auquel vous devriez pouvoir accéder. Si vous ne pouvez accéder au compte ou au contenu SaaS, c'est que la configuration ne fonctionne pas.
2. Essayez d'accéder à un compte ou à du contenu qui devrait être bloqué. Si vous pouvez accéder au compte ou au contenu SaaS, c'est que la configuration ne fonctionne pas.
3. Si les deux étapes précédentes fonctionnent comme prévu, vous pouvez alors Afficher les journaux (si vous avez configuré la journalisation à l'étape 4.6). Vous devriez voir l'activité d'insertion des en-têtes HTTP consignée.

# Conservation des délais d'expiration applicables aux applications du centre de données

Conserver aisément les délais d'expiration applicables aux anciennes applications lorsque vous passez d'une politique fondée sur les ports à une politique fondée sur les applications. Servez-vous de cette méthode pour conserver les délais d'expiration plutôt que de remplacer App-ID (ce qui vous fait perdre la visibilité des applications) ou de créer un App-ID personnalisé (ce qui vous demande temps et recherches).

Pour commencer, configurez les paramètres des délais d'expiration personnalisés dans le cadre d'un objet de service :




Puis, ajoutez l'objet de service à une règle de politique afin d'appliquer les délais d'expiration personnalisés à l'application ou aux applications que la règle met en œuvre.

Les étapes suivantes décrivent la manière d'appliquer des délais d'expiration personnalisés aux applications. Pour appliquer des délais d'expiration personnalisés à des groupes d'utilisateurs, vous pouvez suivre les mêmes étapes, mais vous devez vous assurer d'ajouter l'objet de service à la règle de politique de sécurité qui s'applique aux utilisateurs auxquels vous souhaitez que le délai d'expiration s'applique.

**STEP 1 |** Sélectionnez **Objects (Objets)** > **Services** pour ajouter ou modifier un objet de service.

Vous pouvez également créer des objets de service lors de la définition des critères de mise en correspondance applicables à une règle de politique de sécurité : sélectionnez **Policies (Politiques)** > **Security (Sécurité)** > **Service/URL Category (Catégorie de service/d'URL)**, puis **Add (Ajoutez)** un nouvel objet de service à appliquer au trafic des applications que la règle régit.

**STEP 2 |** Sélectionnez le protocole que le service doit utiliser (TCP ou UDP).

**STEP 3 |** Saisissez le numéro de port de destination ou la plage de numéros de ports utilisé(e) par le service.

**STEP 4 |** Définissez le délai d'expiration de la session pour le service.

- **Inherit from application (Hériter de l'application)** (par défaut) : aucun délai d'expiration basé sur le service n'est appliqué ; c'est le délai d'expiration des applications qui est appliqué.
- **Override (Exercer un contrôle prioritaire)** : définissez un délai d'expiration de la session personnalisé pour le service.

**STEP 5 |** Si vous choisissez de remplacer le délai d'expiration des applications et de définir un délai d'expiration de session personnalisé, poursuivez en faisant ce qui suit :

- Saisissez une valeur de **TCP Timeout (Délai d'expiration TCP)** afin de définir la durée maximale, en secondes, pendant laquelle une session TCP peut demeurer ouverte après le début de la transmission des données. Lorsque ce délai expire, la session est fermée. La plage de valeurs est comprise entre 1 et 604 800, et la valeur par défaut est de 3600 secondes.
- Saisissez une valeur de **TCP Half Closed (sessions TCP à moitié fermées)** pour définir la durée maximale, en secondes, pendant laquelle une session reste dans la table des sessions, entre la réception du premier paquet FIN et celle du second paquet FIN ou RST. Si le délai expire, la session est fermée. La plage de valeurs est comprise entre 1 et 604800, et la valeur par défaut est de 120 secondes.
- Saisissez une valeur de **TCP Wait Time (Temps d'attente TCP)** pour définir la durée maximale, en secondes, pendant laquelle une session reste dans la table des sessions, après la réception du second paquet FIN ou RST. Lorsque le délai expire, la session est fermée. La plage de valeurs est comprise entre 1 et 600, et la valeur par défaut est de 15 secondes.

**STEP 6 |** Cliquez sur **OK** pour enregistrer l'objet de service.

**STEP 7 |** Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis **Add (Ajoutez)** ou modifiez une règle de politique pour régir le trafic des applications que vous souhaitez contrôler.

**STEP 8 |** Sélectionnez **Service/URL Category (Catégorie de service/URL)**, puis **Add (Ajoutez)** l'objet de service que vous venez de créer à la règle de politique de sécurité.

**STEP 9 |** Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.

paloalto TECHDOCS

# Device-ID



# Présentation de Device-ID

Que votre environnement prenne en charge ou non une politique « Bring Your Own Device » (Apportez votre propre appareil - BYOD), vous avez probablement déjà un grand nombre de périphériques dans votre réseau ; peut-être même plus que vous ne le pensez. Combiné au besoin d'évolutivité à mesure que le nombre d'utilisateurs et les périphériques qui les accompagnent sur votre réseau augmentent, sans parler de l'infrastructure croissante de l'internet des objets (IdO), cela représente un domaine de risque en constante augmentation avec de nombreuses possibilités d'exploitation par des utilisateurs malveillants. En outre, une fois que vous avez identifié ces périphériques, comment les protéger contre les vulnérabilités telles que des logiciels d'exploitation obsolètes ? En utilisant Device-ID™ sur votre pare-feu ou pour pousser la politique à partir de Panorama, vous pouvez obtenir le contexte du périphérique pour les événements sur votre réseau, obtenir des recommandations de règles de politique pour ces périphériques, écrire des politiques basées sur les périphériques, et appliquer la politique de sécurité basée sur les recommandations.

Tout comme User-ID fournit une politique basée sur l'utilisateur et App-ID une politique basée sur l'application, Device-ID fournit des règles de politique qui sont basées sur un périphérique, indépendamment des changements de son adresse IP ou de son emplacement. En assurant la traçabilité des périphériques et en associant les événements du réseau à des périphériques spécifiques, Device-ID vous permet de mettre en contexte la façon dont les événements sont liés aux périphériques et d'écrire des politiques qui sont associées aux périphériques, plutôt qu'aux utilisateurs, aux emplacements ou aux adresses IP, qui peuvent changer au fil du temps. Vous pouvez utiliser Device-ID dans les politiques de sécurité, de décryptage, de qualité de service (QoS) et d'authentification.

***Device-ID nécessite une licence Sécurité IdO, une licence de lac de données Cortex (CDL) et le certificat du périphérique.***

Si vous utilisez PAN-OS version 8.1.0 à PAN-OS 9.1.x sur un pare-feu, la licence Sécurité IdO fournit une classification des périphériques, une analyse du comportement et une analyse des menaces pour vos périphériques. Si vous utilisez PAN-OS 10.1 ou une version ultérieure, vous pouvez utiliser Device-ID pour obtenir des mappages adresse IP-périphérique afin de voir le contexte du périphérique pour les événements réseau, utiliser IoT Security pour obtenir des recommandations de règles de politique pour ces périphériques, et obtenir la visibilité pour les périphériques dans les rapports et l'ACC.

***Vous pouvez créer une politique de sécurité basée sur le périphérique sur tout Panorama ou pare-feu qui utilise PAN-OS version 10.1 ou supérieure. Pour appliquer la politique de sécurité, le périphérique doit avoir une licence valide de IoT Security.***

Pour identifier et classer les périphériques, l'application IoT Security utilise les métadonnées des journaux, des protocoles réseau et des sessions sur le pare-feu. Cela n'inclut pas les informations ou données privées ou sensibles qui ne sont pas pertinentes pour l'identification du périphérique. Les métadonnées constituent également la base du comportement attendu pour le périphérique, qui établit ensuite les critères pour la recommandation de règle de politique qui définit le trafic et les protocoles à autoriser pour ce périphérique.

Lorsqu'un pare-feu importe des recommandations de règles de stratégie de sécurité et des mappages d'adresses IP vers des appareils depuis IoT Security, le pare-feu envoie son device certificate (certificat de périphérique) à un serveur périphérique pour s'authentifier. Le serveur Edge

s'authentifie auprès du pare-feu en envoyant son propre certificat. Le pare-feu utilise le protocole OCSP (Online Certificate Status Protocol) pour valider le certificat du serveur en le comparant aux sites suivants à l'aide de HTTP sur le port TCP 80 :

- ocsp.int-x3.letsencrypt.org
- isrg.trustid.ocscp.identrust.com
- crl.identrust.com

Panorama effectue la même vérification pour valider le certificat du serveur Edge lorsque Panorama importe des recommandations de règles de politique depuis IoT Security.

Une fois que IoT Security a identifié et classifié les périphériques de votre réseau à l'aide des pare-feu Palo Alto Networks déjà présents dans votre réseau, afin que vous n'ayez pas à mettre en œuvre de nouveaux périphériques ou des solutions tierces, Device-ID peut exploiter ces données pour faire correspondre les périphériques aux règles de politique et fournir un contexte de périphérique pour les événements du réseau. Grâce à la visibilité que le pare-feu ou Panorama fournit pour le trafic, les applications, les utilisateurs, les périphériques et les menaces, vous pouvez instantanément retracer les événements du réseau jusqu'aux périphériques individuels et obtenir des recommandations de règles de sécurité pour sécuriser ces périphériques.

*Toutes les plateformes de pare-feu qui prennent en charge PAN-OS 10.1 prennent en charge Device-ID et l'application IoT Security, à l'exception de la série VM-50, de la série VM-200, de la série CN et de Prisma Access.*

Il existe six niveaux de classification (également appelés attributs) pour les périphériques :

| Attribut | Exemple |
|---|---|
| Catégorie | `Guichet automatique` ; `Imprimante 3D` |
| Profil | `Périphérique Palo Alto Networks` |
| Modèle | `iPad` |
| OS Version (Version de système d'exploitation) | `iOS 9.9.3` |
| Famille de système d'exploitation | `Android` ; `iOS` |
| Constructeur | `ASUS` ; `Philips` |

Pour obtenir des recommandations de règles de politique pour les périphériques de votre réseau, le pare-feu observe le trafic pour générer des journaux d'application améliorés (EAL). Le pare-feu transmet ensuite les EAL au lac de données Cortex (CDL) pour traitement. L'application IoT Security sur le concentrateur reçoit les journaux de la CDL pour analyse, fournit des mappages adresse IP-périphérique et génère les dernières recommandations de règles de politique pour vos périphériques. En utilisant l'application IoT Security, vous pouvez examiner ces recommandations de règles de politique et créer une politique de sécurité pour ces périphériques. Après avoir activé les règles de

politique dans l'application IoT Security, importez-les dans le pare-feu ou Panorama et validez votre politique de sécurité.

Le pare-feu doit être capable d'observer la diffusion DHCP et le trafic unicast sur votre réseau pour identifier les périphériques. Plus le trafic que le pare-feu peut observer est important, plus les recommandations de règles de politique sont précises pour le périphérique et plus les mappages adresse IP-périphérique sont rapides et précis pour le périphérique. Lorsqu'un périphérique envoie du trafic DHCP pour obtenir une adresse IP, le pare-feu observe ce type de requête, il génère des EAL à envoyer au lac de données Cortex pour traitement puis analyse par IoT Security.

***Pour observer le trafic sur une interface L2, vous devez configurer un VLAN pour cette interface. En permettant au pare-feu de traiter l'interface comme une interface L3 pour un relais DHCP, il peut observer le trafic de diffusion DHCP sans affecter le trafic ou les performances.***

Comme le pare-feu doit à la fois détecter les périphériques en fonction de leur trafic et appliquer la politique de sécurité pour ces périphériques, le pare-feu agit à la fois comme un ***capteur*** pour collecter les métadonnées des dispositifs et comme un ***applicateur*** en appliquant votre politique de sécurité pour les périphériques. L'application IoT Security détecte automatiquement les nouveaux périphériques dès qu'ils envoient du trafic DHCP et peut identifier 95 % des périphériques dès la première semaine.

Chaque application a une recommandation individuelle que vous importez dans le pare-feu ou Panorama comme règle. Lorsque vous importez la recommandation, le pare-feu ou Panorama crée au moins deux objets pour définir le comportement du périphérique à partir de la recommandation :

- Un objet de périphérique source qui identifie le périphérique d'où provient le trafic
- Un ou plusieurs objets de destination qui identifient les destinations autorisées pour le trafic, qui peuvent être un périphérique, une adresse IP ou un nom de domaine complet (FQDN)

Si l'un de ces objets de périphérique existe déjà sur le pare-feu ou Panorama, le pare-feu ou Panorama met à jour l'objet au lieu de créer un nouvel objet de périphérique. Vous pouvez utiliser ces objets de périphérique dans les politiques de sécurité, de décryptage et de qualité de service (QoS).

De plus, le pare-feu attribue deux tags (balises) à chaque règle :

- Un qui identifie le périphérique source, y compris la catégorie (comme `NetworkDevice - TrendNet`).
- Un qui indique que la règle est une recommandation de règle de politique IoT (`IoTSecurityRecommended`).

***Comme les étiquettes que le pare-feu attribue à la règle sont le seul moyen de restaurer vos mappages s'ils deviennent désynchronisés, ne modifiez pas ou ne supprimez pas les étiquettes.***

Pour un déploiement et un fonctionnement optimal de Device-ID, nous recommandons les meilleures pratiques suivantes :

- Déployez Device-ID sur les pare-feux qui sont situés au centre de votre réseau. Par exemple, si vous avez un environnement étendu, déployez Device-ID sur un pare-feu qui se trouve en amont

du périphérique de gestion des adresses IP (IPAM). Si vous avez un petit environnement, déployez Device-ID sur un pare-feu qui agit comme un serveur DHCP.

- Lors du déploiement initial, permettez à Device-ID de collecter les métadonnées de votre réseau pendant au moins quatorze jours. Si les périphériques ne sont pas actifs quotidiennement, le processus d'identification peut prendre plus de temps.
- Rédigez une politique basée sur les périphériques dans l'ordre de vos périphériques les plus critiques aux moins critiques. Établissez des priorités par :
  1. Classe (des périphériques en réseau sécurisés d'abord)
  2. Périphériques critiques (tels que les serveurs ou les machines IRM)
  3. Périphériques spécifiques à l'environnement (tels que les alarmes incendie et les lecteurs de badges)
  4. Périphériques IdO destinés aux consommateurs (tels qu'une montre connectée ou un haut-parleur connecté)
- Activez Device-ID par zone pour les zones internes uniquement.

# Préparation au déploiement de Device-ID

Pour préparer votre réseau au déploiement de Device-ID, effectuez les tâches de pré-déploiement suivantes pour permettre à votre pare-feu de générer et d'envoyer des journaux d'applications améliorées (EAL) au lac de données Cortex pour traitement et analyse par IoT Security pour la génération de recommandations de règles de politique.

**STEP 1 |** Si vous ne l'avez pas encore fait, installez le certificat de l'appareil sur votre pare-feu ou Panorama.

> *Si vous utilisez Panorama pour gérer plusieurs pare-feu, Palo Alto Networks recommande fortement de mettre à niveau tous les pare-feu de votre déploiement Device-ID vers PAN-OS 10.0 ou une version ultérieure. Si vous créez une règle qui utilise le* ***Device (périphérique)*** *comme critère de correspondance et que Panorama transmet la règle vers un pare-feu qui utilise PAN-OS 9.1 ou une version antérieure, le pare-feu omet les critères de correspondance du* ***Device (périphérique)*** *car il n'est pas pris en charge, ce qui peut entraîner des problèmes avec la politique correspondance de trafic de règle.*

**STEP 2 |** Activez votre instance lac de données Cortex (CDL) et connectez votre pare-feu à l'instance.

1. Activate (Activez) une instance de lac de données Cortex.
2. Connect (Connectez) votre pare-feu au lac de données Cortex.

**STEP 3 |** (Interfaces L2 uniquement) Créez une interface VLAN pour chaque interface L2 de sorte que le pare-feu puisse observer le trafic de diffusion DHCP.

**STEP 4 |** (Facultatif) Configurez un itinéraire de service pour permettre le trafic nécessaire à Device-ID et IoT Security.

Par défaut, le pare-feu utilise l'interface de gestion. Pour utiliser une autre interface, effectuez les étapes suivantes.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Services** puis sélectionnez **Service Route Configuration (Configuration de l'itinéraire de service)**.
2. **Customize (Personnalisez)** un Itinéraire de service.
3. Sélectionnez le protocole **IPv4**.

   > *Device-ID et IoT Security ne prennent pas en charge IPv6.*

4. Sélectionnez **Data Services (Services de données)** dans la colonne Service.
5. Sélectionnez une **Source Interface (Interface source)** et une **Source Address (Adresse source)**.
6. Cliquez deux fois sur **OK**.

**STEP 5 |** Utilisez les App-ID pour permettre le trafic nécessaire à Device-ID et IoT Security.

| Objectif | App-ID |
|---|---|
| Récupérez les recommandations de règles de politique et autorisez le trafic entre l'application IoT Security et votre pare-feu ou Panorama. | **paloalto-iot-security** |
| Autorisez le trafic pour tous les EAL et tous les journaux de session. | **paloalto-logging-service** |
| Récupérez les mises à jour dynamiques de la sécurité IoT et les mises à jour du dictionnaire des périphériques. | **paloalto-updates** |

*Si vous avez un pare-feu non-Palo Alto Networks entre le pare-feu utilisant le Device-ID et Internet, vérifiez que le pare-feu non-Palo Alto Networks peut accéder à iot.services-edge.paloaltonetworks.com:443.*

**STEP 6 |** Utilisez les App-ID pour permettre le trafic nécessaire à Device-ID et IoT Security.

| Objectif | Adresse | Port TCP |
|---|---|---|
| (PAN-OS versions 10.0.3 and later (PAN-OS versions 10.0.3 et ultérieures)) Recevoir le FQDN régional permet à Device-ID de récupérer les mappages d'adresse IP à appareil et les recommandations de règles de politique de la sécurité IoT. | **enforcer.iot.services-edge.paloaltonetworks.com** | 443 |
| (PAN-OS versions 10.0.0—10.0.2 and later (PAN-OS versions 10.0.0 à 10.0.2 et versions ultérieures)) Autorisez Device-ID à recevoir des recommandations de règles de politique et des mappages d'adresse IP vers périphérique de la sécurité IoT. | **iot.services-edge.paloaltonetworks.com**<br>*L'adresse ci-dessus est le FQDN régional pour les États-Unis. Pour les autres régions, effectuez une mise à niveau vers la version 10.0.3 ou ultérieure pour spécifier et vous connecter à un nom de domaine complet régional. Sinon, le pare-feu se connecte au FQDN américain par défaut.* | 443 |
| Autorisez Panorama à envoyer des requêtes de | L'URL varie en fonction de la configuration CDL. Pour plus d'informations, reportez-vous | 444 |

| Objectif | Adresse | Port TCP |
|---|---|---|
| journaux à Cortex Data Lake. | à TCP Ports and FQDNs Required for Cortex Data Lake (Ports TCP et noms de domaine complets requis pour Cortex Data Lake). | |

**STEP 7 |** Si vous utilisez des pare-feux, autorisez le trafic nécessaire pour Device-ID et IoT Security.

| Objectif | Adresse | Port TCP |
|---|---|---|
| (PAN-OS versions 10.0.3 and later (PAN-OS versions 10.0.3 et ultérieures)) Recevez le nom de domaine complet régional pour récupérer les mappages d'adresses IP vers les périphériques et les recommandations de règles de politique de la sécurité IoT. | **enforcer.iot.services-edge.paloaltonetworks.com** | N/A |
| (PAN-OS versions 10.0.0—10.0.2 (PAN-OS versions 10.0.0—10.0.2)) Autorisez le pare-feu à recevoir des recommandations de règles de politique et des mappages d'adresse IP vers périphérique de la sécurité IoT. | **iot.services-edge.paloaltonetworks.com** | 443 |
| Téléchargez les fichiers du dictionnaire du périphérique à partir du serveur de mise à jour. | **updates.paloaltonetworks.com** | 443 |
| Transférer les journaux vers Cortex Data Lake | N/A | 444 et 3978 |

**STEP 8 |** Configurez votre pare-feu pour qu'il observe et génère des journaux pour le trafic DHCP, puis transmettez ces journaux pour traitement et analyse par IoT Security.

- Si le pare-feu agit comme un serveur DHCP :
  1. Enable (Activez) la journalisation améliorée des applications.
  2. Créez un profil de transfert des journaux pour transférer les journaux au CDL pour traitement.
  3. (Not supported on the PA-3200, PA-5200, PA-5450, or PA-7000 (Non pris en charge sur le PA-3200, PA-5200, PA-5450 ou PA-7000)) Activez l'option de **DHCP Broadcast**

**Session (session de diffusion DHCP)** (**Device (périphérique)** > **Setup (Configuration)** > **Session** > **Session settings (Paramètres de session)**).

4. Créez une règle de politique de sécurité pour autoriser **dhcp** comme type d'**Application**.

- Si le pare-feu n'est pas un serveur DHCP, configurez une interface comme DHCP relay agent (Agent de relais DHCP) afin que le pare-feu puisse générer des EAL pour le trafic DHCP qu'il reçoit des clients.
- Si votre serveur DHCP se trouve sur le même segment de réseau que l'interface de votre pare-feu, déployez une interface câble virtuel devant le serveur DHCP pour vous assurer que le pare-feu génère des EAL pour tous les paquets dans l'échange DHCP initial avec un impact minimal sur les performances.

  1. Configurez une interface virtual wire (câble virtuel) avec des zones correspondantes et activez l'option **Multicast Firewalling (Pare-feu multicast)** (**Network (Réseau)** > **Virtual Wires (Câbles virtuels)** > **Add (Ajouter)**).
  2. Configurez une règle pour autoriser le trafic DHCP vers et depuis le serveur DHCP entre les zones de câble virtuel. La politique doit autoriser tout le trafic existant que le serveur observe actuellement et utiliser le même profil de transfert de journal que le reste de vos règles.
  3. Pour permettre aux serveurs DHCP de vérifier si une adresse IP est active avant de l'attribuer en location à une nouvelle demande, configurez une règle pour autoriser les pings du serveur DHCP vers le reste du sous-réseau.
  4. Configurez une règle pour autoriser tout autre trafic vers et depuis le serveur DHCP qui ne transmet pas les journaux pour les correspondances de trafic.
  5. Configurez l'hôte du serveur DHCP pour utiliser la première interface câble virtuel et le commutateur réseau pour utiliser la deuxième interface câble virtuel. Pour minimiser le câblage, vous pouvez utiliser un VLAN isolé dans l'infrastructure de commutation au lieu de connecter l'hôte du serveur DHCP directement au pare-feu.
- Si vous souhaitez utiliser une interface tap pour obtenir une visibilité sur le trafic DHCP que le pare-feu n'observe généralement pas en raison de la configuration ou de la topologie actuelle du réseau, utilisez la configuration suivante comme meilleure pratique.

  1. Configurez une interface tap et une zone correspondante.
  2. Configurez une règle pour faire correspondre le trafic DHCP qui utilise le même profil de transfert des journaux que le reste de vos règles.
  3. Pour minimiser la charge de la session sur le pare-feu, configurez une règle pour abandonner tout autre trafic.
  4. Connectez l'interface tap au miroir de port sur le commutateur réseau.

**STEP 9 |** Ajoutez des types de journaux de session au profil de transfert des journaux.

S'il n'y a pas d'entrées existantes dans le profil de transfert des journaux, la sélection de l'option **Enable enhanced application logging to Cortex Data Lake (Activer la journalisation améliorée**

**des applications sur le lac de données Cortex) (y compris les journaux de trafic et d'url)** ajoute tous les types de journaux.

1. **Add (Ajoutez)** un nouveau profil et saisissez un nom.
2. Sélectionnez **traffic (trafic)** comme **Log type (Type de journal)**.
3. Sélectionnez **All logs (Tous les journaux)** comme **Filter (Filtre)**.
4. Sélectionnez l'option **Cortex Data Lake (Lac de données Cortex)**.
5. Cliquez sur **OK**.
6. Répétez les sous-étapes 1 à 5 pour les types de journaux **threat (menace)** et, si vous avez un abonnement, **wildfire**.

# Configuration de Device-ID

Effectuez les tâches suivantes pour importer les mappages adresse IP-périphérique et les recommandations de règles de politique de IoT Security vers votre pare-feu ou Panorama.

*Si vous utilisez Panorama pour gérer plusieurs pare-feu, Palo Alto Networks recommande fortement de mettre à niveau tous les pare-feu de votre déploiement Device-ID vers PAN-OS 10.0 ou une version ultérieure. Si vous créez une règle qui utilise* ***Device (périphérique)*** *comme critère de correspondance et que Panorama pousse la règle vers un pare-feu qui utilise PAN-OS 9.1 ou une version antérieure, le pare-feu omet les critères de correspondance du* ***Device (périphérique)*** *car il n'est pas pris en charge, ce qui peut entraîner des problèmes avec la stratégie correspondance de trafic de règle.*

**STEP 1 |** Activez votre licence IoT Security sur le concentrateur.

1. Suivez les instructions que vous avez reçues dans votre e-mail pour activer votre licence IoT Security.
2. Initialisez votre application IoT Security. Pour plus d'informations, consultez la section Get Started with IoT Security (Premiers pas avec IoT Security) et les IoT Security Best Practices (Meilleures pratiques de IoT Security).
3. Appliquez la licence aux pare-feu que vous souhaitez utiliser pour appliquer la politique de IoT Security.
4. Actualisez votre licence sur le pare-feu ou Panorama.

**STEP 2 |** Définissez votre politique de IoT Security sur l'application IoT Security.

1. Sur l'application IoT Security, sélectionnez l'objet du périphérique source.
2. **Create (Créez)** un nouvel ensemble de règles de politique pour l'objet du périphérique source.

   Pour plus d'informations sur la création de stratégies de sécurité avec l'application IoT Security, reportez-vous à IoT Security Best Practices (Recommander des stratégies de sécurité).
3. **Activate (Activez)** les règles de politique pour confirmer vos changements.

**STEP 3 |** Importez les mappages adresse IP-périphérique et les recommandations de règles de politique au pare-feu ou à Panorama.

1. Importez la recommandation de règle de politique.
   - Sur le pare-feu, sélectionnez **Device (Périphérique)** > **Policy Recommendation (Recommandation de politique)** > **IoT**.
   - Pour Panorama, sélectionnez **Panorama** > **Policy Recommendation (Recommandation de politique)** > **IoT** puis transférer les règles de politique jusqu'aux pare-feux que Panorama gère.

     *Après avoir poussé la politique vers les pare-feu, vous devez synchroniser les règles de politique sur les pare-feu pour créer le mappage recommandation de règle de politique-règle de politique.*

   Lorsque vous sélectionnez Recommandation de politique, le pare-feu ou Panorama communique avec IoT Security pour obtenir les dernières recommandations de règles de politique. Les recommandations de règles de politique ne sont pas mises en cache sur le pare-feu ou Panorama.

   *Comme IoT Security crée la recommandation de règle de politique en utilisant le comportement de confiance pour le périphérique, l'action par défaut pour la règle est allow (autoriser).*
2. Sélectionnez le **Source Device Profile (Profil de périphérique source)**.
3. Vérifiez que le **Destination Device Profile (Profil de périphérique de destination)** et les **Applications** autorisées sont corrects.
4. Sélectionnez **Import Policy Rules (Importer les règles de politique)** pour importer les règles de politique.
5. (Panorama uniquement) Sélectionnez **Location (Emplacement)** du groupe d'appareils où importer les règles de politique.
6. Saisissez un **Name (Nom)** à donner aux règles de politique.
7. (Panorama uniquement) Sélectionnez le **Destination Type (Type de destination)** (**Pre-Rulebase (Basé sur la règle « avant »)** ou **Post-Rulebase (Basé sur la règle « après »)**).
8. Sélectionnez **After Rule (Règle « après »** pour définir l'emplacement de la règle dans la base de règles.
   - **No Rule Selection (Aucune sélection de règle)** : place la règle au sommet de la base de règles.
   - **Default One (Par défaut)** : place la règle après la règle indiquée.

   *Dans votre politique de sécurité, les règles relatives à Device-ID doivent précéder toutes les règles existantes qui s'appliquent aux périphériques.*
9. Répétez ce processus pour chaque recommandation de règle de politique afin de créer des règles pour permettre l'accès de chaque objet de périphérique aux destinations nécessaires.
10. Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.

**STEP 4 |** Activez Device-ID dans chaque zone où vous souhaitez utiliser Device-ID pour détecter les périphériques et appliquer votre politique de sécurité.

Par défaut, Device-ID cartographie tous les sous-réseaux dans les zones où vous l'activez. Vous pouvez modifier les sous-réseaux où Device-ID effectue le mappage dans la **Include List (Liste d'inclusion)** et la **Exclude List (Liste d'exclusion)**.

*La meilleure pratique consiste à activer Device-ID dans la zone source pour détecter les périphériques et appliquer la politique de sécurité. Vous ne devez activer Device-ID que pour les zones internes.*

1. Sélectionnez **Network (Réseau)** > **Zones**.
2. Sélectionnez la zone dans laquelle vous souhaitez activer Device-ID.
3. **Enable Device Identification (Activez l'identification de périphérique)** puis cliquez sur **OK**.

**STEP 5 |** **Commit (Validez)** vos modifications.

**STEP 6 |** Vérifiez que votre politique de sécurité est correcte.

1. Sélectionnez des **Policies (Politiques)** puis sélectionnez la règle que vous avez créée à partir de la recommandation de règle de politique générale.

   IoT Security attribue une **Description** qui contient l'objet du dispositif source et des **Tags (Étiquettes)** pour identifier l'objet de périphérique source et que cette règle est une recommandation de IoT Security.

   *Les noms d'objet de périphérique doivent être uniques.*

2. Sélectionnez l'onglet **Source**, puis vérifiez le **Source Device Profile (Profil de périphérique source)**.
3. Sélectionnez l'onglet **Destination** et vérifiez le **Destination Device Profile (Profil de périphérique de destination)**.
4. Sélectionnez l'onglet **Application** et vérifiez les **Applications**.
5. Sélectionnez l'onglet **Actions** et vérifiez l'**Action** (par défaut : **Allow (Autoriser)**).
6. Utilisez Explore (Explorer) pour vérifier que CDL reçoit vos journaux et examiner quels journaux CDL reçoit.

**STEP 7 |** Créez des objets de périphérique personnalisés pour tous les périphériques qui n'ont pas de recommandations de règles de politique de IoT Security.

Par exemple, vous ne pouvez pas sécuriser des périphériques tels que les ordinateurs portables et les smartphones en utilisant les recommandations de règles de politique, vous devez donc créer manuellement des objets de périphérique pour ces types de périphériques afin de les utiliser dans votre politique de sécurité. Pour plus d'informations sur les objets de périphérique personnalisés, consultez la section Gestion de Device-ID.

**STEP 8 |** Utilisez les objets de périphérique pour faire respecter les règles de politique et pour surveiller et identifier les problèmes potentiels.

La liste suivante comprend quelques exemples de cas d'utilisation d'objets de périphérique.

- Utilisez les objets de périphérique source et de périphérique de destination dans les politiques de sécurité, d'authentification, de QoS et de décryptage.
- Utilisez le journal de décryptage pour identifier les défaillances et les actifs les plus critiques à décrypter.
- Visualisez l'activité des objets de périphérique dans ACC pour suivre les nouveaux périphériques et leur comportement.
- Utilisez les objets de périphérique pour créer un rapport personnalisé (par exemple, pour les rapports d'incident ou les audits).

# Gestion de Device-ID

Effectuez les tâches suivantes, si nécessaire, pour vous assurer que vos recommandations de règles de politique et vos objets de périphérique sont à jour ou pour restaurer les mappages des recommandations de règles de politique.

**STEP 1 |** Mettez à jour votre recommandation de règle de politique générale chaque fois que la colonne **New Updates Available (Nouvelles mises à jour disponibles)** affiche **Yes (Oui)** pour cette recommandation.

À mesure que les dispositifs acquièrent de nouvelles capacités, IoT Security met à jour les recommandations des règles de politique pour indiquer le trafic ou les protocoles supplémentaires que le pare-feu ou Panorama devrait autoriser. Vérifiez quotidiennement IoT Security pour les mises à jour et mettez à jour vos recommandations de règles politiques dès que possible.

1. Sur l'application IoT Security, **Edit (Modifiez)** les règles de politique puis cliquez sur **Next (Suivant)**.
2. Sélectionnez la nouvelle recommandation puis cliquez sur **Next (Suivant)**.
3. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.
4. Sur le pare-feu ou Panorama, cliquez sur **Import Policy Rules (Importer les règles de politique)** puis cliquez sur **Yes (Oui)** pour confirmer que vous voulez écraser la règle actuelle.

   *Cette action écrase la recommandation pour la règle, et non la règle elle-même.*

5. (Panorama uniquement) Répétez l'étape précédente pour tous les groupes d'appareils.
6. **Commit (Validez)** vos modifications.

**STEP 2 |** Examinez, mettez à jour et maintenez les objets de périphérique dans le Dictionnaire de périphériques.

*Vous devez créer des objets de périphérique pour tout périphérique qui n'a pas de recommandation de règle de politique de IoT Security. Par exemple, vous ne pouvez pas sécuriser des périphériques tels que les ordinateurs portables et les smartphones en utilisant les recommandations de règles de la politique de IoT Security, vous devez donc créer des objets de périphérique pour ces types de périphériques et les utiliser dans votre politique de sécurité pour sécuriser ces périphériques.*

1. Sélectionnez **Objects (Objets)** > **Devices (Périphériques)**.
2. **Add (Ajoutez)** un objet de périphérique.
3. **Browse (Parcourez)** la liste ou **Search (Recherchez)** à l'aide de mots clés.

   Les résultats de la recherche peuvent inclure plusieurs types d'attributs d'objets de périphérique (par exemple, à la fois **Category (Catégorie)** et **Profile (Profil)**).
4. Pour ajouter un objet de périphérique personnalisé, saisissez un **Name (Nom)** et en option une **Description** pour l'objet de périphérique.

   *Utilisez toujours un nom unique pour chaque objet de périphérique. Ne modifiez pas les étiquettes dans la description des objets de périphérique par rapport aux recommandations des règles de politique générale.*
5. (Panorama uniquement) Sélectionnez l'option **Shared (Partage)** pour mettre cet objet de périphérique à la disposition d'autres groupes d'appareils.
6. Sélectionnez les attributs pour l'objet de périphérique (**Category (Catégorie)**, **OS (Système d'exploitation)**, **Profile (Profil)**, **Osfamily (Famille de système d'exploitation)**, **Model (Modèle)** et **Vendor (Fournisseur)**).
7. Cliquez sur **OK** pour confirmer vos modifications.

**STEP 3 |** Dans certains cas (par exemple, si vous restaurez une configuration précédente), les correspondances entre les recommandations et les règles de politique générale peuvent être désynchronisées. Vous devez également synchroniser les mappages sur chaque pare-feu après avoir poussé les règles de politique de Panorama vers les pare-feu que Panorama gère. Pour synchroniser les mappages :

- Sur le pare-feu, sélectionnez **Device (Périphérique)** > **Policy Recommendation (Recommandation de politique)** > **IoT** > **Sync Policy Rules (Règles de politique de synchronisation)**
- Pour Panorama, sélectionnez **Panorama** > **Policy Recommendation (Recommandation de politique)** > **IoT** > **Sync Policy Rules (Règles de politique de synchronisation)**.

Le pare-feu ou Panorama analyse toutes les règles de la base de règles pour rechercher les étiquettes qui identifient une règle comme une recommandation de règle de politique de IoT Security, obtient les informations sur l'objet de périphérique source et repeuple la base de données des recommandations de règles de politique locale.

**STEP 4 |** Supprimez toute recommandation de règle politique qui n'est plus nécessaire.

Si une recommandation de règle de politique générale ne s'applique plus, vous pouvez la supprimer. Vous devez également supprimer la règle pour la recommandation de règle de politique afin d'appliquer la politique de sécurité mise à jour.

1. Sur l'application IoT Security, sélectionnez **Delete (Supprimer)**.
2. Cliquez sur **Mark as Removed (Marquer comme supprimée)** pour sélectionner l'élimination de cette recommandation.
3. Supprimez le mappage.
   - Sur le pare-feu, sélectionnez **Device (Périphérique)** > **Policy Recommendation (Recommandation de politique)** > **IoT** > **Remove Policy Mapping (Supprimer le mappage de politique)**.
   - Pour Panorama, sélectionnez **Device (Périphérique)** > **Policy Recommendation (Recommandation de politique)** > **IoT** > **Remove Policy Mapping (Supprimer le mappage de politique)** puis sélectionnez le **Location (Emplacement)** à partir duquel vous voulez supprimer le mappage.
4. Cliquez sur **Yes (Oui)** pour confirmer la suppression du mappage.
5. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**. Pour Panorama, sélectionnez **Policies (Politiques)** > **Security (Sécurité)** > **Pre Rules/Post-Rules (Règles « avant »/ Règles « après »)**.
6. Sélectionnez la règle pour la recommandation de règle politique que vous souhaitez supprimer puis sélectionnez **Delete (Supprimer)**.
7. **Commit (Validez)** vos modifications.

**STEP 5 |** Utilisez les commandes CLI pour résoudre tout problème entre le pare-feu et IoT Security.

# Commandes CLI pour Device-ID

Utilisez les commandes CLI suivantes pour afficher des informations permettant de résoudre tout problème entre le pare-feu et la IoT Security. En général, les commandes CLI qui incluent **eal** montrent des compteurs pour les données sortantes et les commandes CLI qui incluent **icd** montrent des compteurs pour les données entrantes.

| Exemple | Commande |
|---|---|
| Voir les compteurs EAL (Enhanced Application Logging), tels que le nombre de connexions entre le pare-feu et le lac de données Cortex et le volume des journaux. | **show iot eal all** |
| Voir plus de détails sur la connexion entre le pare-feu et le lac de données Cortex. | **show iot eal conn** |
| Voir un résumé des compteurs EAL par plan (plan de données ou plan de gestion), comme la version PAN-OS et le numéro de série. | **show iot eal dpi-eal** |
| Visualisez les compteurs EAL par plan (plan de données ou plan de gestion) et par protocole. | **show iot eal dpi-stats all** |
| Voir les compteurs EAL par protocole. | **show iot eal dpi-stats subtype dhcp\|http** |
| Voir un résumé des compteurs de rapports de jumelage des profils d'information sur l'hôte (HIP). | **show iot eal hipreport-eal** |
| Voir les compteurs de temps de réponse du journal EAL. | **show iot eal response-time** |
| Voir les détails de la santé de la connexion au service de périphérie entre le pare-feu et l'application IoT Security et les compteurs pour les mappages adresse IP-périphérique et les recommandations de règles de politique. | **show iot icd statistics all** |
| Voir les compteurs pour la connexion au service de périphérie. | **show iot icd statistics conn** |
| Voir les compteurs pour les mappages adresse IP-périphérique. | **show iot icd statistics verdict** |
| Voir tous les mappages adresse IP-périphérique sur le pare-feu. | **show iot ip-device-mapping-mp all** |

| Exemple | Commande |
| --- | --- |
| Voir le mappage adresse IP-périphérique pour une adresse IP spécifique. | **show iot ip-device-mapping-mp ip *IP-address*** |
| Voir une liste des mappages adresse IP-périphérique sur le plan de données. | **show iot ip-device-mapping all** |
| Effacer les mappages d'adresse IP-périphérique sur le plan de gestion. | **debug iot clear-all type device** |
| Effacer les mappages adresse IP-périphérique sur le plan de données. | **clear user-cache all** |

# Prévention contre les menaces

Le pare-feu Palo Alto Networks® de dernière génération protège et défend votre réseau contre les menaces touchant les produits informatiques et les menaces persistantes avancées (APT). Les nombreux mécanismes de détection du pare-feu incluent une approche basée sur des signatures (IPS/Commande et Contrôle/Antivirus), une approche basée sur des heuristiques (détection de robots), une approche basée sur un sandbox (WildFire) et une approche basée sur l'analyse du protocole de Couche 7 (App-ID).

Les menaces touchant les appareils informatiques sont des exploitations qui sont moins sophistiquées et plus facilement détectées et évitées grâce à une combinaison alliant antivirus, antispyware, ainsi que des fonctions de protection contre les vulnérabilités en plus des capacités d'identification de filtrage des URL/applications du pare-feu.

Les menaces avancées sont perpétrées par des cyber-criminels qui utilisent des vecteurs d'attaque sophistiqués pour cibler votre réseau, généralement pour commettre des vols de propriété intellectuelle et de données financières. Ces menaces sont plus évasives et exigent des mécanismes de surveillance intelligents pour analyser en détail l'hôte et le réseau afin d'identifier la présence d'un logiciel malveillant. Le pare-feu Palo Alto Networks de dernière génération, conjointement avec WildFire™ et Panorama™, fournit une solution complète qui intercepte, rompt la chaîne d'attaques et offre une visibilité pour éviter toute faille de sécurité sur votre infrastructure réseau, qu'il s'agisse d'infrastructures mobiles ou virtualisées.

*Après avoir mis en œuvre vos configurations de prévention contre les menaces, procédez à l'Exportation des données du tableau de configuration pour créer un rapport PDF ou CSV de vos configurations à utiliser à des fins d'examen interne ou d'audit.*

# Meilleures pratiques pour sécuriser votre réseau contre les fuites au niveau des couches 4 et 7

Pour surveiller et protéger votre réseau contre la plupart des attaques des couches 4 et 7, voici quelques recommandations à suivre.

- Mettez à niveau vers la dernière version logicielle et de contenu PAN-OS pour vous assurer de disposer des dernières mises à jour de sécurité. Reportez-vous à la section Installer les mises à jour de contenu et logicielles.
- Activation de la sécurité DNS (nécessite une licence d'abonnement à la prévention des menaces et à la sécurité DNS) pour faire mettre en entonnoir les demandes DNS malveillantes. Palo Alto Networks recommande d'utiliser les paramètres de configuration suivants de la catégorie Sécurité DNS dans votre profil antispyware :

| SIGNATURE SOURCE | LOG SEVERITY | POLICY ACTION | PACKET CAPTURE |
|---|---|---|---|
| : Palo Alto Networks Content | | | |
| default-paloalto-dns | | sinkhole | extended-capture |
| : DNS Security | | | |
| Command and Control Domains | default (high) | sinkhole | extended-capture |
| Dynamic DNS Hosted Domains | default (informational) | sinkhole | disable |
| Grayware Domains | default (low) | sinkhole | disable |
| Malware Domains | default (medium) | sinkhole | disable |
| Parked Domains | default (informational) | sinkhole | disable |
| Phishing Domains | default (low) | sinkhole | disable |
| Proxy Avoidance and Anonymizers | default (low) | sinkhole | disable |
| Newly Registered Domains | default (informational) | sinkhole | disable |

  - Pour les paramètres de gravité du journal, utilisez les paramètres par défaut :
  - Pour l'action de politique, régler toutes les sources de signature sur **entonnoir**.
  - Pour la capteur de paquet, réglez Command (Commande) et Control Domains (Domaines de contrôle) sur **capture étendue**. Laissez toutes les autres catégories aux réglages par défaut.

  Pour plus d'informations sur les paramètres antispyware connexes, voir Meilleures pratiques du profil antispyware pour la passerelle Internet.
- Configurez le pare-feu pour qu'il agisse en tant que proxy DNS et activez les signatures d'évasion :

  ***Le proxy DNS ne fait pas partie du moteur de la politique de sécurité du pare-feu ; à la place, il ordonne au pare-feu de résoudre les noms d'hôtes DNS, tout en maintenant le mappage entre le domaine et l'IP, ce qui est crucial pour empêcher l'évasion TLS/HTTP.***

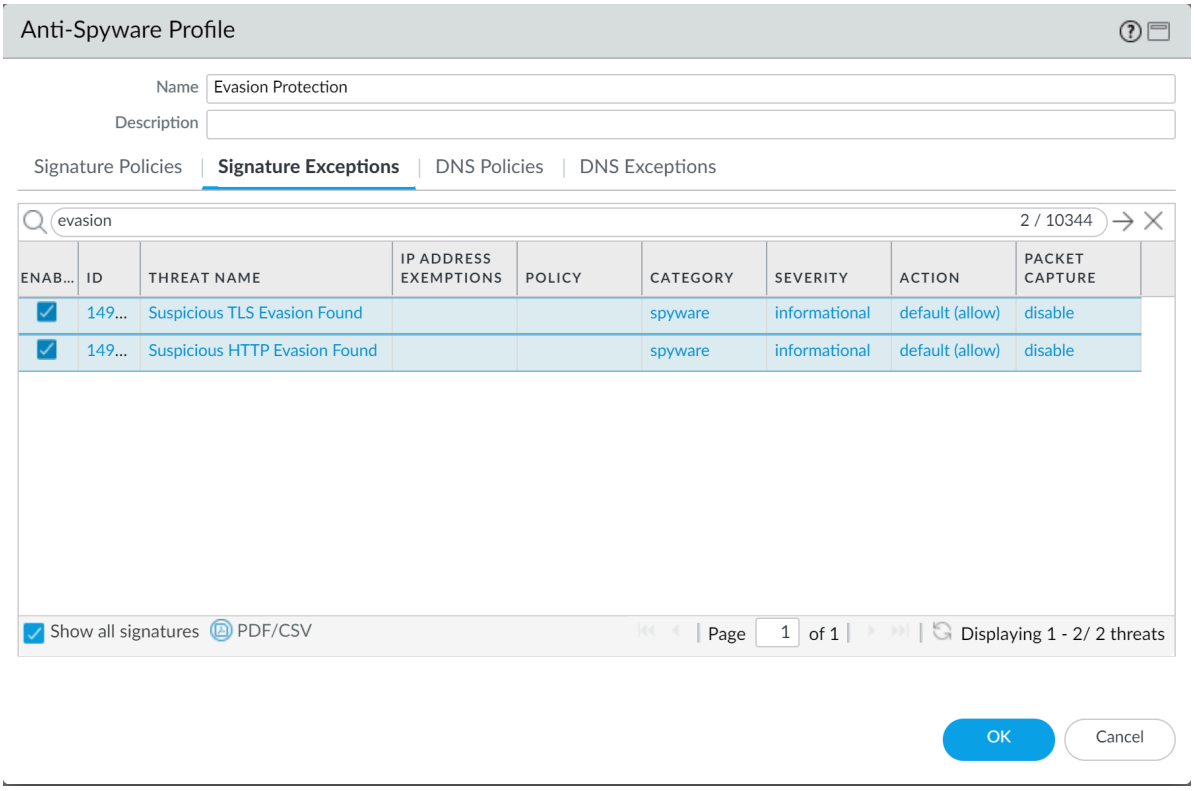
  - Configurez un objet proxy DNS.

    Lorsqu'il sert de proxy DNS, le pare-feu résout les requêtes DNS et met en cache les associations d'adresses IP à un nom d'hôte pour résoudre rapidement et efficacement les requêtes DNS futures.
  - Activer les signatures d'évasion

    Les signatures d'évasion qui détectent des requêtes HTTPS ou TLS fabriquées peuvent envoyer des alertes lorsque des clients se connectent à un domaine autre que celui qui est indiqué dans la requête DNS d'origine. Assurez-vous de configurer le proxy DNS avant d'activer les signatures d'évasion. Sans proxy DNS, les signatures d'évasion peuvent déclencher des alertes lorsqu'un serveur DNS dans une configuration d'équilibrage de charge

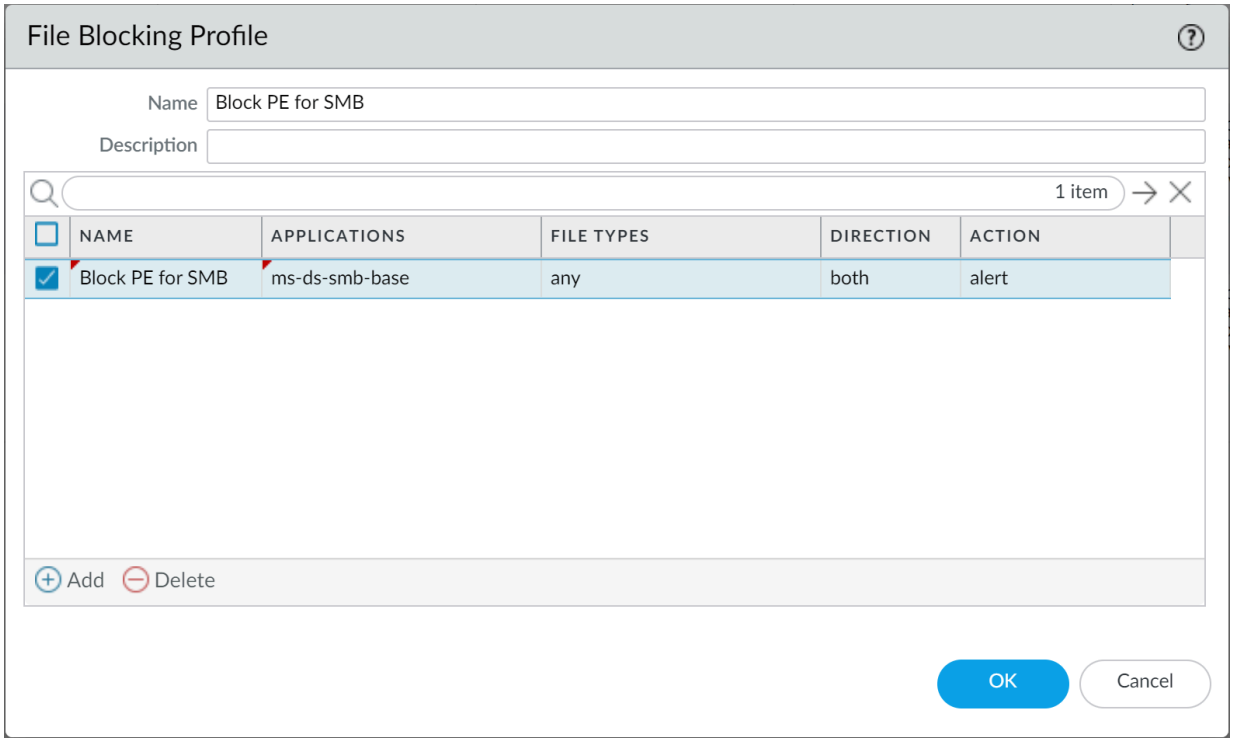
DNS retourne des adresses IP différentes (pour les serveurs qui hébergent des ressources identiques) au pare-feu et au client en réponse à la même requête DNS.




- Pour les serveurs, créez des règles de politique de sécurité qui n'autorisent que les applications que vous autorisez sur chaque serveur. Vérifiez que le port standard pour l'application correspond au port d'écoute sur le serveur. Par exemple, pour garantir que seul le trafic SMTP est autorisé sur votre serveur de messagerie, définissez l'Application sur **smtp (smtp)** et définissez le Service sur **application-default (par défaut de l'application)**. Si votre serveur n'utilise qu'un sous-ensemble de ports standard (par exemple, si votre serveur SMTP n'utilise que le port 587, tandis que les ports standard de l'application SMTP sont définis sur 25 et 587), créez un nouveau service personnalisé qui n'inclut que le port 587 et utilisez ce nouveau service dans votre règle de politique de sécurité plutôt que d'utiliser l'option Par défaut de l'application. De plus, assurez-vous de restreindre l'accès à des zones source et de destination ainsi qu'à des ensembles d'adresses IP donnés.
- Bloquez l'ensemble du trafic et des applications inconnu(es) à l'aide de la politique de sécurité. Normalement, les seules applications qui sont classées dans le trafic inconnu sont des applications internes ou personnalisées sur votre réseau et des menaces potentielles. Le trafic inconnu peut être des applications incompatibles ou des protocoles inhabituels ou anormaux, ou encore des applications connues qui utilisent des ports non standard ; dans tous les cas, le trafic inconnu

doit être bloqué. Reportez-vous à la section Gestion des applications propres à l'entreprise ou inconnues.

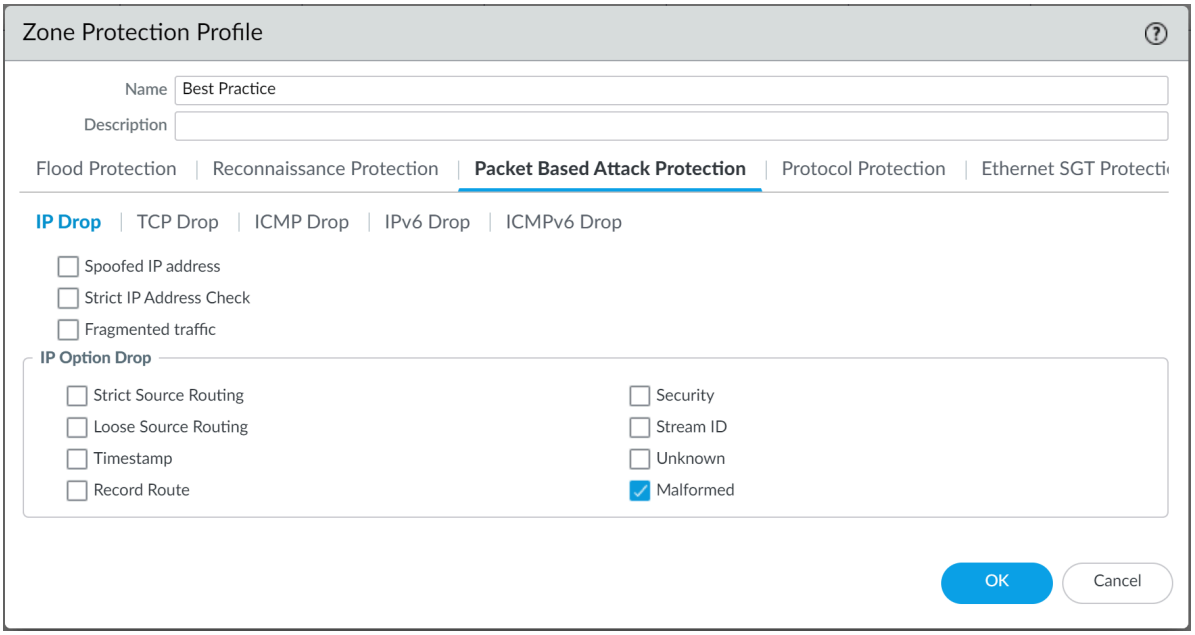
- Procédez au paramétrage du blocage des fichiers pour empêcher les types de fichiers Portable Executable (exécutable portable ; PE) du trafic Server Message Block (blocage des messages du serveur ; SMB) basé sur Internet de transiter entre des zones approuvées à des zones non approuvées (applications ms-ds-smb).




- Block malicious variants of PE (portable executables), PowerShell scripts, and ELF files in real-time (Bloquez les variantes malveillantes de PE (exécutables portables) et les scripts PowerShell en temps réel). L'activation de WildFire Inline ML vous permet d'analyser dynamiquement des fichiers en utilisant l'apprentissage machine sur le pare-feu. Cette couche supplémentaire de protection antivirus complète les signatures basées sur WildFire afin de fournir une couverture étendue pour les fichiers dont les signatures n'existent pas encore.

- Créez un profil de protection de zone configuré pour éviter toute attaque basée sur les paquets (**Network (Réseau)** > **Network Profiles (Profils réseau)** > **Zone Protection (Protection de zone)**) :
  - Sélectionnez l'option de supprimer les paquets IP **Malformed (Mal formés)**Packet Based Attack Protection (**Protection contre les attaques basées sur les paquets)** > **IP Drop (Abandon d'IP)**).




  - Activez l'option **Mismatched overlapping TCP segment (Segments TCP non concordants et se chevauchant)** (**Packet Based Attack Protection (Protection contre les attaques basées sur les paquets)** > **TCP Drop (Abandon TCP)**).

    En établissant délibérément des connexions avec des données superposées, mais différentes, les pirates informatiques essayent d'induire une interprétation erronée de l'action de la connexion et génèrent volontairement des faux positifs ou des faux négatifs. Les pirates utilisent également l'usurpation d'IP et la prédiction du numéro de séquence pour intercepter la connexion d'un utilisateur et y injecter leurs propres données. Sélectionnez l'option **Mismatched overlapping TCP segment (Segment TCP non concordant et se chevauchant)** pour indiquer que PAN-OS ignore les trames contenant des données non concordantes et se chevauchant. Les segments reçus sont ignorés lorsqu'ils sont inclus dans un autre segment, lorsqu'ils chevauchent une partie d'un autre segment ou lorsqu'ils contiennent l'ensemble d'un autre segment.
  - Activez les options d'abandon **TCP SYN with Data (paquets TCP SYN contenant des données)** et d'abandon **TCP SYNACK with Data (paquets TCP SYN-ACK contenant des**

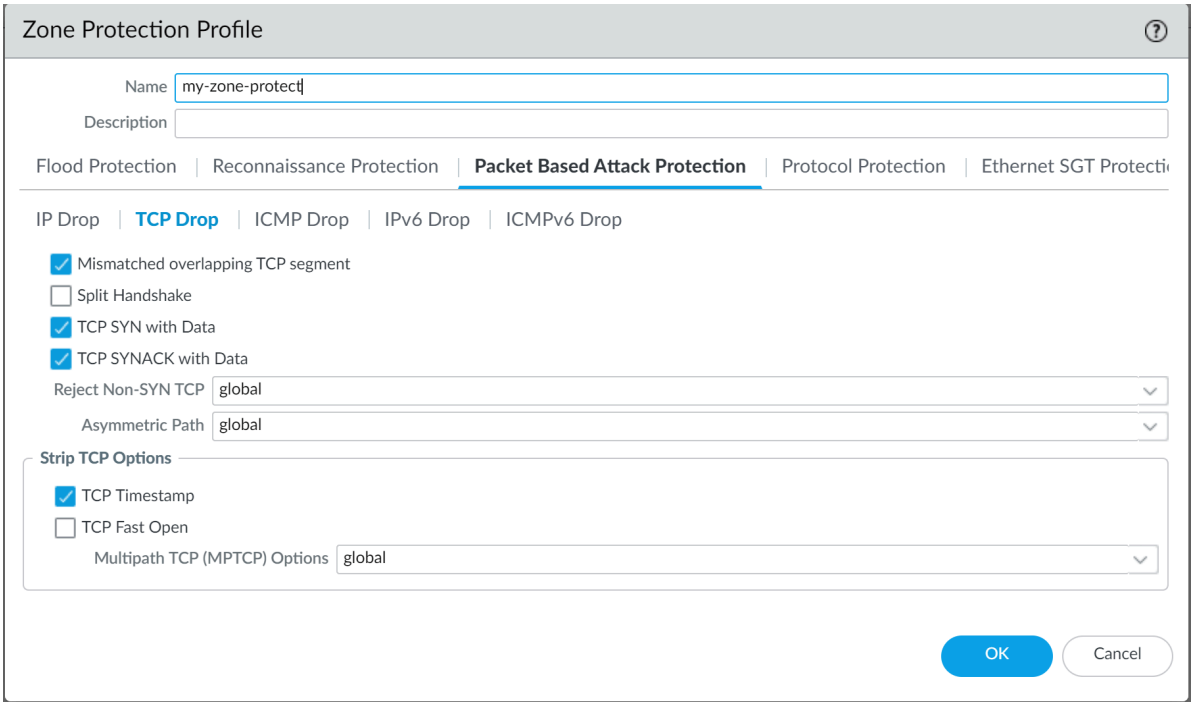
 

**données)** (**Packet Based Attack Protection (Protection contre les attaques basées sur les paquets)** > **TCP Drop (Abandon TCP)**).

L'abandon des paquets SYN et SYN-ACK qui contiennent des données dans la charge utile lors d'une connexion en trois étapes accroît la sécurité en bloquant les logiciels malveillants contenus dans la charge utile et en les empêchant d'extraire des données non autorisées avant que la liaison TCP a été établie.

- Supprimez les horodatagesTCP des paquets SYN avant leur transfert par le pare-feu (**Packet Based Attack Protection (Protection contre les attaques basées sur les paquets)** > **TCP Drop (Abandon TCP)**).

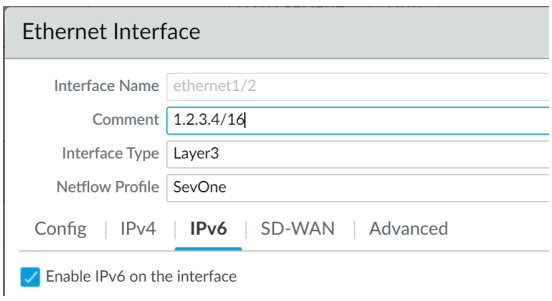
  Lorsque vous activez l'option **Strip TCP Options - TCP Timestamp (Enlever les options TCP - horodatage TCP)**, la pile TCP des deux extrémités de la connexion TCP ne prendra pas en charge les horodatages TCP. Ceci prévient les attaques qui utilisent différents horodatages sur plusieurs paquets ayant le même numéro de séquence.



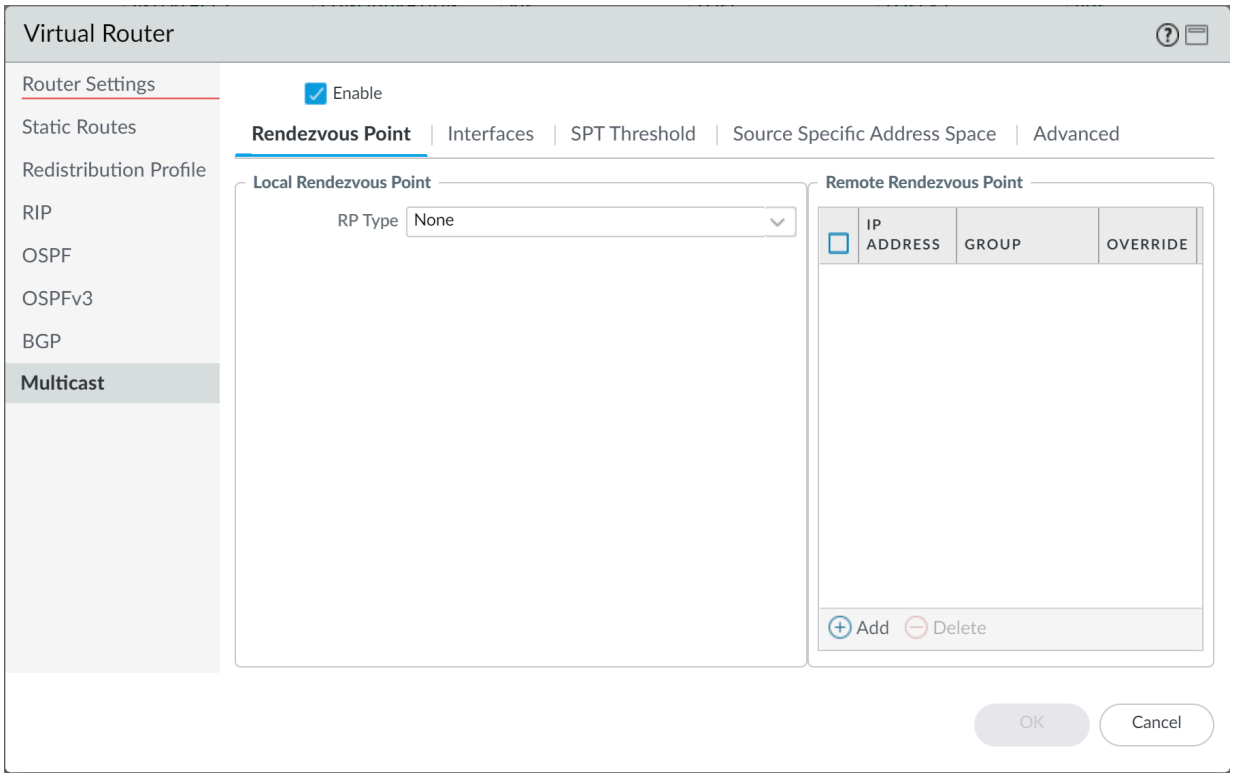

 

- Si vous configurez les adresses IPv6 sur vos hôtes réseau, assurez-vous d'activer la prise en charge de IPv6, si vous ne l'avez déjà fait (**Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet) > IPv6 (IPv6)**).

  L'activation de la prise en charge de IPv6 autorise l'accès aux hôtes IPv6 et permet le filtrage des paquets IPv6 encapsulés dans des paquets IPv4, ce qui évite l'exploitation des adresses IPv6 multicast sur IPv4 pour la reconnaissance réseau.




- Activez le support pour le trafic multicast afin que le pare-feu puisse appliquer une politique au trafic multicast (**Network (Réseau)** > **Virtual Router (Routeur virtuel)** > **Multicast (Multidiffusion)**).



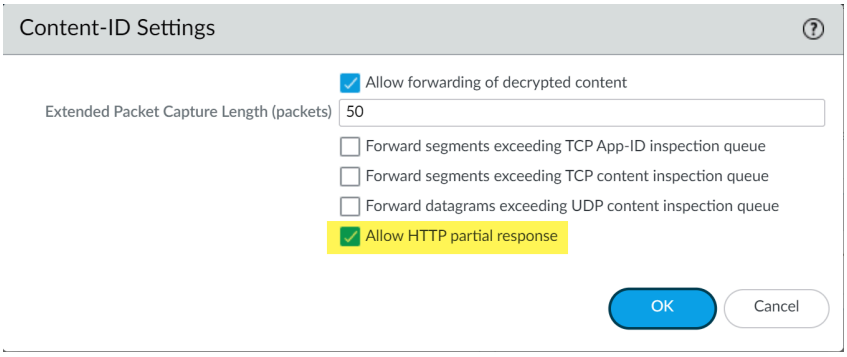
- Désactivez les options vous permettant de **Forward datagrams exceeding UDP content inspection queue (Transmettre les datagrammes qui excèdent la file d'attente d'inspection du contenu UDP)** et **Forward segments exceeding TCP content inspection queue (Transmettre les datagrammes qui excèdent la file d'attente d'inspection du contenu TCP)** (**Device (Périphérique)** > **Setup (Configuration)** > **Content-ID (Content-ID)** > **Content-ID Settings (Paramètres de Content-ID)**).

  Par défaut, lorsque la file d'attente d'inspection du contenu TCP ou UDP est pleine, le pare-feu saute l'inspection de contenu pour les segments TCP ou les datagrammes UDP qui excèdent la limite établie pour la file d'attente, soit 64. Le désactivation de cette option garantit l'inspection du contenu pour tous les segments TCP et les datagrammes UDP autorisés par le pare-feu. Dans des circonstances particulières (par exemple, si la plateforme du pare-feu n'est pas bien dimensionnée pour s'harmoniser à un cas pratique), la désactivation de ce paramètre peut compromettre la performance de l'application.

- Désactivez la **Allow HTTP partial response (option Autoriser la réponse partielle HTTP)** (**Device (Périphérique)** > **Setup (Configuration)** > **Content-ID (Content-ID)** > **Content-ID Settings (Paramètres Content-ID)**).

  L'option de réponse partielle HTTP permet à un client d'extraire seulement une partie d'un fichier. Lorsqu'un pare-feu de nouvelle génération identifie et supprime un fichier malveillant dans le chemin d'accès d'un transfert, il met fin à la session TCP à l'aide d'un paquet RST. Si le navigateur Web implémente l'option de plage HTTP, il peut commencer une nouvelle session pour extraire uniquement la partie restante du fichier, ce qui empêche le pare-feu de déclencher à nouveau la même signature en raison de l'absence de contexte dans la session initiale, tout en permettant au navigateur Web de réassembler le fichier et de livrer le contenu malveillant. Pour éviter ce genre de situation, il suffit de désactiver cette option.

  ***La désactivation de cette option ne devrait avoir aucune incidence sur le rendement du périphérique. Cependant, la récupération après interruption du transfert de fichier HTTP peut être compromise.***




- Créez un profil de protection contre les vulnérabilités qui bloque les anomalies de protocole et toutes les vulnérabilités ayant un niveau de gravité faible et élevé.

  Une anomalie de protocole se produit lorsque le comportement d'un protocole s'écarte de l'utilisation standard et conforme. Par exemple, un paquet malformé, une application mal conçue ou une application qui s'exécute sur un port non standard sont tous des anomalies de protocole et pourraient servir de techniques d'évasion.

  Si vous disposez d'un réseau stratégique, où l'entreprise privilégie la disponibilité des applications, vous devriez commencer par recevoir des alertes lorsque des anomalies de protocole sont

détectées pendant un certain temps pour vous assurer qu'aucune application stratégique interne n'utilise de protocoles établis d'une manière non standard. Si vous découvrez que certaines applications critiques déclenchent des signatures d'anomalies de protocole, vous pouvez alors les exclure de l'application des anomalies de protocole. Pour ce faire, ajoutez une autre règle au profil de protection contre les vulnérabilités qui autorise les anomalies de protocole et associez le profil à la règle de politique de sécurité qui applique le trafic vers les applications critiques et depuis ces dernières.

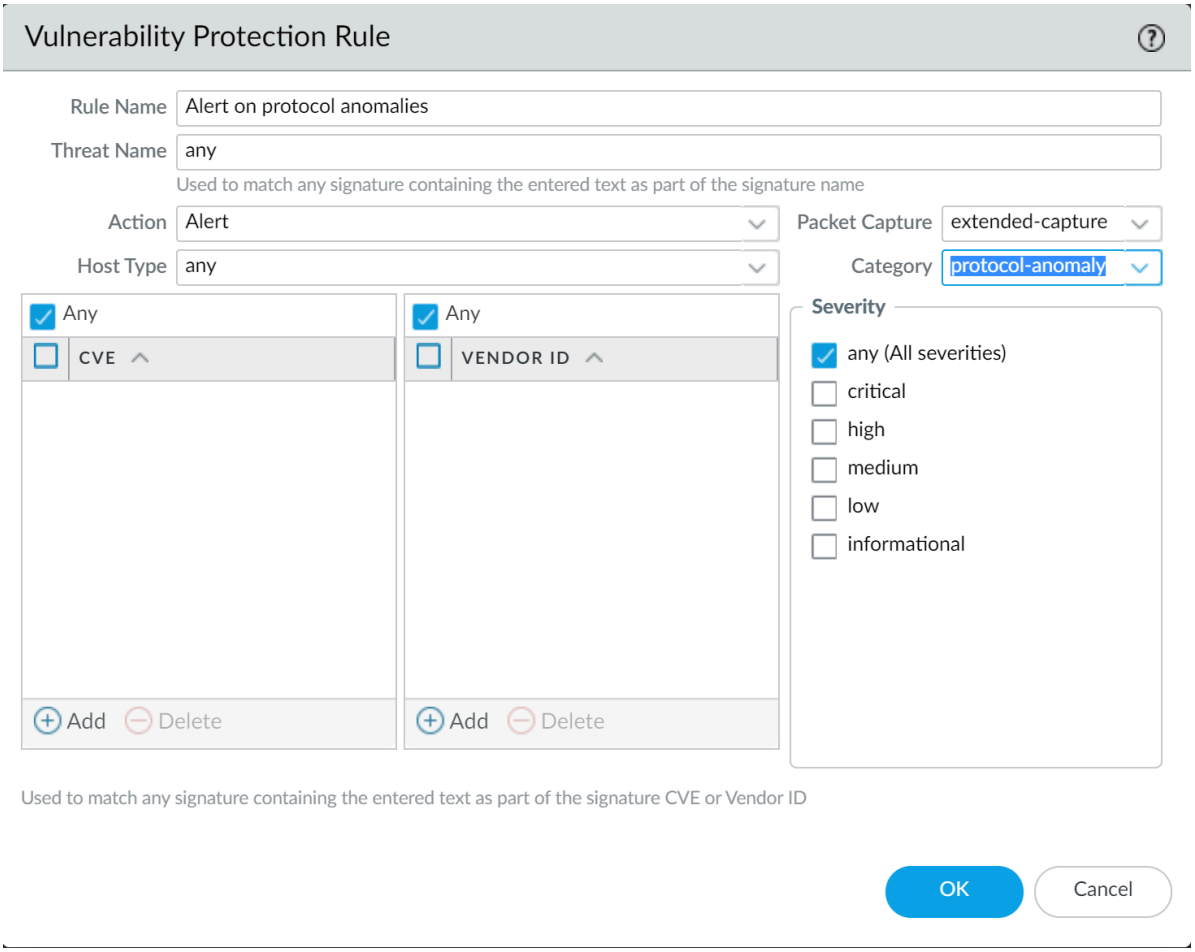
Assurez-vous que les règles du profil de protection contre les vulnérabilités et que les règles du profil de sécurité qui autorisent les anomalies de protocole détectées dans les applications critiques internes se trouvent au-dessus des règles qui bloquent les anomalies de protocole. Le trafic est comparé aux règles de la politique de sécurité et aux règles des profils de protection contre les vulnérabilités de haut en bas ; il est mis en œuvre en fonction de la première règle correspondante.

- Commencez par recevoir des alertes relatives aux anomalies de protocole :

  Créez une règle de profil de protection contre les vulnérabilités pour laquelle l'**Action (Action)** est définie sur Alert (Alerter), la **Category (Catégorie)** est définie sur protocol-anomaly (anomalie de protocole), et la **Severity (Gravité)** est définie sur Any (Tout). Surveillez votre trafic pour déterminer si des applications critiques internes utilisent des protocoles établis de

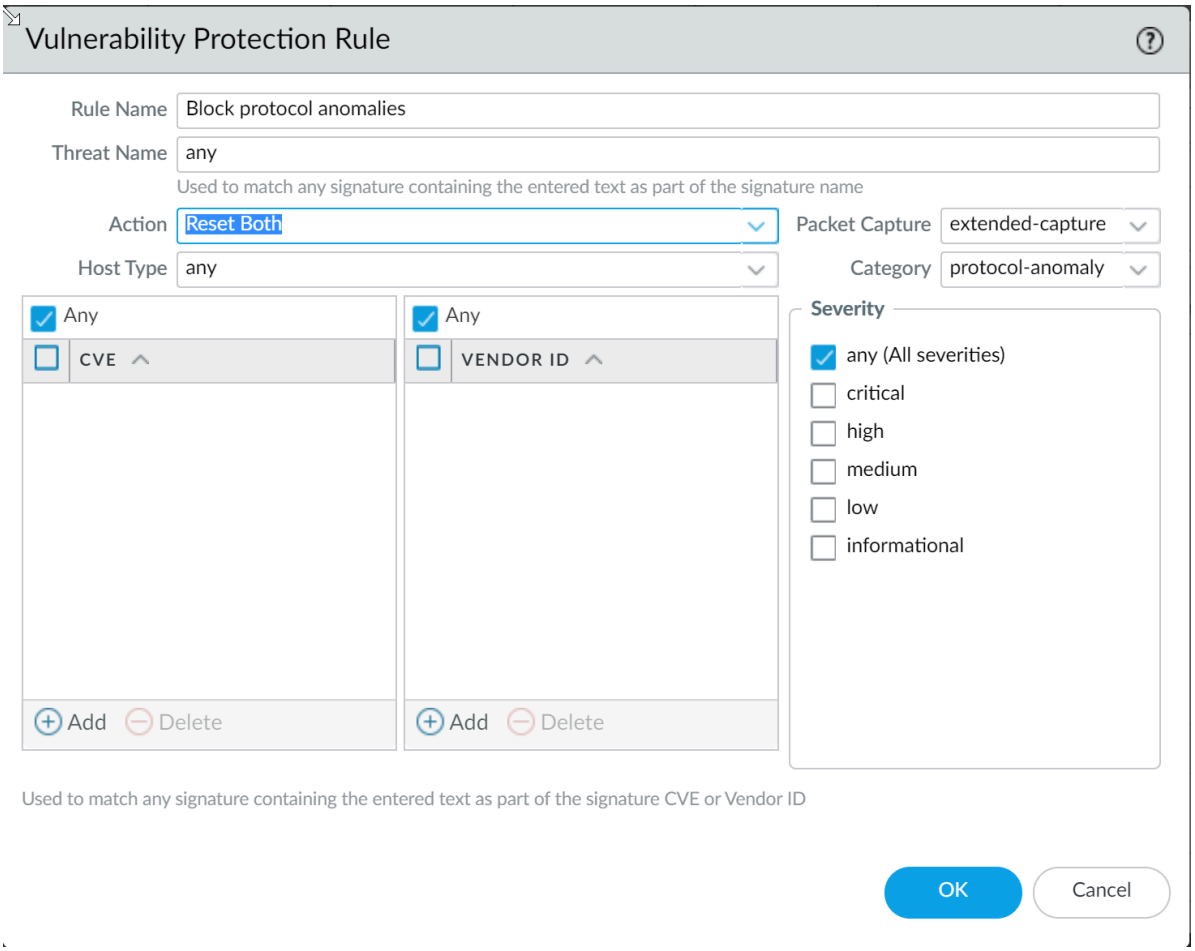
manière non standard. Si c'est le cas, continuez à autoriser les anomalies de protocole pour ces applications, puis bloquez les anomalies de protocole de toutes les autres applications.



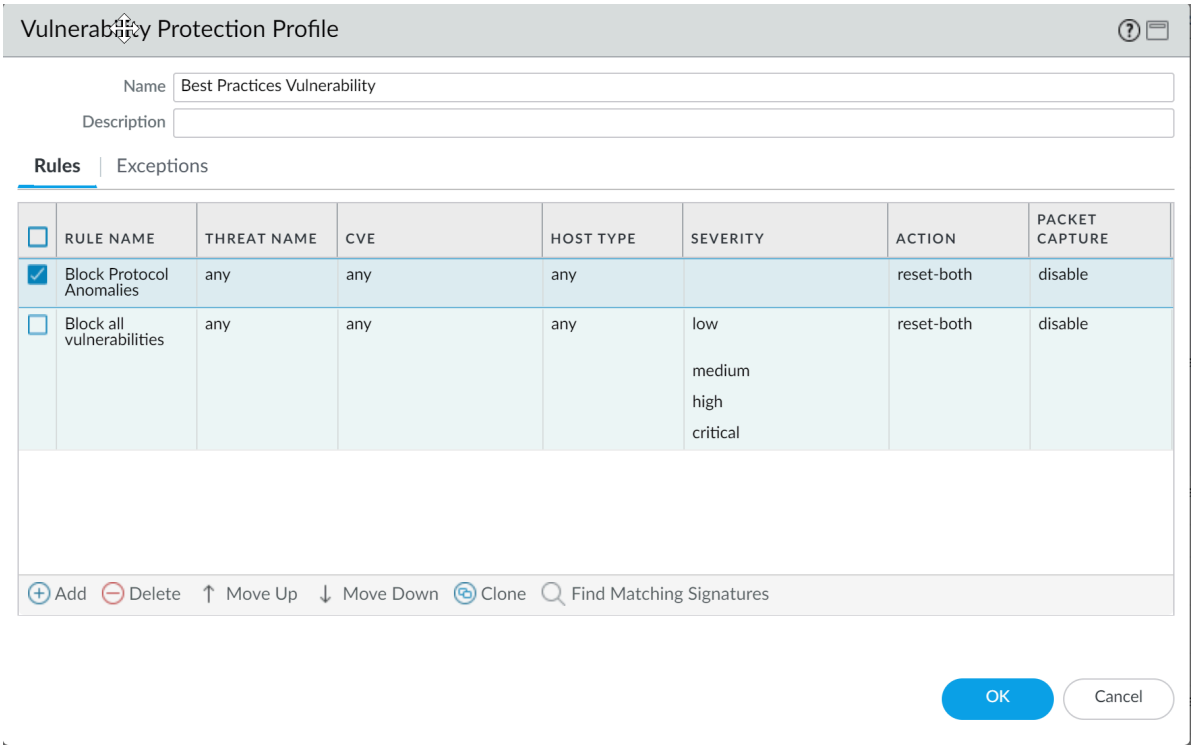
- Bloquez les anomalies de protocole :

  Créez une règle de profil de protection contre les vulnérabilités pour laquelle la **Category (Catégorie)** est définie sur protocol-anomaly (anomalie de protocole), l'**Action (Action)** est définie sur Reset Both (Réinitialiser les deux), et la **Severity (Gravité)** définie sur Any (Tout).




- Vous pouvez éventuellement autoriser les anomalies de protocole pour les applications critiques qui utilisent des protocoles établis de manière non standard. Pour ce faire, créez une règle de profil de protection contre les vulnérabilités qui autorise les anomalies de protocole : définissez l'**Action** de la règle sur Allow (Autoriser), la **Category (Catégorie)** sur protocol-anomaly (anomalie de protocole) et la **Severity (Sévérité)** sur Any (Tout). Associez la règle de profil de protection contre les vulnérabilités à la règle de la politique de sécurité qui applique le trafic vers les applications critiques et depuis ces dernières.

- Ajoutez une autre règle au profil de protection contre les vulnérabilités pour bloquer toutes les vulnérabilités ayant un niveau de gravité faible et plus élevé. Cette règle doit figurer après la règle qui bloque les anomalies de protocole.




- Passez à l'association des profils de sécurité suivants à vos règles de politique de sécurité pour bénéficier d'une protection basée sur les signatures :
  - Un profil antispyware pour bloquer tous les logiciels espions ayant un niveau de gravité faible et plus élevé.
  - Un profil antivirus pour bloquer tout contenu correspondant à une signature antivirus.

# Paramétrage des profils Antivirus, Antispyware et Protection contre les vulnérabilités

Chaque pare-feu de dernière génération Palo Alto Networks est fourni avec les profils Antivirus, Antispyware et Protection contre les vulnérabilités prédéfinis que vous pouvez associer aux politiques de sécurité. Il y a un seul profil Antivirus prédéfini, **DEFAULT (par défaut)**, qui utilise l'action par défaut pour chaque protocole (blocage du trafic HTTP, FTP et SMB, et alerte pour le trafic SMTP, IMAP et POP3). Il existe deux profils Antispyware et Protection contre les vulnérabilités prédéfinis :

- **default (par défaut)** : applique l'action par défaut à l'ensemble des événements de protection contre les vulnérabilités/logiciels espions du client et du serveur dont le niveau de gravité est critique, élevé et moyen. Il ne détecte pas les événements dont le niveau de gravité est faible et informations.
- **strict** : applique la réponse de blocage à l'ensemble des événements de protection contre les vulnérabilités/logiciels espions du client et du serveur dont le niveau de gravité est critique, élevé et moyen. Par ailleurs, il utilise l'action par défaut pour les événements dont le niveau de gravité est faible et informations.

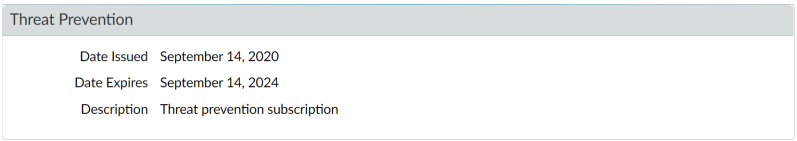
Afin de vous assurer que le trafic entrant sur votre réseau ne comporte aucune menace, associez les profils prédéfinis à vos politiques d'accès Web de base. Lorsque vous surveillez le trafic sur votre réseau et étendez votre base de règles de politique, vous pouvez créer des profils plus granulaires pour répondre à vos besoins spécifiques en matière de sécurité.

Utilisez le flux de travail suivant pour paramétrer les Profils de Sécurité relatifs aux Antivirus, Antispyware et Protection contre les vulnérabilités.

*Palo Alto Networks définit une action par défaut pour toutes les signatures antispyware et de protection contre les vulnérabilités. Pour afficher l'action par défaut, sélectionnez* ***Objects (Objets)*** *>* ***Security Profiles (Profils de sécurité)*** *>* ***Anti-Spyware (Antispyware)*** *ou* ***Objects (Objets)*** *>* ***Security Profiles (Profils de sécurité)*** *>* ***Vulnerability Protection (Protection contre les vulnérabilités)****, puis choisissez un profil. Cliquez sur l'onglet Exceptions puis sur Montrer toutes les signatures pour voir une liste de toutes les signatures et l'****Action*** *correspondante par défaut. Pour modifier l'action par défaut, vous devez créer un nouveau profil, puis spécifier une* ***Action*** *et/ou ajouter des exceptions de signature individuelle dans les* ***Exceptions*** *du profil.*

**STEP 1 |** Vérifiez que vous disposez d'un abonnement Prévention des menaces.

L'abonnement Prévention des menaces regroupe les fonctions Antivirus, Anti-logiciel espion et Protection contre les vulnérabilités. Pour vérifier si vous disposez d'un abonnement Prévention des menaces actif, sélectionnez **Device (Périphérique)** > **Licenses (Licences)** et vérifiez que la date d'expiration de **Threat Prevention (Prévention des Menaces)** se situe dans l'avenir.



**STEP 2 |** Téléchargez la dernière mise à jour du contenu :

1. Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**, puis cliquez sur **Check Now (Vérifier maintenant)** au bas de la page, pour récupérer les dernières signatures.
2. Dans la colonne **Actions**, cliquez sur **Download (Télécharger)** et installez les dernières mises à jour Antivirus, et ensuite téléchargez et **Install (Installez)** les dernières mises à jour pour les Applications et les Menaces.

**STEP 3 |** Planifiez les mises à jour de contenu.

*Passez en revue les* Meilleures pratiques pour les mises à jour du contenu de menace et des applications *pour connaître les informations importantes sur le déploiement des mises à jour.*

1. Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**, puis cliquez sur **Schedule (Calendrier)** pour récupérer automatiquement les mises à jour de signatures pour les **Antivirus** et les **Applications and Threats (Applications et Menaces)**.
2. Précisez la fréquence et la durée des mises à jour :
   - **download-only (télécharger uniquement)** : Le pare-feu télécharge automatiquement les dernières mises à jour selon le calendrier défini mais vous devez les **Install (Installer)** manuellement.
   - **download-and-install (télécharger et installer)** : Le pare-feu télécharge automatiquement les dernières mises à jour selon le calendrier défini et les installe.
3. Cliquez sur **OK** pour sauvegarder le calendrier de mises à jour ; une validation n'est pas requise.
4. (Facultatif) Vous pouvez également saisir le nombre d'heures dans le champ **Threshold (Seuil)** pour indiquer l'antériorité minimale d'une mise à jour avant tout téléchargement. Par exemple, si vous définissez le **Threshold (Seuil)** à **10**, la signature doit dater d'au moins 10 heures avant d'être téléchargée, quel que soit le calendrier.
5. (Configuration HD uniquement) Vous pouvez également choisir de **Sync To Peer (Synchroniser avec l'homologue)**, pour activer la synchronisation de mise à jour de contenu après le téléchargement/l'installation (les paramètres du calendrier ne sont pas transmis au pare-feu homologue ; vous devez configurer manuellement le calendrier sur chaque pare-feu).

   D'autres considérations sont à prendre en compte quand vous choisissez de **Sync To Peer (Synchroniser avec l'homologue)** et la façon de le mettre en place, selon votre déploiement HD :

   - **HD actif/passif** : si le port MGT est utilisé pour le téléchargement des mises à jour de contenu, vous devez configurer les deux pare-feu pour qu'ils procèdent aux téléchargements et aux installations de manière indépendante. Toutefois, si vous utilisez un port de données pour les mises à jour de contenu, le pare-feu passif ne téléchargera ni n'installera aucune mise à jour avant de devenir actif. Pour garder les calendriers synchronisés sur les deux pare-feu quand vous utilisez un port de données pour les mises à jour, programmez les mises à jour sur les deux pare-feu et ensuite activez **Sync To Peer (Synchroniser avec l'homologue)** pour permettre le téléchargement des mises à jour et leur transmission au pare-feu passif, quel que soit le pare-feu actif.

- **HD actif/actif** : si le port MGT est utilisé pour le téléchargement des mises à jour de contenu sur les deux pare-feu, vous devez sélectionner **download-and-install (télécharger et installer)** sur les deux pare-feu et ne pas activer l'option **Sync To Peer (Synchroniser avec l'homologue)**. Toutefois, si vous utilisez un port de données, sélectionnez **download-and-install (télécharger et installer)** sur les deux pare-feu, puis activez **Sync To Peer (Synchroniser avec l'homologue)**. Ainsi, si l'état d'un pare-feu devient actif secondaire, cette option permet au pare-feu actif de télécharger et d'installer les mises à jour et de les transmettre au pare-feu actif secondaire.

**STEP 4 |** (Facultatif) Créez des profils de sécurité personnalisés pour les antivirus, les antispyware, et la protection contre les vulnérabilités.

Vous pouvez également utiliser les profils stricts ou par défaut prédéfinis.

Passez en toute sécurité ***aux*** profils de sécurité exemplaire ***pour disposer de meilleure posture de sécurité.***

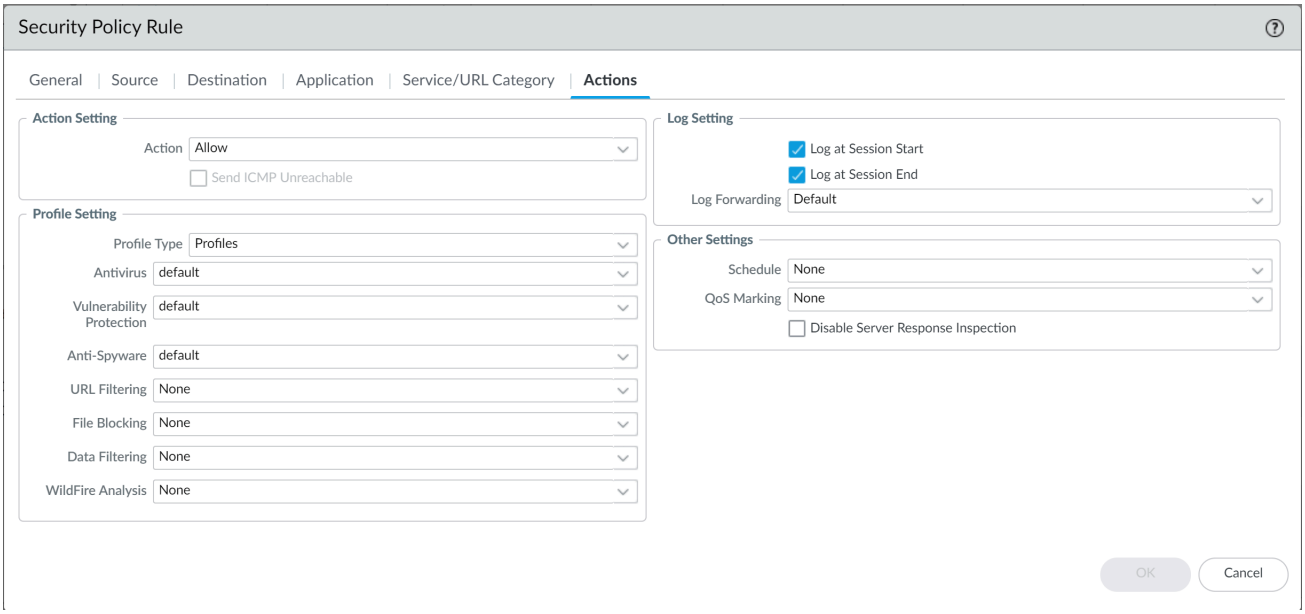
- Pour créer des Profils Antivirus personnalisés, sélectionnez **Objects (Objets)** > **Security Profiles (Profils de Sécurité)** > **Antivirus** et **Add (Ajoutez)** un nouveau profil. Utilisez les étapes de transition vers un profil antivirus pour atteindre votre objectif en toute sécurité
- Pour créer des Anti-spyware Profiles (Profils Antispyware) personnalisés, sélectionnez **Objects (Objets)** > **Security Profiles (Profils de Sécurité)** > **Anti-spyware (Antispyware)** et **Add (Ajoutez)** un nouveau profil. Utilisez les étapes de transition vers un profil antispyware pour atteindre votre objectif en toute sécurité
- Pour créer des Vulnerability Protection Profiles (Profils de Protection contre les Vulnérabilités) personnalisés, sélectionnez **Objects (Objets)** > **Security Profiles (Profils de Sécurité)** > **Vulnerability Protection (Protection contre les Vulnérabilités)** et **Add (Ajoutez)** un nouveau profil. Utilisez les étapes de transition vers un profil de protection contre les vulnérabilités pour atteindre votre objectif en toute sécurité

**STEP 5 |** Associez les profils de sécurité à vos règles de politique de sécurité.

*Quand vous configurez le pare-feu avec une règle de Politique de sécurité qui utilise un profil de Protection contre les vulnérabilités pour bloquer des connexions, le pare-feu bloque automatiquement ce trafic au niveau matériel (reportez-vous à la section* Surveillance des Adresses IP bloquées*).*

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et sélectionnez la règle que vous voulez modifier.
2. Dans l'onglet **Actions**, sélectionnez **Profiles (Profils)** comme **Profile Type (Type de Profil)**.
3. Sélectionnez les profils de sécurité que vous avez créés pour **Antivirus**, **Anti-Spyware (Antispyware)**, et **Vulnerability Protection (Protection contre les Vulnérabilités)**.




**STEP 6 |** Validez vos modifications.

Cliquez sur **Commit (Valider)**.

# Sécurité DNS

La sécurité DNS est un service de prévention contre les menaces en constante évolution qui a été conçu pour protéger et défendre votre réseau contre les menaces avancées au moyen de DNS. En exploitant l'apprentissage machine et l'analyse prédictive, le service fournir une analyse en temps réel des requêtes DNS et produit et distribue rapidement des signatures DNS qui sont spécialement conçues pour vous protéger contre les logiciels malveillants à l'aide de DNS pour le vol C2 et de données. Conjuguée à une architecture cloud extensible, elle donne accès à un système de renseignements sur les menaces évolutif qui permet de tenir à jour les protections de votre réseau.

- À propos de la sécurité DNS
- Protections et signatures DNS fournies par le cloud
- Analyse de sécurité DNS
- Activation de la sécurité DNS
- Collecte et journalisation des données de sécurité DNS

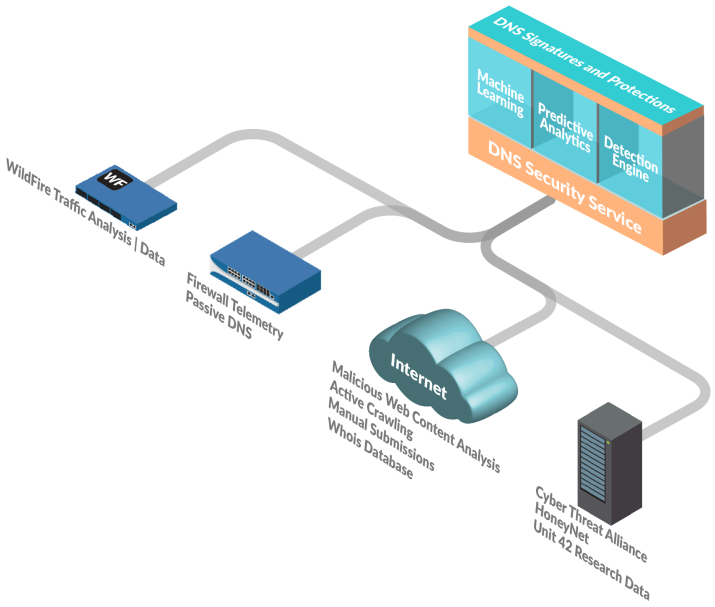
## À propos de la sécurité DNS

Lorsqu'ils possèdent une licence de prévention contre les menaces, les clients peuvent configurer leurs pare-feu pour qu'ils mettent en entonnoir les requêtes DNS à l'aide d'une liste de domaines générée par Palo Alto Networks. Ces listes de signatures DNS accessibles localement et personnalisables sont fournies avec les mises à jour antivirus et WildFire et comprennent les menaces les plus pertinentes pour l'application de la politique et la protection au moment de la publication. Pour améliorer la protection contre les menaces au moyen de DNS, l'abonnement à la sécurité DNS permet aux utilisateurs d'accéder à des protections en temps réel au moyen d'analyses prédictives avancées. En utilisant des techniques comme la détection de la tunnelisation DGA/DNS et l'apprentissage machine, les menaces cachées dans le trafic DNS peut être proactivement identifié et partagé à l'intérieur d'un service Cloud évolutif à l'infini. Comme les protections et signatures DNS sont stockées dans une architecture Cloud, vous pouvez accéder à la base de données complète et évolutive des signatures qui ont été générées à l'aide d'une multitude de sources de données. Vous pouvez ainsi vous défendre contre un éventail de menaces à l'aide de DNS en temps réel et contre les nouveaux domaines malveillants générés. Pour vous défendre contre les menaces futures, des mises à jour des capacités d'analyse, de détection et de prévention du service de sécurité DNS sera disponible par l'intermédiaire des versions de contenu.

Pour accéder au service de sécurité DNS, vous devez disposer d'une licence de sécurité DNS et de prévention contre les menaces.

Le diagramme suivant décrit l'utilisation que fait le service de sécurité DNS des diverses sources de données pour générer des signatures DNS :

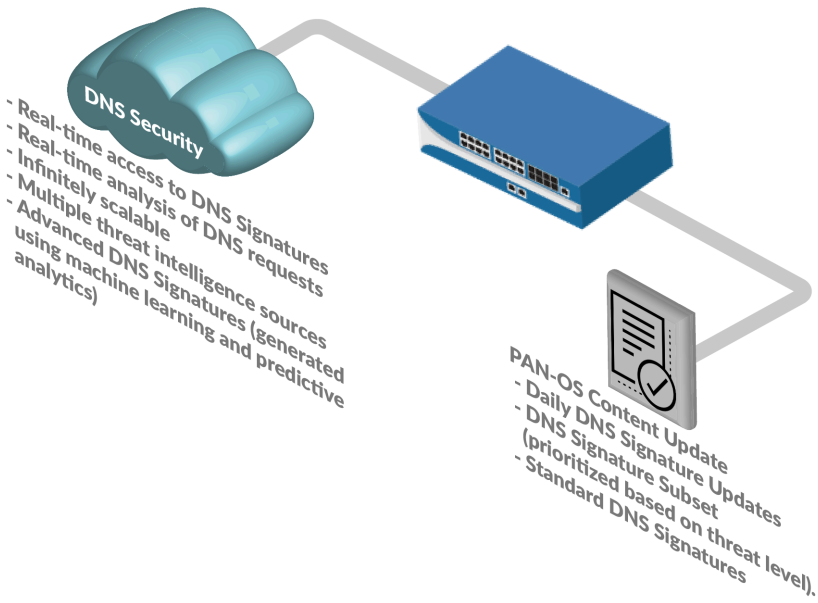
 




# Protections et signatures DNS fournies par le cloud

En tant que service infonuagique, la sécurité DNS vous permet d'accéder à une source de protections et de signatures DNS infiniment extensible pour défendre votre organisation contre les domaines malveillants. Les protections et signatures de domaine générées par Palo Alto Networks proviennent d'une multitude de sources, y compris l'analyse du trafic WildFire, le DNS passif, l'explorative active du Web et l'analyse du contenu Web malveillant, l'analyse des bacs à sable URL, le réseau HoneyNet, ingénierie DGA inverse, les données télémétriques, whois, l'organisation de recherche Unité 42 et des sources de données tierces, comme la Cyber Threat Alliance. Cette base de données sur le cloud à la demande permet aux utilisateurs d'accéder à l'ensemble des signatures DNS de Palo Alto Networks, y compris des signatures générées à l'aide de techniques d'analyse avancées, ainsi qu'à l'analyse en temps réel des requêtes DNS. Les ensembles de signatures DNS localement disponibles et téléchargeables (compris dans les mises à jour antivirus et de WildFire) s'accompagnent d'une limite de capacité programmée en dur de 100 000 signatures et ne comprennent pas les signatures générées par l'analyse avancée. Pour mieux accueillir l'afflux de nouvelles signatures DNS qui sont produites quotidiennement, la base de données de signatures dans le cloud fournit aux utilisateurs un accès instantané aux signatures DNS nouvellement ajoutée sans qu'ils aient à télécharger des mises à jour. En cas d'échec ou d'indisponibilité de la connectivité réseau, le pare-feu utilise l'ensemble de signatures DNS comprises dans la base de données.




# Analyse de sécurité DNS

Le service de sécurité DNS effectue une analyse en temps réel des demandes DNS en utilisant l'analyse prédictive et l'apprentissage machine sur de multiples sources de données DNS. Il est utilisé pour générer des protections contre les menaces basées sur le DNS, qui sont accessibles en temps réel grâce à la configuration du profil de sécurité antispyware joint à une règle de politique de sécurité. Chaque catégorie de menace DNS (la source de signature DNS) vous permet de définir des actions stratégiques distinctes ainsi qu'un niveau de gravité de journal pour un type de signature spécifique. Cela vous permet de créer des politiques de sécurité spécifiques basées sur la nature de la menace, en fonction des protocoles de sécurité de votre réseau. Palo Alto Networks génère et maintient également une liste de domaines explicitement autorisés basée sur les mesures de PAN-DB et Alexa. Ces domaines de liste d'autorisation sont fréquemment consultés et sont connus pour être exempts de contenu malveillant. Les catégories de sécurité DNS et la liste d'autorisation sont mises à jour et extensibles par le biais des publications de contenu PAN-OS.

Vous pouvez consulter les données statistiques DNS de votre organisation générées par le service DNS Security Cloud en utilisant AutoFocus. Cela permet une évaluation rapide et visuelle décrivant la répartition des demandes DNS passant par votre réseau en fonction des catégories DNS disponibles. Vous pouvez également récupérer des informations sur le domaine, ainsi que les détails de la transaction, tels que la latence et le TTL, en utilisant la commande **`test dns-proxy dns-signature fqdn <domain>`**.

*Lors de la mise à niveau vers PAN-OS 10.0 et ultérieur, la source de sécurité DNS est redéfinie dans de nouvelles catégories pour fournir des contrôles granulaires étendus ; en conséquence, les nouvelles catégories écraseront l'action précédemment définie et acquerront des paramètres par défaut. Assurez-vous d'appliquer à nouveau les paramètres de mise en entonnoir, de gravité du journal et de capture de paquet appropriés pour les catégories de sécurité DNS nouvellement définies.*

Le service de sécurité DNS prend actuellement en charge la détection des catégories de menaces DNS suivantes :

- **Command and Control Domains (Domaines de commande et contrôle)** : les C2 comprennent les URL et les domaines utilisés par des logiciels malveillants et/ou des systèmes compromis pour communiquer subrepticement avec le serveur distant d'un attaquant afin de recevoir des commandes malveillantes ou d'exfiltrer des données (cela inclut la détection de tunnellisation DNS et la détection DGA), ou épuise les ressources sur des serveurs DNS autorisés cibles (comme NXNSattack).
  - **DNS Tunnel Detection (Détection de tunnel DNS)** : la tunnellisation DNS peut être utilisée par les attaquants pour coder les données de programmes et protocoles non-DNS dans les requêtes et réponses DNS. Les pirates disposent ainsi d'un canal ouvert par l'intermédiaire duquel ils peuvent transférer des fichiers ou accéder à distance au système. La détection des tunnels DNS utilise l'apprentissage machine pour analyser les qualités comportementales de requêtes DNS, y compris l'analyse de la fréquence n-gramme des domaine, l'entropie, le taux de requêtes et les modèles pour déterminer si la requête est conforme à une attaque basée sur la tunnellisation DNS. Cela inclut certains malwares de tunneling DNS de nouvelle génération qui exfiltrent lentement les données dans plusieurs domaines pour éviter la détection, tels que TriFive et Snugy. Conjugué aux actions automatisées des politiques du pare-feu, cela vous permet de rapidement détecter les C2 ou le vol de données caché dans les tunnels DNS et de les bloquer automatiquement, selon vos règles de politique définies.
  - **DGA Detection (Détection DGA)** : les algorithmes de génération de domaines (DGA) sont utilisés pour générer automatiquement des domaines, généralement en grand nombre dans le cadre de l'établissement d'un canal de communication de commande et de contrôle (C2) malveillant. Les logiciels malveillants basés sur DGA (tels que Pushdo, BankPatch et CryptoLocker) limitent le nombre de domaines pouvant être bloqués en cachant l'emplacement de leurs serveurs C2 actifs parmi un grand nombre de suspects possibles, et peuvent être générés de manière algorithmique en fonction de facteurs tels que l'heure de la journée, les clés cryptographiques, les schémas nominatifs dérivés du dictionnaire ou d'autres valeurs uniques. Bien que la plupart des domaines générés par un DGA ne se résolvent pas en un domaine valide, ils doivent tous être identifiés pour offrir une pleine protection contre une menace donnée. L'analyse du DGA détermine la probabilité qu'un domaine ait été généré par une machine, plutôt que par une personne, en utilisant des techniques d'ingénierie inverse et en analysant d'autres techniques fréquemment utilisées que l'on trouve dans les DGA. Palo Alto Networks utilise ensuite ces caractéristiques pour identifier et bloquer, en temps réel, les menaces basées sur les DGA qui étaient préalablement inconnues.
  - **NXNSAttack** : la vulnérabilité NXNSAttack présente dans le protocole DNS affecte tous les résolveurs DNS récursifs et peut être utilisée par des acteurs malveillants pour lancer des attaques d'amplification de type DDos afin de perturber le fonctionnement normal des serveurs DNS faisant autorité et vulnérables. NXNSAttack peut introduire des pics de trafic massifs sur un serveur DNS faisant autorité en forçant le résolveur DNS récursif à émettre un grand nombre de requêtes invalides pour potentiellement arrêter le serveur.
  - **DNS Rebinding** : les attaques de rebinding DNS attirent les utilisateurs vers un domaine contrôlé par un attaquant configuré avec un paramètre TTL court pour manipuler la façon dont les noms de domaine sont résolus pour exploiter et contourner la politique de même origine dans les navigateurs. Cela permet à des acteurs malveillants d'utiliser la machine cliente comme intermédiaire pour attaquer ou accéder à une ressource contenue dans un réseau privé.

- **Dynamic DNS Hosted Domains (Domaines hébergés par le DNS dynamique)** : les services de DNS dynamique (DDNS) fournissent un mappage entre les noms d'hôtes et les adresses IP en temps quasi réel pour continuer à changer les adresses IP liées à un domaine spécifique, lorsque les IP statiques ne sont pas disponibles. Les attaquants disposent ainsi d'une méthode pour infiltrer les réseaux en utilisant les services DDNS pour modifier les adresses IP qui hébergent les serveurs de commande et de contrôle. Les campagnes de logiciels malveillants et les kits d'exploitation peuvent utiliser les services DDNS dans le cadre de leur stratégie de distribution de la charge utile. En utilisant les domaines DDNS dans le cadre de leur infrastructure de noms d'hôtes, les adversaires peuvent changer l'adresse IP associée à des enregistrements DNS donnés et éviter plus facilement la détection. La sécurité DNS détecte les services DDNS exploiteurs en filtrant et en croisant les données DNS provenant de diverses sources pour générer des listes de candidats qui sont ensuite validées pour maximiser la précision.
- **Malware Domains (Domaines malveillants)** : les domaines malveillants hébergent et distribuent des logiciels malveillants et peuvent inclure des sites web qui tentent d'installer diverses menaces (telles que des exécutables, des scripts, des virus, des téléchargements automatiques). Les domaines malveillants se distinguent des domaines C2 en ce sens qu'ils acheminent des charges utiles malveillantes dans votre réseau via une source externe, alors qu'avec les C2, les terminaux infectés tentent généralement de se connecter à un serveur distant pour récupérer des instructions supplémentaires ou d'autres contenus malveillants.
- **Newly Registered Domains (Domaines récemment enregistrés)** : les domaines récemment enregistrés sont des domaines nouveaux, jamais enregistrés, qui ont été récemment ajoutés par un opérateur TLD ou une entité. Si de nouveaux domaines peuvent être créés à des fins légitimes, la grande majorité d'entre eux sont souvent utilisés pour faciliter des activités malveillantes, comme le fonctionnement en tant que serveurs C2 ou utilisés pour distribuer des logiciels malveillants, du spam, des PUP/logiciels publicitaires. Palo Alto Networks détecte les domaines récemment enregistrés en surveillant des flux spécifiques (registres de domaines et bureaux d'enregistrement) et en utilisant des fichiers de zone, le DNS passif, les données WHOIS pour détecter les campagnes d'enregistrement.
- **Phishing Domains (Domaines de hameçonnage)** : les domaines de hameçonnage tentent d'inciter les utilisateurs à soumettre des données sensibles, telles que des informations personnelles ou des identifiants d'utilisateur, en se faisant passer pour des sites web légitimes par le biais du hameçonnage ou du pharming. Ces activités malveillantes peuvent être menées par des campagnes d'ingénierie sociale (par lesquelles une source apparemment fiable manipule les utilisateurs pour qu'ils soumettent des informations personnelles par e-mail ou d'autres formes de communications électroniques) ou par la réorientation du trafic web, qui dirige les utilisateurs vers des sites frauduleux qui semblent légitimes.
- **Grayware Domains (Domaines indésirables)** : (disponible avec l'installation du contenu PAN-OS version 8290 et ultérieure). Les domaines indésirables ne constituent généralement pas une menace directe pour la sécurité, mais ils peuvent faciliter les vecteurs d'attaque, produire divers comportements indésirables ou simplement contenir des contenus douteux/offensifs.Cela peut inclure des sites Internet qui :
  - Tenter de tromper les utilisateurs pour qu'ils accordent un accès à distance.
  - Contient des logiciels publicitaires et d'autres applications non sollicitées (telles que des cryptomineurs, des pirates de l'air et des PUP [programmes potentiellement indésirables]).
  - Déployez des actions de dissimulation d'identification de domaine à l'aide de techniques de flux rapide.

  - Démontrer le comportement et l'utilisation malveillants comme en témoignent les analyses prédicatives de sécurité DNS (NRD malveillant).
  - Tirez parti des erreurs de l'utilisateur lors de la saisie des adresses de pages Web (typosquattage de domaines).
  - Redirigez le trafic d'une source légitime vers un site Web malveillant en raison d'un enregistrement DNS mal configuré ou périmé sur un serveur DNS faisant autorité qui n'a pas été supprimé ou corrigé (DNS suspendu).
  - Promouvoir des activités illégales ou des escroqueries.
- **Parked Domains (Domaines en parking)** : (disponible avec l'installation du contenu PAN-OS version 8318 et ultérieure) les domaines en parking sont généralement des sites web inactifs qui hébergent un contenu limité, souvent sous la forme de clics publicitaires qui peuvent générer des revenus pour l'entité hôte, mais qui ne contiennent généralement pas de contenu utile pour l'utilisateur final. Bien qu'ils fonctionnent souvent comme un substitut légitime ou comme une simple nuisance bénigne, ils pourraient également être utilisés comme un vecteur possible de distribution de logiciels malveillants.
- **Proxy Avoidance and Anonymizers (Contournement de proxy et anonymiseurs)** : (disponible avec l'installation du contenu PAN-OS version 8340 et ultérieure) le contournement de proxy et les anonymiseurs sont un trafic vers des services qui sont utilisés pour contourner les politiques de filtrage de contenu. Les utilisateurs qui tentent de contourner les politiques de filtrage de contenu d'une organisation via les services proxy de l'anonymiseur sont bloqués au niveau du DNS.

## Activation de la sécurité DNS

Pour activer la mise en entonnoir DNS pour les requêtes de domaine utilisant la sécurité DNS, vous devez activer votre abonnement à la sécurité DNS, créer (ou modifier) une politique antispyware pour référencer le service de sécurité DNS, configurer la gravité du journal et les paramètres de politique pour chaque catégorie de signature DNS, puis joindre le profil à une règle de politique de sécurité.

**STEP 1 |** Activation des licences d'abonnement.

**STEP 2 |** Vérifiez que l'ID d'application ***paloalto-dns-security*** dans votre stratégie de sécurité est configuré pour enable (activer) le trafic provenant du service de sécurité cloud de sécurité DNS.

> ***Si le déploiement de votre pare-feu achemine votre trafic de gestion via un pare-feu de périmètre Internet configuré pour appliquer les politiques de sécurité App-ID, vous devez autoriser les App-ID sur le pare-feu de périmètre ; ne pas le faire empêchera la connectivité de sécurité DNS.***

**STEP 3 |** Configurez les paramètres de la politique de sécurité de signature DNS pour envoyer les demandes de DNS malveillants à la mise en entonnoir définie.

*Si vous utilisez une liste dynamique externe comme liste d'autorisation de domaine, elle n'a pas la priorité sur les actions de politique de domaine de sécurité DNS. Par conséquent, lorsqu'il existe une correspondance de domaine avec une entrée dans l'EDL et une catégorie de domaine de sécurité DNS, l'action spécifiée sous Sécurité DNS est toujours appliquée, même lorsque l'EDL est explicitement configuré avec une action Autoriser. Si vous souhaitez ajouter des exceptions de domaine DNS, configurez un EDL avec une action d'alerte ou ajoutez-les à la liste d'autorisation de domaine DNS/FQDN située dans l'onglet Exceptions DNS (étape 8).*

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware (Antispyware)**.
2. Créez ou modifiez un profil existant ou sélectionnez un des profils par défaut et clonez-le.
3. Donnez un **Name (Nom)** au profil et vous pouvez également fournir une description.
4. Sélectionnez l'onglet **DNS Policies (Politiques de DNS)**.
5. La colonne **Signature Source (Source de signature)**, sous la rubrique DNS Security (Sécurité DNS), contient des sources de signature DNS configurables individuellement, qui vous permettent de définir des actions stratégiques distinctes ainsi qu'un niveau de gravité du journal.

   *Palo Alto Networks recommande de modifier les paramètres par défaut de vos politiques DNS pour les sources de signature afin d'assurer une couverture optimale et de faciliter la réponse aux incidents et les mesures correctives. Suivez les meilleures pratiques pour configurer vos paramètres de sécurité DNS comme indiqué dans les* Meilleures pratiques pour sécuriser votre réseau contre les fuites au niveau des couches 4 et 7**.**

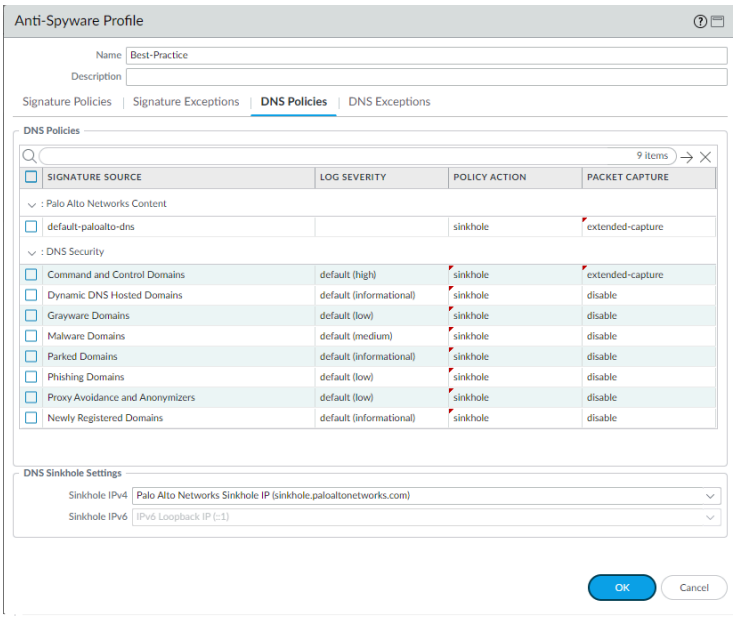
   - Indiquez le niveau de gravité du journal qui est enregistré lorsque le pare-feu détecte un domaine correspondant à une signature DNS. Pour plus d'informations sur les différents niveaux de gravité du journal, consultez Niveaux de gravité des menaces.
   - Sélectionnez une action à prendre lorsque des requêtes DNS correspondant à des sites malveillants connus sont envoyées pour la source de signature de sécurité DNS. Les options sont les suivantes : Alerte, Autoriser, Bloquer ou mise en entonnoir. Vérifiez que l'action est définie sur la mise en entonnoir.
   - Dans le menu déroulant **Packet Capture (Capture de paquet)**, sélectionnez **single-packet (paquet unique)** pour capturer le premier paquet de la session ou **extended-capture (capture étendue)** pour définir entre 1 et 50 paquets. Vous pouvez ensuite utiliser les captures de paquets pour une analyse plus approfondie.
6. À la section **DNS Sinkhole Settings (Paramètres de mise en entonnoir DNS)**, vérifiez que l'option **Sinkhole (Mise entonnoir)** est activée. Pour votre facilité, l'adresse entonnoir par défaut (sinkhole.paloaltonetworks.com) permet d'accéder à un serveur de Palo Alto Networks. Palo Alto Networks peut automatiquement actualiser cette adresse par l'intermédiaire de mises à jour de contenu.

   Si vous souhaitez modifier l'adresse **Sinkhole IPv4 (IPv4 d'entonnoir)** ou **Sinkhole IPv6 (IPv6 d'entonnoir)** vers un serveur local sur votre réseau ou vers une adresse de boucle,

reportez-vous à la section Configuration de l'adresse IP entonnoir vers un serveur local sur votre réseau.

7. Cliquez sur **OK (OK)** pour enregistrer le profil antispyware.




**STEP 4 |** Associez le profil antispyware à une règle de politique de sécurité.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
2. Sélectionnez ou créez une **Security Policy Rule (Règle de politique de sécurité)**.
3. Dans l'onglet **Actions (Actions)**, cochez la case **Log at Session End (Journalisation en fin de session)** pour activer la journalisation.
4. Dans la section Paramètre de profil, cliquez sur la liste déroulante **Profile Type (Type de profil)** pour voir tous les **Profiles (Profils)**. Sélectionnez le nouveau profil ou le profil modifié dans la liste déroulante **Anti-spyware (Antispyware)**.
5. Cliquez sur **OK (OK)** pour enregistrer la règle de politique.

**STEP 5 |** Vérifiez que l'action de politique est appliquée.

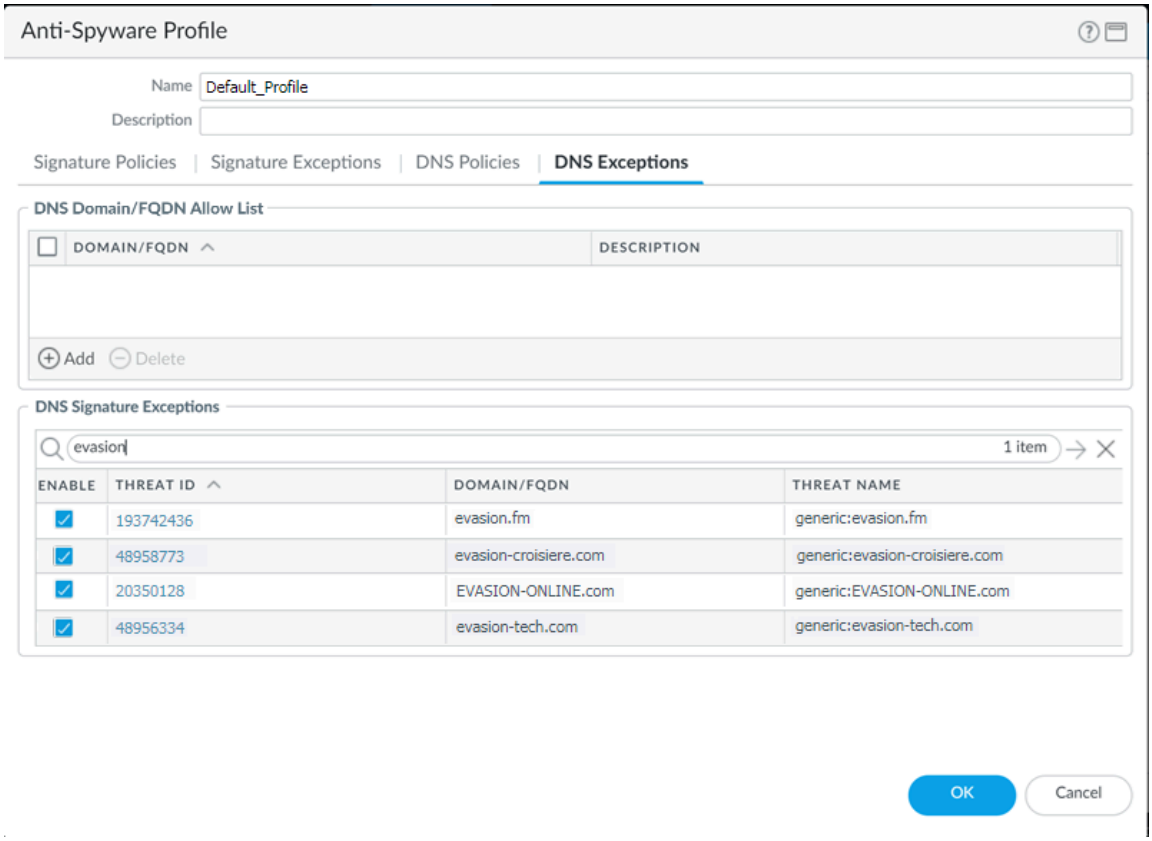
1. Accédez aux domaines d'essai suivants pour vérifier que l'action de la politique pour un type de menace donné est appliquée :
   - C2 : test-c2.testpanw.com
   - DNS Tunneling : test-dnstun.testpanw.com
   - DGA : test-dga.testpanw.com
   - Dynamic DNS : test-ddns.testpanw.com
   - Malware : test-malware.testpanw.com
   - Domaines récemment enregistrés : test-nrd.testpanw.com
   - Hameçonnage : test-phishing.testpanw.com
   - Logiciel indésirable : test-grayware.testpanw.com
   - Domaine en parking : test-parked.testpanw.com
   - Contournement de proxy et anonymiseurs : test-proxy.testpanw.com
2. Pour surveiller l'activité sur le pare-feu :
   1. Sélectionnez **ACC (ACC)** et ajoutez un domaine d'URL en tant que filtre général pour afficher l'activité des menaces et l'activité bloquée pour le domaine auquel vous avez accédé.
   2. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menace)** et filtrez par `(action eq sinkhole)` pour afficher les journaux des domaines mis en entonnoir.

**STEP 6 |** Identifier les hôtes de trafic infectés dans les journaux du trafic

**STEP 7 |** (Facultatif) Ajoutez des exceptions aux signatures de domaine pour les situations où des faux-positifs se produisent.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware (Antispyware)**.
2. Sélectionnez un profil à modifier.
3. **Add (Ajoutez)** ou modifiez le profil antispyware duquel vous souhaitez exclure la signature de menaces, puis sélectionnez **DNS Exceptions (Exceptions de DNS)**.
4. Cherchez une signature DNS à exclure en entrant le nom ou le FQDN.
5. Cochez la case pour chaque **Threat ID (ID de menace)** de la signature DNS que vous souhaitez exclure de l'application.
6. Cliquez sur **OK (OK)** pour enregistrer votre profil antispyware, qu'il soit nouveau ou modifié.



**STEP 8 |** (Facultatif) Ajoutez une liste d'autorisation pour spécifier une liste de domaines DNS/FQDN qui doivent être explicitement autorisés.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware (Antispyware)**.
2. Sélectionnez un profil à modifier.
3. **Add (Ajoutez)** ou modifiez le profil antispyware duquel vous souhaitez exclure la signature de menaces, puis sélectionnez **DNS Exceptions (Exceptions de DNS)**.
4. Pour **Add (Ajouter)** une nouvelle **FQDN Allow List (Liste d'autorisation FQDN)**, fournissez le domaine DNS ou l'emplacement du FQDN et une description.
5. Cliquez sur **OK (OK)** pour enregistrer votre profil antispyware, qu'il soit nouveau ou modifié.

**STEP 9 |** (Facultatif) Vérifiez la connectivité de votre pare-feu avec le service de sécurité DNS. Si vous ne pouvez pas accéder au service, vérifiez que le domaine suivant n'est pas bloqué : dns.service.paloaltonetworks.com.

Utilisez la commande CLI suivante sur le pare-feu pour vérifier la disponibilité de la connexion de votre pare-feu au service de sécurité du DNS.

```
show dns-proxy dns-signature info
```

Par exemple :

```
show dns-proxy dns-signture info

Cloud URL: dns.service.paloaltonetworks.com:443

Telemetry URL: io.dns.service.paloaltonetworks.com:443

Last Result: None

Last Server Address:

Parameter Exchange: Interval 300 sec

Allow List Refresh: Interval 43200 sec

Request Waiting Transmission: 0

Request Pending Response: 0

Cache Size: 0
```

**STEP 10 |** (Facultatif) Récupérez les détails des transactions d'un domaine spécifique, tels que la latence, le TTL et la catégorie de signature.

Pour revoir les détails de la liste, servez-vous de la commande CLI suivante sur le pare-feu :

```
test dns-proxy dns-signature fqdn
```

Par exemple :

```
test dns-proxy dns-signature fqdn www.yahoo.com

DNS Signature Query [ www.yahoo.com ]

Completed in 178 ms

DNS Signature Response

Entries: 2

Domain                                  Category        GTID
     TTL
-------------------------------------------------------------------------------
*.yahoo.com                             Benign          0
     86400
  www.yahoo.com                         Benign          0
     3600
```

**STEP 11 |** (Facultatif) Configurez le paramètre d'expiration de la recherche de signature DNS. Si le pare-feu n'arrive pas à extraire un verdict de signature dans le temps alloué dû à des problèmes de connectivité, la requête et toutes les réponses DNS suivantes sont autorisées. Vous pouvez vérifier la latence moyenne pour vérifier que les requêtes se situent dans l'intervalle de période configurée Si la latence moyenne excède la période configurée, considérez à mettre à jour la valeur avec une valeur plus haute que la latence moyenne afin de prévenir les expirations de requêtes

1. Avec la CLI, tapez la commande suivante pour voir la latence moyenne

   ```
   show dns-proxy dns-signature
   counters
   ```

   Le délai d'expiration par défaut est 100 secondes.
2. Faites défiler vers le bas vers la section de la latence sous l'en-tête API de la requête et vérifiez que la latence moyenne se situe dans l'intervalle d'expiration défini Cette latence indique le temps qu'il faut, en moyenne, pour récupérer un verdict de signatures du service de sécurité DNS Des statistiques de latence additionnelles pour différentes périodes de latence peuvent être trouvées sous les moyennes

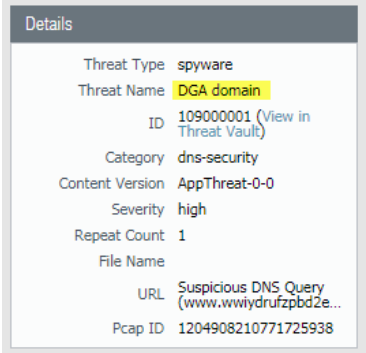
   ```
   Signature query API:
     .
     .
     .
   ```

```
      [latency   ] :
         max    1870 (ms)  min    16(ms)  avg    27(ms)
           50 or less : 47246
           100 or less : 113
           200 or less : 25
           400 or less : 15
                  else : 21
```

3. Si la latence moyenne est constamment au dessus de la valeur par défaut d'expiration, vous pouvez augmenter cette valeur afin que les requêtes se situent dans un intervalle donné Sélectionnez **Device (Périphérique) > Content-ID (ID de contenu)** et mettez à jour le paramètres **Realtime Signature Lookup (Recherche de signature en temps réel)**.
4. Commit (Validez) les modifications.

Pour afficher les requêtes DNS mises en entonnoir, reportez-vous aux journaux des menaces du pare-feu (**Monitor (Moniteur) > Logs (Journaux)**, puis sélectionnez le type de journal dans la liste) :




# Collecte et journalisation des données de sécurité DNS

Le service de DNS Security service (sécurité DNS) collecte les réponses du serveur et les informations de demande en fonction des règles de votre politique de sécurité de pare-feu, de l'action associée et des détails de la requête DNS lors de l'exécution des recherches de domaine. Le pare-feu transmet des données DNS supplémentaires aux serveurs cloud DNS Security et est utilisé par les services de Palo Alto Networks pour fournir des informations de domaine plus précises (telles que l'ASN du fournisseur, les informations d'hébergement et l'identification de géolocalisation). Bien que ces données supplémentaires ne soient pas nécessaires pour faire fonctionner le service de sécurité DNS, elles fournissent les ressources nécessaires pour générer des capacités d'analyse, de détection DNS et de prévention améliorées. Cette action se produit en moins de 30 secondes après la collecte et le traitement par lots n'affecte pas les performances du pare-feu. Dans les cas où le pare-feu subit une charge élevée, la collecte de données DNS est réduite au besoin pour maintenir les niveaux de performances attendus.

Le pare-feu peut soumettre les champs de données suivants :

| Champ | Description |
|---|---|
| Action | Affiche l'action de stratégie prise sur la requête DNS. |
| Type | Affiche le type d'enregistrement DNS. |

| Champ | Description |
|---|---|
| Réponse | L'adresse IP à laquelle le domaine dans la requête DNS a été résolu. |
| Code de réponse | Le code de réponse DNS qui a été reçu en réponse à votre requête DNS. |
| IP source | L'adresse IP du système qui a effectué la requête DNS. |
| Utilisateur source | Lorsque la fonction d'ID utilisateur du pare-feu est activée, l'identité du demandeur DNS est affichée. |
| Zone source | La zone source configurée référencée dans votre règle de politique de sécurité. |

*La collecte de données étendue DNS est contournée pour les domaines ajoutés à la liste verte dans les exceptions DNS.*

Les champs de données qui peuvent être utilisés pour identifier potentiellement les utilisateurs (IP source, utilisateur source et zone source) peuvent être exclus de la soumission automatique à l'aide de la commande CLI suivante : **`set deviceconfig setting ctd cloud-dns-privacy-mask yes`**. Vous devez **`commit (valider)`** les modifications pour que la mise à jour prenne effet.

# Utilisation de requêtes DNS pour identifier des hôtes infectés sur le réseau

L'action de mise en entonnoir DNS des profils Antispyware permet au pare-feu de falsifier une réponse à une requête DNS d'un domaine malveillant connu, ou un domaine personnalisé pour que vous puissiez identifier les hôtes sur votre réseau qui ont été infectés par le logiciel malveillant. Un hôte compromis peut initier la communication avec un serveur de commande et contrôle (C2). Une fois la connexion établie, un pirate peut contrôler à distance l'hôte infecté afin d'infiltrer davantage le réseau ou d'exfiltrer les données.

Les requêtes DNS vers n'importe quel domaine inclus dans la liste de signatures DNS de Palo Alto Networks sont mises en entonnoir vers une adresse IP de serveur Palo Alto Networks.

Le pare-feu possède deux sources de signatures DNS qu'il peut utiliser pour identifier les domaines malveillants et C2 :

- (Exige la prévention contre les menaces) Signatures DNS locales : Il s'agit d'un ensemble restreint de signatures DNS que le pare-feu peut utiliser pour identifier les domaines malveillants. Le pare-feu obtient de nouvelles signatures DNS dans le cadre des mises à jour antivirus quotidiennes.
- (Exige la sécurité DNS) Les signatures de Sécurité DNS : le pare-feu accède au service Cloud DNS de Palo Alto Networks pour vérifier les domaines malveillants en les comparant à la base de données complète des signatures DNS. Certaines signatures (que seule la sécurité DNS fournit) peuvent uniquement détecter les attaques C2 qui utilisent les techniques d'apprentissage machine, comme les Domain Generation Algorithms (algorithmes de génération de domaines ; DGA) et la tunnellisation DNS.

Les requêtes DNS aux domaines dans l'ensemble de signatures DNS local ou l'ensemble de signatures de sécurité DNS sont redirigées vers un serveur Palo Alto Networks, et l'hôte est incapable d'accéder au domaine malveillant. Les rubriques suivantes fournissent des détails sur l'activation de la mise en entonnoir DNS pour que vous puissiez identifier les hôtes infectés.

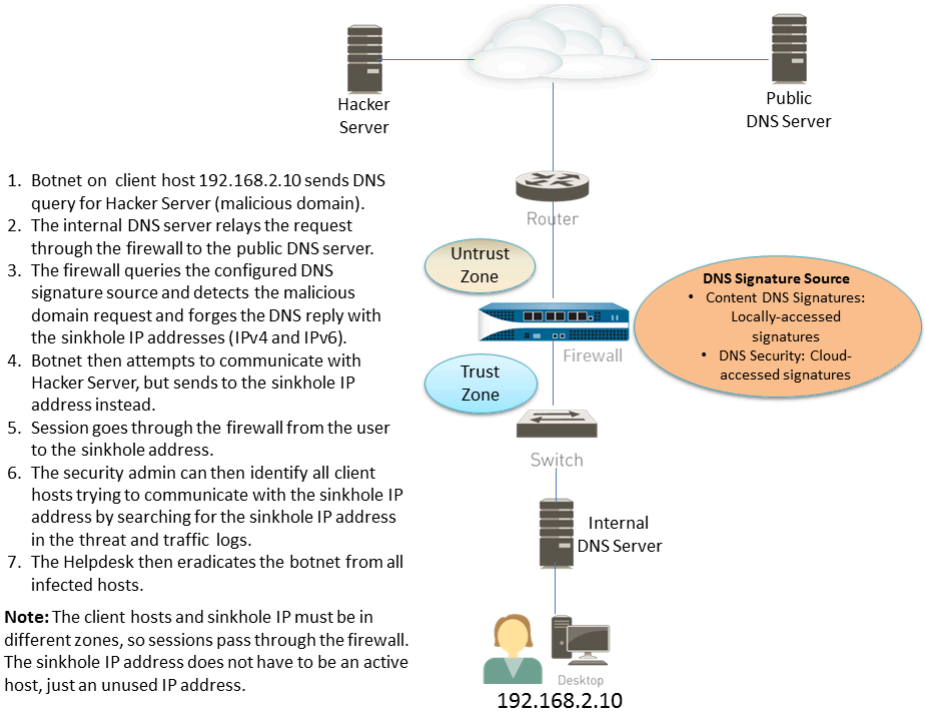
- Apprenez à Fonctionnement de la mise en entonnoir DNS.
- Configuration de la mise en entonnoir DNS.
- Configuration de la mise en entonnoir DNS pour une liste de domaines personnalisés.
- Activation de la sécurité DNS pour mettre en entonnoir les domaines C2.
- Configuration de l'adresse IP entonnoir vers un serveur local sur votre réseau.
- Voir les hôtes infectés qui ont tenté de se connecter à un domaine malveillant.

## Fonctionnement de la mise en entonnoir DNS

La mise en entonnoir DNS vous permet d'identifier les hôtes infectés sur le réseau protégé utilisant le trafic DNS dans les cas où le pare-feu ne peut pas voir la requête DNS du client infecté (c'est-à-dire que le pare-feu ne peut pas voir l'auteur de la requête DNS). Dans un déploiement type où le pare-feu est au nord du serveur DNS local, le journal des menaces identifie le résolveur DNS local comme la source du trafic plutôt que l'hôte réellement infecté. La mise en entonnoir des requêtes DNS malveillantes résout ce problème de visibilité en falsifiant les réponses aux requêtes d'un hôte client adressées à des domaines malveillants, ainsi les clients tentant de se connecter à des domaines malveillants (pour la commande et le contrôle, par exemple) essaieront plutôt de se

connecter à une adresse IP d'entonnoir par défaut de Palo Alto Networks (ou à une adresse IP que vous définissez si vous choisissez de procéder à la Configuration de la mise en entonnoir DNS pour une liste de domaines personnalisée). Les hôtes infectés peuvent alors être facilement identifiés dans les journaux du trafic.




# Configuration de la mise en entonnoir DNS

Pour activer la mise en entonnoir DNS, associez le profil anti-spyware par défaut à une règle de politique de sécurité (reportez-vous à la section Paramétrage d'un antivirus, d'un antispyware et de la protection contre les vulnérabilités). Les requêtes DNS envoyées à tout domaine compris dans la source de signatures DNS de Palo Alto Networks que vous avez spécifié sont résolues en adresse IP entonnoir Palo Alto Networks. À l'heure actuelle, les adresses IP sont les suivantes : sinkhole.paloaltonetworks.com pour IPv4 et ::1 pour l'adresse IPv6 en boucle. Ces adresse peuvent changer et peuvent être modifiées dans les mises à jour de contenu.

**STEP 1 |** Activez la mise en entonnoir DNS pour la liste de domaines personnalisée d'une liste dynamique externe.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware (Antispyware)**.
2. Modifiez un profil existant ou sélectionnez un des profils par défaut et clonez-le.
3. Donnez un **Name (Nom)** au profil, puis sélectionnez l'onglet **DNS Policies (Politiques de DNS)**.
4. Vérifiez que **default-paloalto-dns** est présent dans la **Signature Source (Source de signature)**.
5. (Facultatif) Dans la liste déroulante **Packet Capture (Capture de paquets)**, sélectionnez **single-packet (un seul paquet)** pour capturer le premier paquet de la session ou **extended-**

**capture (capture étendue)** pour définir de 1 à 50 paquets. Vous pouvez ensuite utiliser les captures de paquets pour une analyse plus approfondie.

**STEP 2 |** Vérifiez les paramètres de mise en entonnoir sur le profil antispyware.

1. Sur l'onglet **DNS Policies (Politiques de DNS)**, vérifiez que **Policy Action** on DNS Queries (Action de politique pour les requêtes DNS) est définie sur **sinkhole (entonnoir)**.
2. À la section DNS Sinkhole Settings (Paramètres de mise en entonnoir DNS), vérifiez que l'option **Sinkhole (Entonnoir)** est activée. Pour votre facilité, l'adresse IP entonnoir par défaut est définie sur un serveur de Palo Alto Networks. Palo Alto Networks peut automatiquement actualiser cette adresse IP par l'intermédiaire de mises à jour de contenu.

   Si vous souhaitez modifier l'adresse **Sinkhole IPv4 (IPv4 d'entonnoir)** ou **Sinkhole IPv6 (IPv6 d'entonnoir)** vers un serveur local sur votre réseau ou vers une adresse de boucle, reportez-vous à la section Configuration de l'adresse IP entonnoir vers un serveur local sur votre réseau.
3. Cliquez sur **OK (OK)** pour enregistrer le profil antispyware.

**STEP 3 |** Associez le profil antispyware à une règle de politique de sécurité.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis sélectionnez une règle de politique de sécurité.
2. Dans l'onglet **Actions (Actions)**, cochez la case **Log at Session Start (Journalisation en début de session)** pour activer la journalisation.
3. Dans la section Paramètre de profil, cliquez sur la liste déroulante **Profile Type (Type de profil)** pour voir tous les **Profiles (Profils)**. Sélectionnez le nouveau profil dans la liste déroulante **Anti-spyware (Antispyware)**.
4. Cliquez sur **OK (OK)** pour enregistrer la règle de politique.

**STEP 4 |** Testez que l'action de la politique est appliquée en surveillant l'activité sur le pare-feu.

1. Sélectionnez **ACC (ACC)** et ajoutez un domaine d'URL en tant que filtre général pour afficher l'activité des menaces et l'activité bloquée pour le domaine auquel vous avez accédé.
2. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menace)** et filtrez par `(action eq sinkhole)` pour afficher les journaux des domaines mis en entonnoir.

## Configuration de la mise en entonnoir DNS pour une liste de domaines personnalisée

Pour activer la mise en entonnoir DNS pour une liste de domaines personnalisée, vous devez créer une liste dynamique externe qui englobe les domaines, autoriser l'action de mise en entonnoir dans un profil antispyware et associer le profil à une règle de politique de sécurité. Lorsqu'un client tente d'accéder à un domaine malveillant qui figure dans cette liste, le pare-feu remplace l'adresse IP de destination du paquet par l'adresse IP du serveur Palo Alto Networks définie par défaut pour la mise en entonnoir ou par celle définie par un utilisateur.

Pour chaque nom de domaine personnalisé qui est inclus dans la liste dynamique externe, le pare-feu génère des signatures de logiciel espion basées sur DNS. La signature se nomme Requête DNS

malveillante personnalisée <nom de domaine> et correspond à un type de spyware de niveau de gravité moyen ; chaque signature est un hachage 24 octets du nom de domaine.

Chaque modèle de pare-feu prend en charge un maximum de 50 000 noms de domaines totaux dans au moins une liste dynamique externe, mais aucune limite maximale n'est appliquée à une liste.

**STEP 1 |** Activez la mise en entonnoir DNS pour la liste de domaines personnalisée d'une liste dynamique externe.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware (Antispyware)**.
2. Modifiez un profil existant ou sélectionnez un des profils par défaut et clonez-le.
3. Donnez un **Name (Nom)** au profil, puis sélectionnez l'onglet **DNS Policies (Politiques de DNS)**.
4. Sélectionnez un EDL à partir de la source de signature **External Dynamic Lists (Listes dynamiques externes)**.

   *Si vous avez déjà créé une liste dynamique externe de type : **Domain List (Liste de domaines)**, vous pouvez la sélectionnez ici. Les listes dynamiques externes de type URL ou Adresse IP que vous pourriez avoir créées ne figurent pas dans la liste.*
5. Configurez la liste dynamique externe à partir du profile antispyware (reportez-vous à la section Configuration du pare-feu pour qu'il accède à une liste dynamique externe). Le **Type (Type)** est prédéfini sur **Domain List (Liste de domaines)**.
6. (Facultatif) Dans la liste déroulante **Packet Capture (Capture de paquets)**, sélectionnez **single-packet (un seul paquet)** pour capturer le premier paquet de la session ou **extended-capture (capture étendue)** pour définir de 1 à 50 paquets. Vous pouvez ensuite utiliser les captures de paquets pour une analyse plus approfondie.

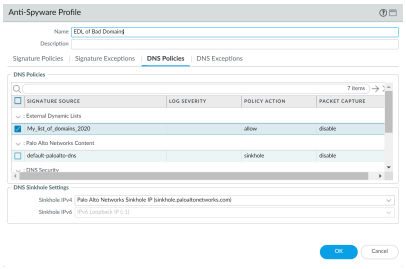
**STEP 2 |** Vérifiez les paramètres de mise en entonnoir sur le profil antispyware.

1. Sur l'onglet **DNS Policies (Politiques de DNS)**, vérifiez que **Policy Action** on DNS Queries (Action de politique pour les requêtes DNS) est définie sur **sinkhole (entonnoir)**.
2. À la section DNS Sinkhole Settings (Paramètres de mise en entonnoir DNS), vérifiez que l'option **Sinkhole (Entonnoir)** est activée. Pour votre facilité, l'adresse IP entonnoir par défaut est définie sur un serveur de Palo Alto Networks. Palo Alto Networks peut automatiquement actualiser cette adresse IP par l'intermédiaire de mises à jour de contenu.

   Si vous souhaitez modifier l'adresse **Sinkhole IPv4 (IPv4 d'entonnoir)** ou **Sinkhole IPv6 (IPv6 d'entonnoir)** vers un serveur local sur votre réseau ou vers une adresse de boucle,

reportez-vous à la section Configuration de l'adresse IP entonnoir vers un serveur local sur votre réseau.




3. Cliquez sur **OK (OK)** pour enregistrer le profil antispyware.

**STEP 3 |** Associez le profil antispyware à une règle de politique de sécurité.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis sélectionnez une règle de politique de sécurité.
2. Dans l'onglet **Actions (Actions)**, cochez la case **Log at Session Start (Journalisation en début de session)** pour activer la journalisation.
3. Dans la section Paramètre de profil, cliquez sur la liste déroulante **Profile Type (Type de profil)** pour voir tous les **Profiles (Profils)**. Sélectionnez le nouveau profil dans la liste déroulante **Anti-spyware (Antispyware)**.
4. Cliquez sur **OK (OK)** pour enregistrer la règle de politique.

**STEP 4 |** Vérifiez que l'action de politique est appliquée.

1. Afficher les entrées de la liste dynamique externe qui appartiennent à la liste de domaine et accédez à un domaine de la liste.
2. Pour surveiller l'activité sur le pare-feu :
   1. Sélectionnez **ACC (ACC)** et ajoutez un domaine d'URL en tant que filtre général pour afficher l'activité des menaces et l'activité bloquée pour le domaine auquel vous avez accédé.
   2. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menace)** et filtrez par `(action eq sinkhole)` pour afficher les journaux des domaines mis en entonnoir.

**STEP 5 |** Vérifiez si des entrées de la liste dynamique externe sont ignorées ou sautées.

Pour revoir les détails de la liste, servez-vous de la commande CLI suivante sur le pare-feu :

```
request system external-list show type domain name <list_name>
```

Par exemple :

```
request system external-list show type domain name
My_List_of_Domains_2015
vsys1/EBLDomain:
Next update at : Thu May 21 10:15:39 2015
Source : https://1.2.3.4/My_List_of_Domains_2015
Referenced : Yes
Valid : Yes
Number of entries : 3
```

```
domains:www.example.com
baddomain.com
qqq.abcedfg.com
```

**STEP 6 |** (Facultatif) Récupérez la liste dynamique externe à la demande.

Pour forcer le pare-feu à récupérer la liste actualisée à la demande plutôt qu'au prochain intervalle d'actualisation (la fréquence de **Repeat (Répétition)** que vous avez définie pour la liste dynamique externe), servez-vous de la commande CLI suivante :

```
request system external-list refresh type domain name  <list_name>
```

*Vous pouvez également utiliser l'interface du pare-feu pour la* récupération d'une liste dynamique externe du serveur Web*.*

## Configuration de l'adresse IP entonnoir vers un serveur local sur votre réseau

Par défaut, la mise en entonnoir DNS est activée pour toutes les signatures DNS de Palo Alto Networks, et l'adresse IP entonnoir est définie pour permettre l'accès à un serveur de Palo Alto Networks. Servez-vous des directives présentées dans cette section si vous souhaitez définir l'adresse IP entonnoir sur un serveur local de votre réseau.

Vous devez obtenir des adresses IPv4 et IPv6, qui serviront d'adresses IP entonnoir, car un logiciel malveillant peut exécuter des requêtes DNS via un de ces protocoles, ou les deux. L'adresse d'entonnoir DNS doit se trouver dans une zone différente des hôtes clients pour s'assurer, lorsqu'un hôte infecté tente d'ouvrir une session avec l'adresse IP d'entonnoir, qu'il sera acheminé via le pare-feu.

*Les adresses d'entonnoir doivent être réservées à cet effet et ne doivent pas nécessairement être associées à un hôte physique. Vous pouvez éventuellement utiliser un serveur « pot de miel » comme hôte physique pour analyser le trafic malveillant de manière plus approfondie.*

*Les étapes de configuration qui suivent utilisent les exemples d'adresses d'entonnoir DNS suivantes :*

*Adresse d'entonnoir DNS IPv4 : 10.15.0.20*

*Adresse d'entonnoir DNS IPv6 : fd97:3dec:4d27:e37c:5:5:5:5*

**STEP 1 |** Configurez l'interface et la zone de l'entonnoir.

Le trafic provenant de la zone sur laquelle les hôtes clients résident doit être acheminé vers la zone sur laquelle l'adresse IP d'entonnoir est définie. Le trafic sera ainsi consigné.

*Utilisez une zone dédiée pour le trafic d'entonnoir car l'hôte infecté enverra du trafic à cette zone.*

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)**, puis choisissez l'interface que vous souhaitez configurer comme votre interface d'entonnoir.
2. Dans la liste déroulante **Interface Type (Type d'interface)**, sélectionnez **Layer3 (Couche 3)**.
3. Pour ajouter une adresse IPv4, sélectionnez l'onglet **IPv4 (IPv4)**, sélectionnez **Static (Statique)**, puis cliquez sur **Add (Ajouter)**. Dans cet exemple, ajoutez 10.15.0.20 comme adresse d'entonnoir DNS IPv4.
4. Sélectionnez l'onglet **IPv6 (IPv6)**, cliquez sur **Static (Statique)**, puis sur **Add (Ajouter)** et saisissez une adresse IPv6 et un masque de sous-réseau. Dans cet exemple, saisissez fd97:3dec:4d27:e37c::/64 comme adresse d'entonnoir DNS IPv6.
5. Cliquez sur **OK (OK)** pour enregistrer les paramètres.
6. Pour ajouter une zone pour l'entonnoir, sélectionnez **Network (Réseau)** > **Zones (Zones)**, puis cliquez sur **Add (Ajouter)**.
7. Saisissez un **Name (Nom)** de zone.
8. Dans la liste déroulante **Type (Type)**, sélectionnez **Layer3 (Couche 3)**.
9. Dans la section **Interfaces (Interfaces)**, cliquez sur **Add (Ajouter)** et ajoutez l'interface que vous venez de configurer.
10. Cliquez sur **OK**.

**STEP 2 |** Activation de la mise en entonnoir DNS

Par défaut, la mise en entonnoir est activée pour toutes les signatures DNS Palo Alto Networks. Pour définir l'adresse entonnoir sur votre serveur local, reportez-vous à l'étape Vérifier les paramètres de la mise en entonnoir DNS sur le profil antispyware à la section Configuration de la mise en entonnoir DNS pour une liste de domaines personnalisée.

**STEP 3 |** Modifiez la règle de sécurité autorisant le trafic des hôtes clients de la zone approuvée vers la zone non approuvée afin d'inclure la zone d'entonnoir en tant que destination et d'associer le profil antispyware.

La modification de la ou des règles de politique de sécurité qui autorisent le trafic des hôtes clients de la zone approuvée vers la zone non approuvée vous permet de vous assurer que vous identifiez le trafic provenant d'hôtes infectés. L'ajout à la règle de la zone d'entonnoir en tant que destination permet aux clients infectés d'envoyer de fausses requêtes DNS à l'entonnoir DNS.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
2. Sélectionnez une règle existante qui autorise le trafic de la zone de l'hôte client vers la zone non approuvée.
3. Dans l'onglet **Destination (Destination)**, **Add (Ajoutez)** la zone d'entonnoir. Le trafic de l'hôte client peut ainsi être acheminé vers la zone d'entonnoir.
4. Dans l'onglet **Actions (Actions)**, cochez la case **Log at Session Start (Journalisation en début de session)** pour activer la journalisation. Ceci garantit que le trafic provenant

d'hôtes clients de la zone approuvée sera consigné lors de l'accès à la zone non approuvée ou d'entonnoir.

5. Dans la section **Profile Setting (Paramètre de profil)**, sélectionnez le profil **Anti-Spyware (Antispyware)** dans lequel vous avez activé la mise en entonnoir DNS.
6. Cliquez sur **OK (OK)** pour enregistrer la règle de politique de sécurité, puis sur **Commit (Valider)**.

**STEP 4 |** Pour confirmer que vous allez pouvoir identifier les hôtes infectés, vérifiez que le trafic entre l'hôte client de la zone approuvée vers la nouvelle zone d'entonnoir est consigné.

Dans cet exemple, l'hôte client infecté est 192.168.2.10 et l'adresse d'entonnoir IPv4 est 10.15.0.20.

1. Sur un hôte client de la zone approuvée, ouvrez une invite de commande et exécutez la commande suivante :

```
C:\>ping <sinkhole address>
```

L'exemple suivant indique la requête ping sur l'adresse d'entonnoir DNS 10.15.0.2 et le résultat `Request timed out` car l'adresse IP d'entonnoir n'est pas associée à un hôte physique :

```
C:\>ping 10.15.0.20
Pinging 10.15.0.20 with 32 bytes of data:
Request timed out.
Request timed out.
Ping statistics for 10.15.0.20:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

2. Sur le pare-feu, sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)** et recherchez l'entrée de log avec la source 192.168.2.10 et la destination 10.15.0.20. Ceci confirme que le trafic vers l'adresse IP d'entonnoir passe par les zones du pare-feu.

*Vous pouvez rechercher et/ou filtrer les journaux et n'afficher que les journaux avec la destination 10.15.0.20. Pour cela, cliquez sur l'adresse IP (10.15.0.20) dans la colonne **Destination (Destination)**. Le filtre (addr.dst in 10.15.0.20) est ainsi ajouté au champ de recherche. Cliquez sur l'icône Appliquer un filtre à droite du champ de recherche pour appliquer le filtre.*

**STEP 5 |** Testez que la mise en entonnoir DNS est bien configurée.

Vous simulez l'action que poserait un client infecté lorsqu'une application malveillante tente de contacter sa base.

1. Trouvez un domaine malveillant qui figure dans la base de données de signatures antivirus actuelle du pare-feu pour tester la mise en entonnoir.
   1. Sélectionnez **Device (Périphérique)** > **Dynamic (Dynamique) Updates (Mises à jour dynamiques)**, puis, dans la section **Antivirus (Antivirus)**, cliquez sur le lien **Release Notes (Notes de publication)** de la base de données antivirus installée. Vous pouvez également trouver les notes de version antivirus qui indiquent les mises à jour

incrémentielles des signatures, à la section Mises à jour dynamiques du site de support Palo Alto Networks.

2. Dans la deuxième colonne de la note de version, recherchez un élément de ligne avec une extension de domaine (par exemple, .com, .edu ou .net). La colonne de gauche indique le nom du domaine. Par exemple, dans la version Antivirus 1117-1560, un élément dans la colonne de gauche est nommé « tbsbana » et la colonne de droite indique « net ».

   La chaîne suivante correspond au contenu de cet élément de ligne dans la note de version :

   ```
   conficker:tbsbana 1
   variants: net
   ```

2. Sur l'hôte client, ouvrez une invite de commande.
3. Exécutez une commande NSLOOKUP sur une URL que vous avez identifiée comme un domaine malveillant.

   Par exemple, avec l'URL `track.bidtrk.com` :

   ```
   C:\>nslookup
    track.bidtrk.com
    Server: my-local-dns.local
    Address: 10.0.0.222
    Non-authoritative answer:
    Name: track.bidtrk.com.org
    Addresses: fd97:3dec:4d27:e37c:5:5:5:510.15.0.20
   ```

   Notez, dans le résultat, que la commande NSLOOKUP sur le domaine malveillant a été falsifiée à l'aide des adresses IP d'entonnoir que nous avons configurées (10.15.0.20). Le domaine correspondant à une signature DNS malveillante, l'action d'entonnoir a été exécutée.
4. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menace)** et recherchez l'entrée du journal des menaces correspondante pour vérifier que l'action appropriée a été exécutée sur la requête NSLOOKUP.
5. Exécutez une commande ping sur **`track.bidtrk.com`**, ce qui générera du trafic réseau vers l'adresse d'entonnoir.

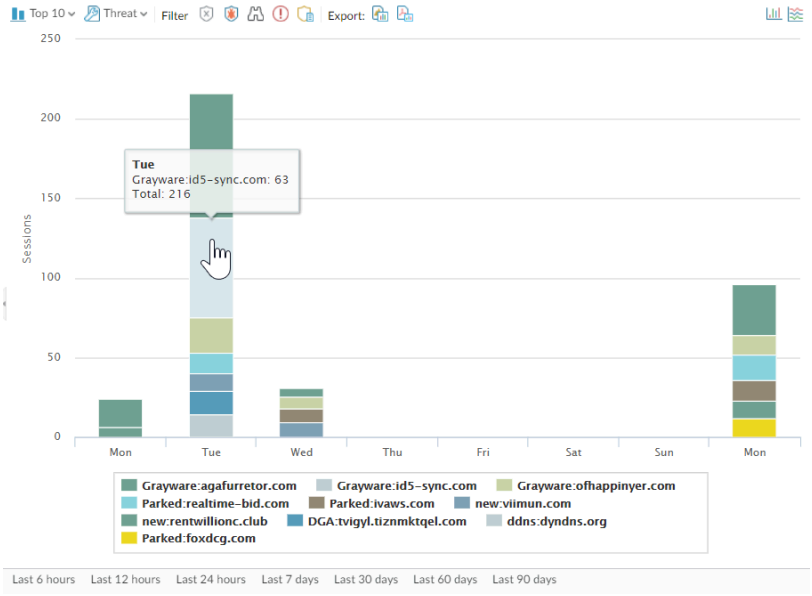
## Voir les hôtes infectés qui ont tenté de se connecter à un domaine malveillant

Après avoir configuré la mise en entonnoir DNS et vérifié que le trafic vers un domaine malveillant est transmis à l'adresse d'entonnoir, vous devez surveiller régulièrement le trafic vers l'adresse d'entonnoir afin de pouvoir suivre les hôtes infectés et de supprimer les menaces.

- Utilisez App Scope pour identifier les hôtes clients infectés.
  1. Sélectionnez **Monitor (Surveillance)** > **App Scope (App Scope)**, puis **Threat Monitor (Surveillance des menaces)**.
  2. Cliquez sur le bouton **Show spyware (Afficher les logiciels espions)** en haut de la page affichée.
  3. Sélectionnez une plage horaire.

     La capture d'écran ci-dessous illustre trois instances de requêtes DNS suspectes qui ont été générées alors que l'hôte client de test exécutait une commande NSLOOKUP sur un domaine malveillant connu. Cliquez sur le graphique pour plus de détails sur l'événement.




- Configurez un rapport personnalisé afin d'identifier tous les hôtes clients qui ont envoyé du trafic à l'adresse IP d'entonnoir, 10.15.0.20 dans cet exemple.

  ***Transférez-le à un gestionnaire SNMP, un serveur Syslog et/ou à Panorama pour activer des alertes sur ces événements.***

  Dans cet exemple, l'hôte client infecté exécutait une commande NSLOOKUP sur un domaine malveillant connu et répertorié dans la base de données de signatures DNS Palo Alto Networks. La requête a été envoyée au serveur DNS local, qui l'a ensuite transféré via le pare-feu à un serveur DNS externe. La politique de sécurité du pare-feu et le profil antispyware configuré ont comparé la requête avec la base de données de signatures DNS, puis falsifié la réponse avec l'adresse d'entonnoir 10.15.0.20 et fd97:3dec:4d27:e37c:5:5:5:5. Le client tente d'ouvrir une session et le journal du trafic enregistre l'activité avec l'hôte source et l'adresse de destination, qui est désormais redirigée vers l'adresse d'entonnoir falsifiée.

  Consultez le journal du trafic sur le pare-feu pour identifier tout hôte client qui envoie du trafic vers l'adresse d'entonnoir. Dans cet exemple, les journaux indiquent que l'adresse source 192.168.2.10 a envoyé la requête DNS malveillante. L'hôte peut alors être retrouvé et nettoyé. Sans l'option d'entonnoir DNS, l'administrateur ne verrait le serveur DNS local que comme le système à l'origine de la requête et ne verrait pas l'hôte client infecté. Si vous avez généré un

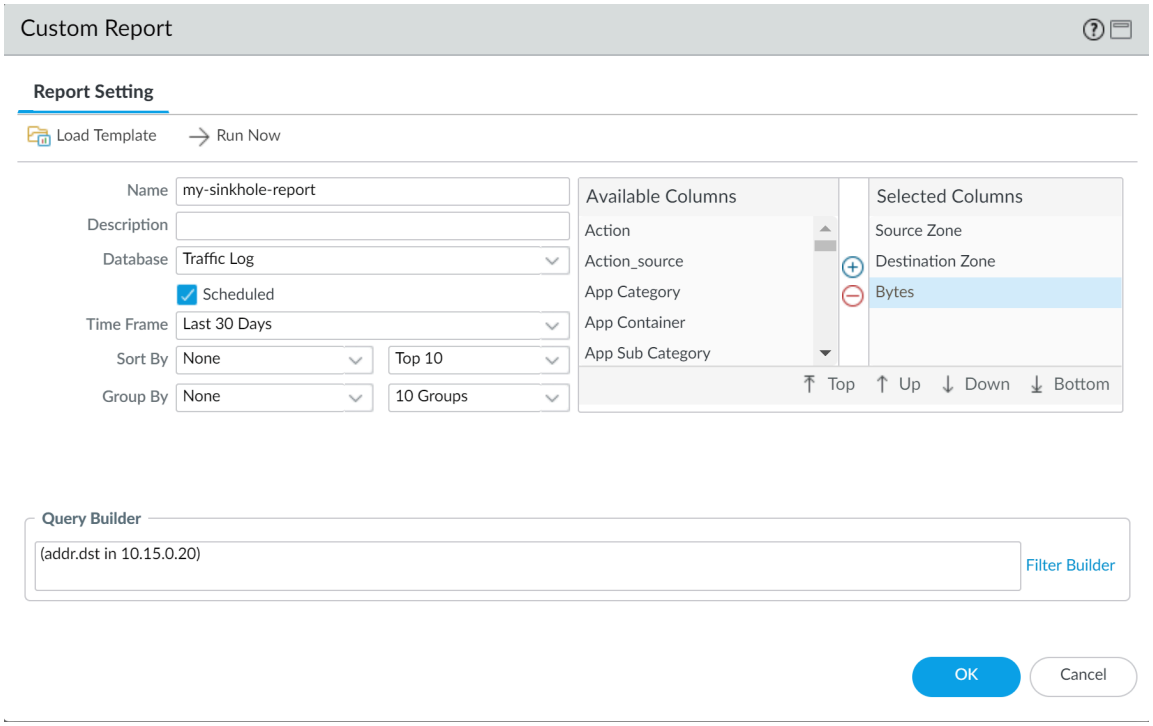
 

rapport sur le journal des menaces à l'aide de l'action Entonnoir, le journal indique le serveur DNS local, et non l'hôte infecté.

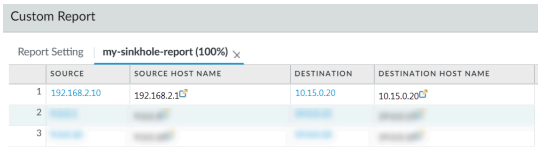
1. Sélectionnez **Monitor (Surveillance)** > **Manage Custom Reports (Gérer les rapports personnalisés)**.
2. Cliquez sur **Add (Ajouter)** et donnez un **Name (Nom)** au rapport.
3. Définissez un rapport personnalisé qui capture le trafic vers l'adresse d'entonnoir comme suit :
   - **Database (Base de données)** : sélectionnez **Traffic Log (Journal du trafic)**.
   - **Scheduled (Planifié)** : activez **Scheduled (Planifié)** pour que le rapport soit généré chaque nuit.
   - **Time Frame (Intervalle de temps)** : 30 jours.
   - **Selected Columns (Colonnes sélectionnées)** : sélectionnez **Source address (Adresse source)** ou **Source User (Utilisateur source)** (si vous avez configuré un User-ID), qui identifiera l'hôte client infecté dans le rapport, et **Destination address (Adresse de destination)**, qui correspondra à l'adresse d'entonnoir.
   - Dans la section au bas de l'écran, créez une requête personnalisée pour le trafic vers l'adresse d'entonnoir (10.15.0.20 dans cet exemple). Vous pouvez saisir l'adresse de destination dans la fenêtre **Query Builder (Générateur de requêtes)** (**addr.dst in 10.15.0.20**) ou sélectionner les valeurs suivantes dans chaque colonne et cliquer sur

**Add (Ajouter)** : Connecteur = and, Attribut = Destination Address, Opérateur = in, et Valeur = 10.15.0.20. Cliquez sur **Add (Ajouter)** pour ajouter la requête.




4. Cliquez sur **Run Now (Exécuter maintenant)** pour générer le rapport. Le rapport indiquera tous les hôtes clients qui ont envoyé du trafic à l'adresse d'entonnoir, indiquant ainsi les plus susceptibles d'être infectés. Vous pouvez alors suivre les hôtes et les analyser à la recherche de logiciels espions.




5. Pour afficher les rapports planifiés exécutés, sélectionnez **Monitor (Surveillance)** > **Reports (Rapports)**.

# Filtrage des données

Utilisez les Profils de Filtrage de Données pour empêcher vos données propriétaires, confidentielles et sensibles de quitter votre réseau. Les modèles prédéfinis, les paramètres intégrés et les options personnalisables vous permettent de protéger facilement les fichiers qui contiennent certaines propriétés de fichier (comme un titre de document ou un auteur), les numéros de carte de crédit, les informations réglementées de différents pays (comme les numéros de sécurité sociale) et les étiquettes de data loss prevention (prévention des pertes de données ; DLP).

- **Modèles de données prédéfinis** : filtrez en toute facilité les modèles courants, y compris les numéros de cartes de crédit. Les modèles prédéfinis de filtrage des données identifient également des informations spécifiques (réglementées) dans différents pays du monde, comme les numéros de sécurité sociale (États-Unis), les numéros d'identification de l'INSEE (France) et les numéros d'identification du Département du revenu interne de la Nouvelle-Zélande. Bon nombre des modèles de filtrage des données prédéfinis assurent le respect des normes comme la HIPPA, le GDPR et la loi Gramm-Leach-Bliley.
- **Support intégré pour Azure Information Protection et Titus Data Classification** : les propriétés de fichiers prédéfinies vous permettent de filtrer le contenu en fonction des étiquettes de Azure Information Protection et de Titus. Les étiquettes d'Azure Information Protection sont stockées dans les métadonnées, assurez-vous donc de connaître le GUID de l'étiquette Azure Information Protecton que vous voulez que le pare-feu filtre.
- **Modèles de données personnalisés pour les solutions de prévention des pertes de données** : si vous utilisez une solution DLPde point de terminaison tierce qui renseigne les propriétés des fichiers afin d'indiquer la sensibilité du contenu, vous pouvez créer un modèle de données personnalisé pour identifier les propriétés des fichiers et les valeurs étiquetées par votre solution DLP, puis journaliser ou bloquer les fichiers que votre profil de filtrage des données détecte à l'aide de ce modèle.

## Création d'un profil de filtrage des données

Les profils de filtrage des données peuvent empêcher les informations de nature délicate de sortir de votre réseau.

Pour commencer, vous créez un modèle de données qui spécifie les types d'information et les champs que vous souhaitez que le pare-feu filtre. Puis, vous associez ce modèle à un profil de filtrage des données, qui spécifie la manière dont vous souhaitez appliquer le contenu que le pare-feu filtre. Ajoutez le profil de filtrage des données à une règle de politique de sécurité pour commencer à filtrer le trafic qui correspond à la règle.

**STEP 1 |** Définissez un nouveau modèle de données de l'objet pour détecter les données que vous voulez filtrer.

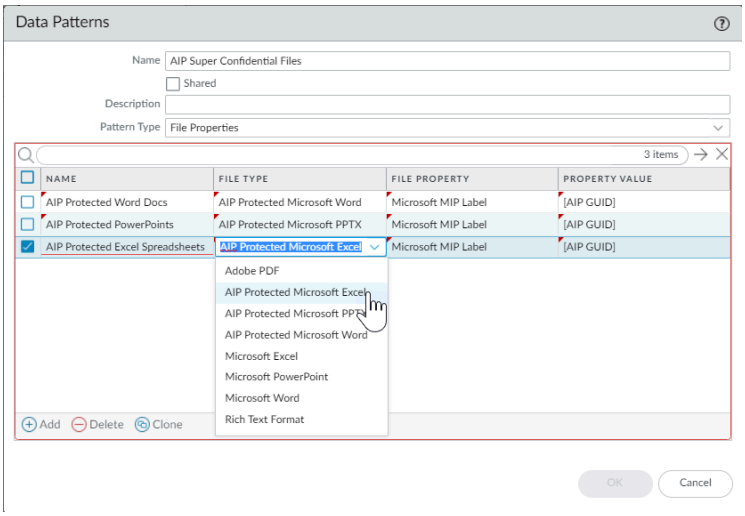
1. Sélectionnez **Objects (Objets)** > **Custom Objects (Objets personnalisés)** > **Data Patterns (Modèles de données)** et **Add (Ajoutez)** un nouvel objet.
2. Donnez un **Name (Nom)** descriptif au nouvel objet.
3. (Facultatif) Sélectionnez **Shared (Partagé)** si vous souhaitez que le modèle de données soit disponible pour :
   - **Tous les systèmes virtuels (vsys) sur un pare-feu comportant plusieurs vsys** - S'il est effacé (désactivé), le modèle de données est disponible uniquement pour le système virtuel sélectionné dans l'onglet **Objects (Objets)**.
   - **Tous les groupes de périphériques sur Panorama** - S'il est effacé (désactivé), le modèle de données est disponible uniquement pour le groupe de périphériques sélectionné dans l'onglet **Objects (Objets)**.
4. (Facultatif - Uniquement Panorama) Sélectionnez **Disable override (Désactiver le contrôle prioritaire)** pour empêcher les administrateurs de remplacer les paramètres du modèle de données de l'objet pour les groupes de périphériques qui héritent de l'objet. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l'objet.
5. (Facultatif - Uniquement Panorama) Sélectionnez **Data Capture (Capture de donnée)** pour collecter automatiquement les données bloquées par le filtre.

   ***Indiquez un mot de passe pour l'option Gérer la protection des données à la page Paramètres pour afficher vos données capturées (Device (Périphérique) > Setup (Configuration) > Content-ID > Manage Data Protection (Gestion de la protection des données)).***
6. Définissez le **Pattern Type (Type de Modèle)** sur l'une des options suivantes :
   - **Predefined Pattern (Modèle prédéfini)** : filtrez la carte de crédit, les numéros de sécurité sociale et les informations d'identification personnelle pour plusieurs normes de conformité, y compris l'HIPAA, GDPR, la Gramm-Leach-Bliley Act.
   - **Regular Expression (Expressions courantes)** – Filtre pour des modèles de données personnalisées.
   - **File Properties (Propriétés des fichiers)** – Filtre basé sur les propriétés des fichiers et les valeurs associées.
7. **Add (Ajoutez)** une nouvelle règle au modèle de données de l'objet.
8. Définissez le modèle de données selon le **Pattern Type (Type de modèle)** que vous avez sélectionné pour cet objet :
   - **Prédéfini** — Sélectionnez le **Name (Nom)** et choisissez le modèle de données prédéfini sur lequel effectuer le filtrage.
   - **Expression Courante** – Définissez un **Name (Nom)** descriptif, sélectionnez le **File Type (Type de Fichier)** (ou les types) que vous voulez balayer, et saisissez ensuite le **Data Pattern (Modèle de données)** spécifique qui doit être détecté par votre pare-feu.
   - **File Properties (Propriétés des Fichiers)**– Définissez un **Name (Nom)** descriptif, sélectionnez le **File Type (Type de Fichier)** et la **File Property (Propriété du fichier)**

que vous voulez balayer, et saisissez ensuite le **Property Value (Valeur de la Propriété)** spécifique qui doit être détectée par votre pare-feu.

- **Pour filtrer les documents classés Titus** : Sélectionnez l'un des types de fichiers qui ne sont pas protégés par AIP et définissez la **File Property (Propriété du fichier)** sur TITUS GUID. Saisissez le GUID de l'étiquette Titus en tant que **Property Value (Valeur de la propriété)**.
- **Pour les documents ayant une étiquette Azure Information Protection** : Sélectionnez n'importe quel **File Type (Type de fichier)**, sauf le format RTF. Pour le type de fichier que vous choisissez, définissez les **File Property (Propriétés du fichier)** sur Microsoft MIP Label (Étiquette MIP de Microsoft) et saisissez le GUID de l'étiquette Azure Information Protection en tant que **Property Value (Valeur de propriétés)**.




9. Cliquez sur **OK** pour enregistrer le modèle de données.

**STEP 2 |** Ajoutez le modèle de données de l'objet à un profil de filtrage de données.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de Sécurité)** > **Data Filtering (Filtrage des données)** et **Add (Ajouter)** ou modifiez un profil de filtrage de données.
2. Donnez un **Name (Nom)** descriptif au nouveau profil.
3. **Add (Ajoutez)** une nouvelle règle de profil et sélectionnez le modèle de données que vous avez créé à l'étape .
4. Définissez **Applications**, **File Types (Type de Fichiers)**, et la **Direction** du trafic (en amont ou en aval) que vous voulez filtrer basé sur le modèle de données.

   *Le type de fichier que vous sélectionnez doit être le même type de fichier que celui que vous avez défini préalablement pour le modèle de données ou il doit d'agir d'un type de fichier qui inclut le type de fichier du modèle de données. Par exemple, vous pouvez définir aussi bien le modèle de données de l'objet que le profil de filtrage de données pour balayer tous les documents Microsoft Office. Vous pouvez également définir le modèle de données de l'objet à faire correspondre uniquement aux présentations Microsoft Powerpoint tandis que le profil de filtrage de données balaye tous les documents Microsoft Office.*

   Si un modèle de données de l'objet est associé à un profil de filtrage de données et si les types de fichiers configurés ne s'ajustent pas entre les deux, le profil ne filtrera pas correctement les documents correspondants au modèle de données de l'objet.
5. Réglez le **Alert Threshold (Seuil d'Alerte)** pour préciser le nombre de fois que le modèle de données doit être détecté dans un fichier pour déclencher une alerte.
6. Réglez le **Block Threshold (Seuil de Blocage)** pour bloquer les fichiers qui contiennent de nombreux exemples du modèle de données.
7. Réglez la **Log Severity (Gravité des Journaux)** enregistrée pour des fichiers correspondant à cette règle.
8. Cliquez sur **OK** pour enregistrer le profil de filtrage des données.

**STEP 3 |** Appliquez les réglages de filtrage des données au trafic.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et **Add (ajoutez)** ou modifiez une règle de politique de sécurité.
2. Sélectionnez **Actions** et définissez le Profile Type (Type de profil) sur **Profiles (Profils)**.
3. Associez le profil de filtrage des données que vous avez créé à l'étape 2 à la règle de politique de sécurité.
4. Cliquez sur **OK**.

**STEP 4 |** (Recommandé) Empêchez les navigateurs web de reprendre une session interrompue par le pare-feu.

*Cette option garantit que, lorsque le pare-feu détecte puis abandonne un fichier sensible, un navigateur web ne peut ni restaurer la session ni récupérer le fichier.*

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Content-ID (Content-ID)** et modifiez les paramètres de Content-ID.
2. Décochez la case **Allow HTTP partial response (Autoriser la réponse partielle HTTP)**.
3. Cliquez sur **OK**.

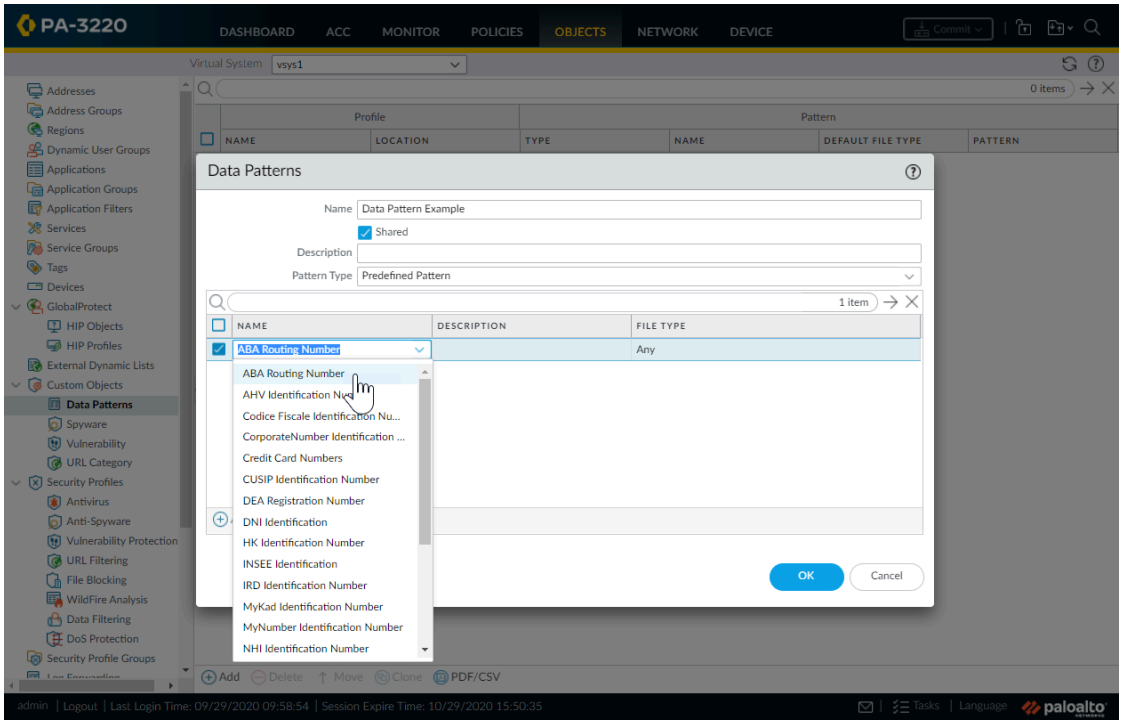
**STEP 5 |** Surveillez les fichiers que le pare-feu filtre.

Sélectionnez **Monitor (Surveillance)** > **Data Filtering (Filtrage des données)** pour voir les fichiers que le pare-feu a détectés et bloqués, basé sur vos réglages de filtrage des données.

## Modèles prédéfinis de filtrage des données

Pour respecter des normes comme la HIPAA, le GDPR et la loi Gramm-Leach-Bliley, le pare-feu fournit des modèles de données prédéfinis. Vous pouvez utiliser ces modèles pour empêcher que les types les plus courants d'informations de nature délicate, comme les numéros de sécurité sociale et de carte de crédit, ne quittent votre réseau.

Vous pouvez trouver les modèles de données prédéfinis en sélectionnant **Objects (Objets) > Custom Objects (Objets personnalisés) > Data Patterns (Modèles de données)** et en cliquant sur **Add (Ajouter)** un nouvel objet. Puis, définissez le **Pattern Type (Type de modèle)** sur **Predefined Pattern (Modèle prédéfini)** et **Add (Ajoutez)** une nouvelle règle à l'objet de modèle de données. Sélectionnez un modèle de données dans la liste qui figure sous **Name (Nom)**.



***Si le type d'informations que vous voulez protéger n'est pas couvert dans la liste des modèles prédéfinis, vous pouvez utiliser des expressions régulières pour créer des modèles personnalisés.***

Voici une liste des modèles de données disponibles :

| Pattern | Description |
|---|---|
| Numéros de carte de crédit | Numéros de carte de crédit à 16 chiffres |
| Numéros de sécurité sociale | Numéros de sécurité sociale à 9 chiffres et comporter des tirets. |
| Numéros de sécurité sociale (sans tiret) | Numéros de sécurité sociale à 9 chiffres sans tiret |
| Numéro d'acheminement d'ABA | Numéro d'acheminement de l'American Banking Association |
| Numéro d'identification AHV | Alters und Hinterlassenenversicherungsnummer suisse |
| Numéro Codice Fiscale Identification | Numéro d'identification du code fiscal italien |
| Numéro d'identification d'entreprise | Numéro d'entreprise de l'agence nationale d'administration fiscale du Japon |
| Numéro d'identification CUSIP | Numéro d'identification du Committee on Uniform Security Identification Procedures |
| Numéro d'enregistrement de la DEA | É.-U. Numéro d'enregistrement de la U.S. Drug Enforcement Administration |
| Numéro d'identification DNI | Numéro d'identification du Documento nacional de identidad d'Espagne |
| Numéro d'identification HK | Numéro d'identification des résidents de Hong Kong |
| Numéro d'identification de l'INSEE | Numéro d'identification de l'Institut national de la statistique et des études économiques de France |
| Numéro d'identification de l'IRD | Numéro d'identification de l'Internal Revenue Department de Nouvelle-Zélande |
| Numéro d'identification MyKad | Numéro d'identification de la carte d'identité MyKad de Malaisie |

| Pattern | Description |
|---|---|
| Numéro d’identification MyNumber | Numéro d'identification du système fiscal et de la sécurité sociale du Japon |
| Numéro d’identification du NHI | Numéro du National Health Index de Nouvelle-Zélande |
| Numéro d’identification NIF | Numéro d'identification fiscale d’Espagne |
| Numéro d’identification NIN | Numéro de la carte d'identification de Taïwan |
| Numéro d’identification NRIC | Numéro d’identification de la carte d'identité nationale de Singapour |
| Numéro d’identification de compte permanent | Numéro d’identification de compte permanent d’Inde pour les ressortissants indiens |
| Numéro d’identification de la RPC | Numéro d'identification des résidents de la République populaire de Chine |
| Numéro d’identification PRN | Numéro d'enregistrement des résidents de la République de Corée du Sud |
| Enregistrement des résidents de la République de Corée du Sud | Numéro d'enregistrement des résidents de la République de Corée du Sud |

# WildFire Inline ML

L'option inline ML de WildFire dans les profils d'antivirus permet aux plan de données du pare-feu d'appliquer l'apprentissage machine aux scripts PowerShell, fichiers PE (Portable Executable) et fichiers ELF (format exécutable et lié) en temps réel. Cette couche de protection antivirus complète les signatures basées sur WildFire afin de fournir une couverture étendue pour les fichiers dont les signatures n'existent pas encore. Chaque modèle ML détecte dynamiquement les fichiers malveillants d'un type donné en évaluant les détails du fichier, y compris les champs et schémas du décodeur, afin de formuler une classification à forte probabilité d'un fichier. Cette protection s'étend aux variantes actuellement inconnues et aux variantes futures des menaces qui correspondent aux caractéristiques que Palo Alto Networks a identifiées comme étant malveillantes. Afin d'être au courant des dernières évolutions des menaces, les modèles Inline ML sont ajoutés ou mis à jour via des communiqués de contenu. Avant de pouvoir activer WildFire Inline ML, vous devez posséder un abonnement WildFire actif.

La protection basée sur Inline ML peut également être activée pour détecter les URL malveillantes en temps réel dans le cadre de la configuration de votre filtrage des URL. Pour en savoir plus, reportez-vous à la section : Filtrage des URL Inline ML

***WildFire Inline ML n'est pas pris en charge sur l'appareil virtuel VM-50 ou VM50L.***

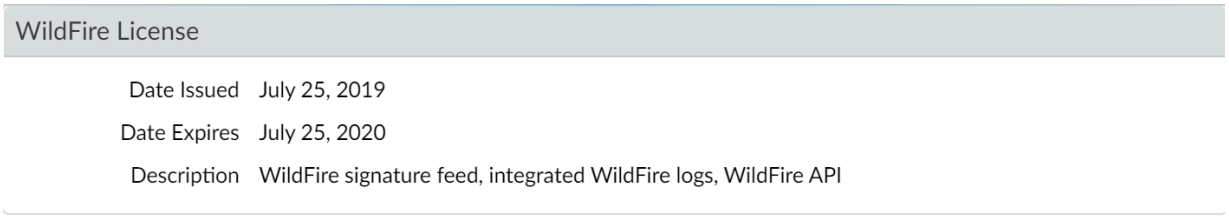
## Configuration de WildFire Inline ML

Pour activer votre configuration WildFire inline ML, attachez le profil antivirus configuré avec les paramètres Inline ML à une règle de politique de sécurité (voir Set Up Antivirus, Anti-Spyware, and Vulnerability Protection (Configuration de l'antivirus, de l'antispyware et de la protection contre les vulnérabilités)).

***WildFire Inline ML n'est actuellement pas pris en charge sur l'appareil virtuel VM-50 ou VM50L.***

**STEP 1 |** Pour profiter de WildFire Inline ML, vous devez avoir un abonnement WildFire actif pour analyser les exécutables Windows.

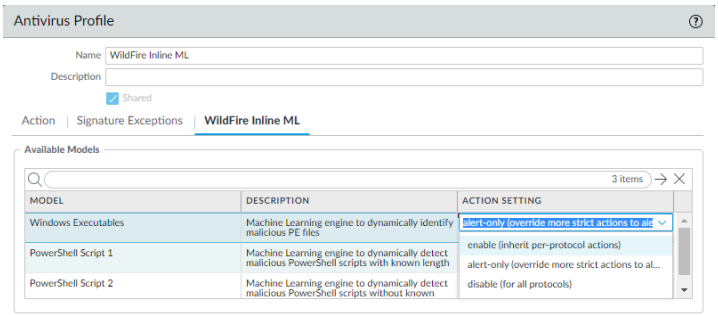
Vérifiez que vous disposez d'un abonnement WildFire. Pour vérifier quels sont les abonnements pour lesquels vous avez actuellement des licences, sélectionnez **Device (Périphérique)** > **Licenses (Licences)** et vérifier que les licences appropriées s'affichent et n'ont pas expiré.



**STEP 2 |** Créez un nouveau profil de sécurité antivirus ou mettez à jour votre ou vos profils de sécurité antivirus existants pour utiliser les modèles de WildFire Inline ML en temps réel.

1. Sélectionnez un **Antivirus Profile (Profil antivirus)** existant ou créez un nouveau profil (sélectionnez **Objects (Objets) > Security Profiles (Profils de sécurité) > Antivirus** et **Add (Ajoutez)** un nouveau profil.
2. Configurez votre profil antivirus.
3. Sélectionnez l'onglet **WildFire Inline ML** et appliquez un **Action Setting (Paramètre d'action)** pour chaque modèle WildFire Inline ML. Cela permet d'appliquer les paramètres des actions WildFire Inline ML configurés pour chaque protocole sur la base d'un modèle. Les moteurs de classification suivants sont disponibles : Exécutables Windows, PowerShell Scripts 1, PowerShell Scripts 2 et Executable Linked Format (disponible avec l'installation du contenu PAN-OS version 8367 et versions ultérieures).




   - **enable (activer) (hériter des actions par protocole)** : WildFire inspecte le trafic en fonction de vos sélections dans la colonne Action WildFire Inline ML dans la section décodeurs de l'onglet **Action**.
   - **alert-only (alerte uniquement) (passer outre des actions plus strictes pour alerter)** : WildFire inspecte le trafic en fonction de vos sélections dans la colonne Action WildFire Inline ML dans la section décodeurs de l'onglet **Action** et annule toute action dont le niveau de gravité est supérieur à `alert (alerte)` (`drop (abandon)`, `reset-client (réinitialisation du client)`, `reset-server (réinitialisation du serveur)`, `reset-both (réinitialisation des deux)`) `alert (alerte)`, qui permet le passage du trafic tout en générant et en enregistrant une alerte dans les journaux des menaces.
   - **disable (désactiver) (pour tous les protocoles)** : WildFire permet au trafic de passer sans aucune action de politique.
4. Cliquez sur **OK** pour quitter la fenêtre de configuration du profil antivirus et **Commit (Validez)** vos nouveaux paramètres.

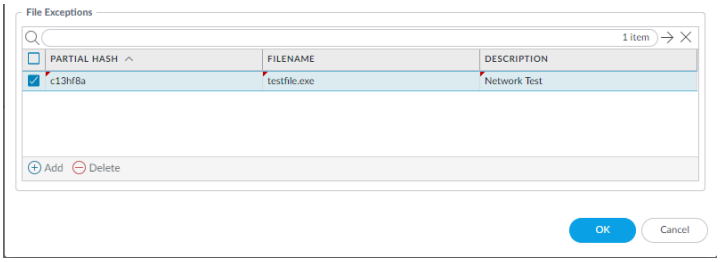
**STEP 3 |** (Facultatif) Ajoutez des exceptions de fichier à votre profil de sécurité antivirus si vous rencontrez des faux positifs. Cela est généralement fait pour les utilisateurs qui ne transfèrent pas de fichiers à WildFire pour analyse. Vous pouvez ajouter les détails des exceptions de

fichiers directement à la liste des exceptions ou en spécifiant un fichier à partir des journaux des menaces.

*Si votre profil de sécurité WildFire Analysis est configuré pour transmettre les types de fichiers analysés à l'aide de WildFire inline ML, les faux positifs sont automatiquement corrigés dès leur réception. Si vous continuez à voir des alertes ml-virus pour des fichiers classés comme bénins par WildFire Analysis, veuillez contacter l'assistance de Palo Alto Networks.*

- Ajout d'exceptions de fichiers directement à la liste des exceptions.
  1. Sélectionnez **Objects (Objets) > Security Profiles (Profils de sécurité) > Antivirus**.
  2. Sélectionnez un profil antivirus pour lequel vous souhaitez exclure des fichiers spécifiques, puis sélectionnez **WildFire Inline ML**.
  3. Ajoutez le hachage, le nom de fichier et la description du fichier que vous voulez exclure de l'application.




  4. Cliquez sur **OK** pour enregistrer le profil antivirus puis **Commit (Validez)** vos mises à jour.
- Ajout d'exceptions de fichiers à partir des entrées des journaux des menaces.
  1. Sélectionnez **Monitor (Moniteur) > Logs (Journaux) > Threat (Menace)** et filtrer les journaux pour le type de menace **ml-virus**. Sélectionnez un journal des menaces pour un fichier pour lequel vous souhaitez créer une exception de fichier.
  2. Accédez à **Detailed Log View (Vue détaillée du journal)** et faites défiler vers le bas jusqu'au volet **Details (Détails)** puis sélectionnez **Create Exception (Créer une exception)**.


  3. Ajoutez une **Description** et cliquez sur **OK** pour ajouter l'exception de fichier.
  4. La nouvelle exception de fichier se trouve dans la liste **File Exceptions (Exceptions de fichier)** sous **Objects (Objets) > Security Profiles (Profils de sécurité) > Antivirus > WildFire Inline ML**.

**STEP 4 |** (Facultatif) Vérifiez l'état de la connectivité de votre pare-feu au service Inline ML dans le cloud.

Utilisez la commande CLI suivante sur le pare-feu pour afficher l'état de la connexion.

```
show mlav cloud-status
```

Par exemple :

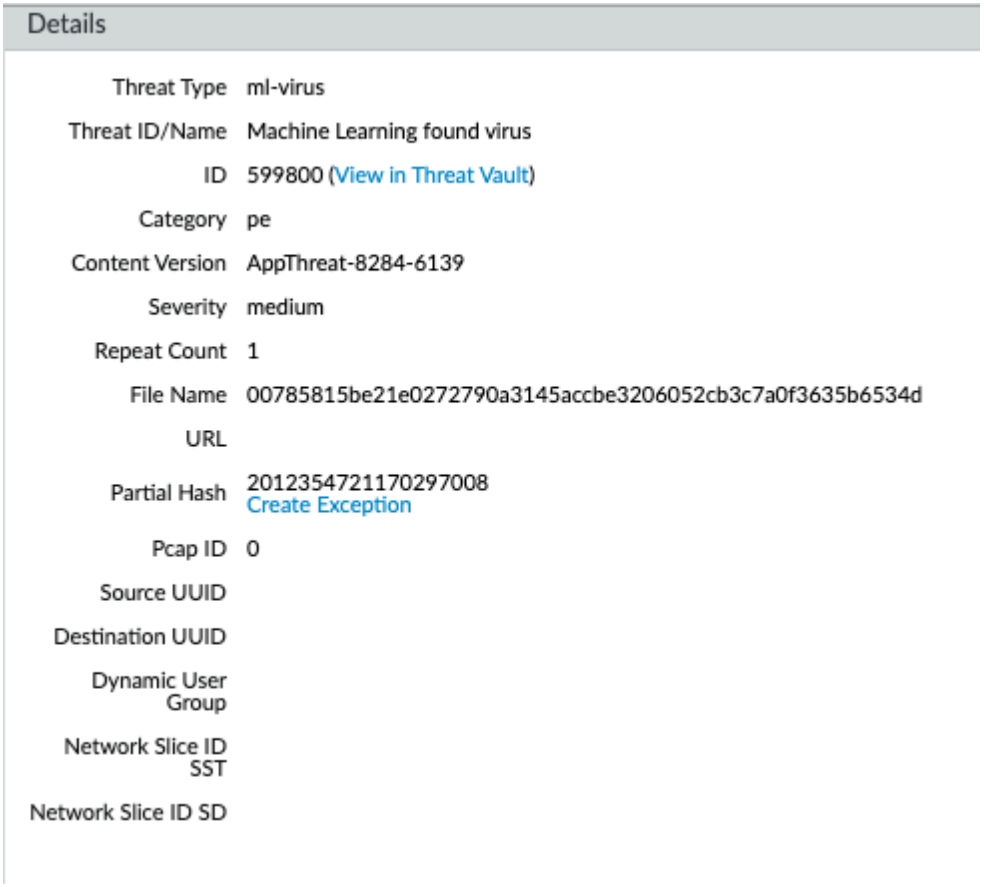
```
show mlav cloud-status
```

```
MLAV cloud
Current cloud server:          ml.service.paloaltonetworks.com
Cloud connection:              connected
```

Si vous ne pouvez pas vous connecter au service cloud Inline ML, vérifiez que le domaine suivant n'est pas bloqué : ml.service.paloaltonetworks.com.

Pour consulter les informations sur les fichiers qui ont été détectés à l'aide de WildFire Inline ML, examinez les journaux de menaces (**Monitor (Moniteur) > Logs (Journaux) > Threat (Menace)**, puis sélectionnez le type de journal dans la liste). Les fichiers qui ont été analysés à l'aide de WildFire Inline ML sont étiquetés avec le type de menace **ml-virus** :



# Paramétrer le blocage des fichiers

Les Profils de blocage des fichiers vous permettent d'identifier les types de fichiers spécifiques que vous souhaitez bloquer ou surveiller. Pour la plupart du trafic (y compris le trafic sur votre réseau interne), bloquez les fichiers qui comportent généralement des menaces ou qui n'ont pas besoin d'être chargés ou téléchargés. À l'heure actuelle, il s'agit de fichiers batch, de fichiers DLL, de fichiers de classe Java, de fichiers d'aide, de raccourcis Windows (.lnk) et de fichiers BitTorrent. En outre, pour procurer une protection contre les téléchargements automatiques, autorisez le chargement/téléchargement de fichiers exécutables et de fichiers d'archives (.zip et .rar), en forçant toutefois les utilisateurs à reconnaître qu'ils transfèrent un fichier pour qu'ils sachent que le navigateur tente de télécharger un fichier à leur insu. Pour des règles de politique qui autorisent la navigation générale sur le web, soyez plus strict en matière de blocage de fichiers, car le risque que des utilisateurs téléchargent des fichiers malveillants à leur insu est beaucoup plus élevé. Pour ce type de trafic, associez un profil de blocage des fichiers beaucoup plus strict qui bloquera également des fichiers PE (exécutable portable).

Vous pouvez définir vos propres profils de blocage des fichiers personnalisés, ou choisir l'un des profils prédéfinis suivants lors de l'application de blocage de fichiers à une règle de politique de sécurité : Vous pouvez cloner et modifier les profils prédéfinis, qui sont disponibles avec la version de contenu 653 ou toute version ultérieure. Suivez ensuite les étapes de transition vers un profil de blocage des fichiers pour préserver la disponibilité des applications lors de votre transition vers les paramètres exemplaires de blocage des fichiers :

- **basic file blocking (blocage de base des fichiers)** : Associez ce profil aux règles de politique de sécurité qui autorisent du trafic en provenance de et en destination des applications moins sensibles afin de bloquer des fichiers qui sont fréquemment inclus dans les campagnes d'attaques par logiciels malveillants ou qui n'ont pas besoin d'être chargés ou téléchargés. Ces profils bloquent le chargement/téléchargement de fichiers PE ( .scr, .cpl, .dll, .ocx, .pif, .exe) , de fichiers de classe Java (.class, .jar), de fichiers d'aide (.chm, .hlp) et d'autres types de fichiers potentiellement malveillants, comprenant les fichiers .vbe, .hta, .wsf, .torrent, .7z, .rar, .bat. De plus, cela invite les utilisateurs à accepter de télécharger des fichiers rar chiffrés ou des fichiers zip chiffrés. Cette règle génère une alerte pour tous les autres types de fichier pour vous apporter une visibilité complète sur tous les fichiers qui entrent et sortent de votre réseau.
- **strict file blocking (blocage strict de fichiers)** : utiliser ce profil plus strict pour les règles de politique de sécurité permettant un accès aux applications les plus sensibles. Ce profil bloque le même type de fichiers que l'autre profil, et bloque également les fichiers flash, .tar, .cab, .msi, les fichiers avec codage à niveaux multiples, les fichiers rar chiffrés, ainsi que les fichiers zip chiffrés.

Ces profils prédéfinis ont été conçus pour vous apporter la meilleure posture de sécurité pour votre réseau. Toutefois, si des applications vitales pour votre fonctionnement dépendent d'applications bloquées qui sont par défaut dans ces profils, vous pouvez cloner ces profils et les modifier selon vos besoins. Assurez-vous d'utiliser les profils modifiés uniquement pour les utilisateurs qui ont des besoins de chargement/téléchargement de fichiers à risque. De plus, pour réduire votre surface d'attaque, veillez à utiliser d'autres mesures de sécurité pour garantir que les fichiers chargés ou téléchargés par vos utilisateurs ne représentent pas de menace pour votre organisation. Par exemple, si vous devez autoriser le téléchargement de fichiers PE, veillez à Faire analyser tous les fichiers PE inconnus par WildFire. Enfin, maintenez une politique de filtrage des URL stricte pour garantir que les utilisateurs ne puissent pas télécharger de contenu sur des sites web identifiés comme hébergeant du contenu malveillant.

**STEP 1 |** Créez le profil de blocage des fichiers.

1. Select **Objects (Objets)** > **Security Profiles (Profils de Sécurité)** > **File Blocking (Blocage des fichiers)** et **Add (Ajoutez)** un profil.
2. Donnez un **Name (Nom)** au profil de blocage des fichiers, par exemple, **`Block_EXE`**.
3. (Facultatif) Vous pouvez éventuellement saisir une **Description**, telle que **`Empêcher les utilisateurs de télécharger des fichiers exécutables des sites Web`**.
4. (Facultatif) Précisez si le profil est **Partagé** avec :
   - **Tous les systèmes virtuels (vsys) sur un pare-feu comportant plusieurs vsys** - S'il est effacé (désactivé), le profil est disponible uniquement dans le système virtuel sélectionné dans l'onglet **Objects (Objets)**.
   - **Tous les groupes de périphériques sur Panorama** - S'il est effacé (désactivé), le profil est disponible uniquement dans le groupe de périphériques sélectionné dans l'onglet **Objects (Objets)**.
5. (Facultatif - Uniquement Panorama) Sélectionnez **Disable override (Désactiver le contrôle prioritaire)** pour empêcher les administrateurs de remplacer les paramètres du profil de blocage des fichiers dans les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres de tous les groupes de périphériques qui héritent du profil.

**STEP 2 |** Configurez les options de blocage des fichiers.

1. Cliquer sur **Add (Ajouter)** et définissez une règle pour le profil.
2. Saisissez un **Name (Nom)** pour la règle, par exemple **`BlockEXE`**.
3. Sélectionnez **Any (Indifférent)** ou précisez une ou plusieurs **Applications** spécifiques pour le filtrage, comme la **web-browsing (navigation web)**.

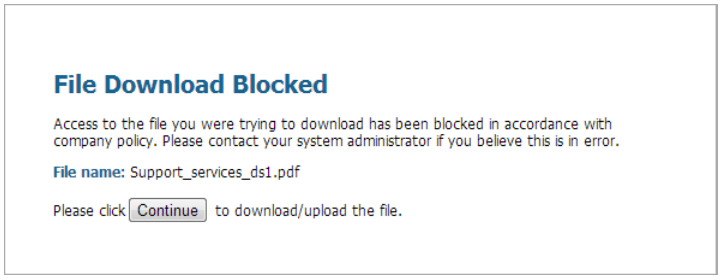
   *Seuls les navigateurs web peuvent afficher une page de réponse (Invite pour continuer) qui autorise les utilisateurs à confirmer que le fait de Choisir toute autre application aura pour conséquence de bloquer le trafic vers ces applications, car il n'y a pas d'invite affichée permettant aux utilisateurs de continuer.*
4. Sélectionnez **Any (Indifférent)** ou précisez une ou plusieurs **File Types (Types de fichier)** spécifiques, comme par exemple **exe**.
5. Définissez la **Direction**, par exemple**download (téléchargement)**.
6. Définissez l'**Action** (**alert (alerte)**, **block (blocage)**, ou **continue (continuer)**). Par exemple, sélectionnez **continue (continuer)** pour inviter les utilisateurs à confirmer avant d'avoir l'autorisation télécharger un fichier exécutable (.exe). D'autre part, vous pouvez **block (bloquer)** les fichiers spécifiés ou vous pouvez configurer le pare-feu afin qu'il déclenche une **alert (alerte)** quand un utilisateur télécharge un fichier exécutable.
7. Cliquez sur **OK** pour enregistrer le profil.

**STEP 3 |** Appliquez le profil de blocage des fichiers à une règle de politique de sécurité.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et choisissez une règle de politique existante ou **Add (Ajoutez)** une nouvelle règle comme indiqué à la section Configuration d'une politique de sécurité de base.
2. Dans l'onglet **Actions**, sélectionnez le profil de blocage des fichiers configuré dans l'étape précédente. Dans ce cas, le nom du profil est **`Block_EXE`**.
3. **Commit (Validez)** vos modifications.

**STEP 4 |** Pour tester votre configuration de blocage des fichiers, accédez à un PC terminal dans la zone approuvée du pare-feu et tentez de télécharger un fichier exécutable sur un site Web se trouvant dans la zone non approuvée. Une page de réponse devrait s'afficher. Cliquez sur **Continue (Continuer)** pour confirmer que vous pouvez télécharger le fichier. Vous pouvez également définir d'autres actions, par exemple, **alert (alerter)** ou **block (bloquer)**, qui ne présentent à l'utilisateur aucune option pour poursuivre son téléchargement. Voici un exemple de page de réponse par défaut pour le blocage des fichiers :




**STEP 5 |** (Facultatif) Définissez des pages de réponse personnalisées pour le blocage de fichiers (**Device (Périphérique)** > **Response Pages (Pages de réponse)**). Cela vous permet de fournir plus d'informations aux utilisateurs sur une page de réponse. Vous pouvez inclure des informations telles que des informations relatives à la politique de l'entreprise et des informations de contact pour un service de support.

*Lorsque vous créez un profil de blocage des fichiers à l'aide de l'action **continue (continuer)**, vous pouvez uniquement choisir l'application **web-browsing (navigation-web)**. Si vous choisissez une autre application, le trafic correspondant à la politique de sécurité ne traverse pas le pare-feu car aucune page invitant l'utilisateur à continuer ne s'affiche. Vous devez également configurer et activer une politique de décryptage pour les sites web HTTPS.*

*Vérifiez vos journaux pour déterminer quelles sont les applications utilisées quand vous testez cette fonctionnalité. Par exemple, si vous utilisez Microsoft SharePoint pour télécharger les fichiers, même si vous utilisez un navigateur Web pour accéder au site, l'application est en fait `sharepoint-base` ou `sharepoint-document`. (Pour plus de facilité, vous pouvez définir le type d'application sur **Any (Indifférent)** pour le test.)*

# Prévention des attaques par force brute

Une attaque par force brute utilise un important volume de requêtes/réponses d'une même adresse ID source ou de destination pour pénétrer par effraction dans un système. Le pirate utilise une méthode essai-et-erreur pour deviner la réponse à un défi ou une requête.

Le profil Protection des vulnérabilités du pare-feu contient des signatures afin de vous protéger des attaques par force brute. Chaque signature dispose d'un ID, d'un nom de menace et d'un niveau de gravité. Elle se déclenche lors de l'enregistrement d'un modèle. Le modèle indique les conditions et l'intervalle d'identification du trafic en tant qu'attaque par force brute ; certaines signatures sont associées à une autre signature enfant dont la gravité est moindre et qui indique le modèle de correspondance. Lorsqu'un modèle correspond à la signature ou à la signature enfant, il déclenche l'action par défaut de la signature.

Pour appliquer une protection :

- Associez le profil de protection contre les vulnérabilités à une règle de politique de sécurité. Consultez la section Paramétrage des profils Antivirus, Antispyware et Protection contre les vulnérabilités.
- Installez les mises à jour du contenu qui renferment de nouvelles signatures pour vous protéger des menaces émergentes. Reportez-vous à la section Installer les mises à jour de contenu et logicielles

# Personnalisation de l'action et des conditions de déclenchement de la signature d'une attaque par force brute

Le pare-feu contient deux types de signatures d'attaques par force brute : des signatures parent et des signatures enfant. Une signature enfant est l'occurrence unique d'un modèle de trafic correspondant à la signature. Une signature parent est associée à une signature enfant et se déclenche lorsque plusieurs événements se produisent au cours d'un intervalle de temps donné et correspondent au modèle de trafic défini dans la signature enfant.

En général, une signature enfant applique l'action ***autoriser*** par défaut, car un événement unique n'est pas révélateur d'une attaque. On s'assure ainsi que le trafic légitime n'est pas bloqué et que des journaux de menaces ne sont pas générés pour des événements anodins. Palo Alto Networks vous recommande de ne pas modifier l'action par défaut sans y avoir bien réfléchi.

En général, la signature d'une attaque par force brute est un événement notable en raison de son modèle récurrent. Au besoin, vous pouvez procéder de l'une des manières suivantes pour personnaliser l'action de la signature d'une attaque par force brute :

- Créez une règle pour modifier l'action par défaut de toutes les signatures de la catégorie Force brute. Vous pouvez choisir d'autoriser, d'alerter, de bloquer, de réinitialiser ou de supprimer le trafic.
- Définissez une exception pour une signature spécifique. Par exemple, vous pouvez rechercher des CVE et définir une exception pour ces derniers.

Pour une signature parent, les conditions de déclenchement et l'action peuvent être modifiées ; pour une signature enfant, seule l'action peut être modifiée.

*Pour atténuer efficacement une attaque, spécifiez l'action bloquer-adresse ip plutôt que l'action « supprimer » ou « réinitialiser » pour la plupart des signatures d'attaques par force brute.*

**STEP 1 |** Créez un nouveau profil de protection contre les vulnérabilités.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Vulnerability Protection (Protection contre les vulnérabilités)** et **Add (Ajoutez)** un profil.
2. Donnez un **Name (Nom)** au profil de protection contre les vulnérabilités.
3. (Facultatif) Saisissez une **Description (Description)**.
4. (Facultatif) Précisez si le profil est **Partagé** avec :
   - **Tous les systèmes virtuels (vsys) sur un pare-feu comportant plusieurs vsys** - S'il est effacé (désactivé), le profil est disponible uniquement dans le système virtuel sélectionné dans l'onglet **Objects (Objets)**.
   - **Tous les groupes de périphériques sur Panorama** - S'il est effacé (désactivé), le profil est disponible uniquement dans le groupe de périphériques sélectionné dans l'onglet **Objects (Objets)**.
5. (Facultatif—Panorama uniquement) Sélectionnez **Disable override (Désactiver le contrôle prioritaire)** pour empêcher les administrateurs de remplacer les paramètres de ce profil

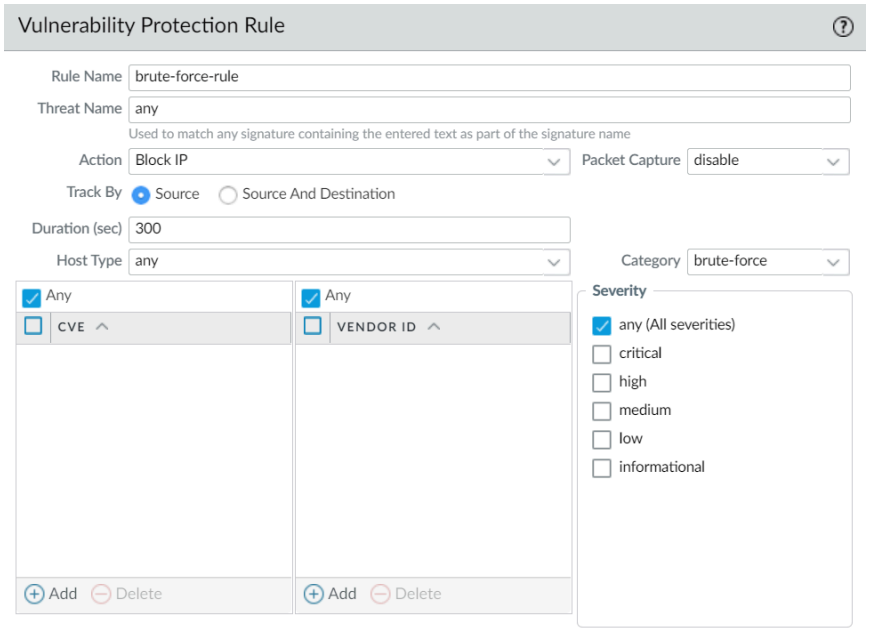
 

de protection contre les vulnérabilités dans les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres de tous les groupes de périphériques qui héritent du profil.

**STEP 2 |** Créez une règle qui définit l'action de toutes les signatures d'une catégorie.

1. À l'onglet **Rules (Règles)**, **Add (Ajoutez)** une nouvelle règle et donnez-lui un **Rule Name (Nom de règle)**.
2. (Facultatif) Indiquez un nom de menace particulier (**any (Indifférent)** est défini par défaut).
3. Définissez l'**Action (Action)**. Dans cet exemple, elle est définie sur **Block IP (Bloquer les adresses IP)**.

   *Si vous définissez un profil de protection contre les vulnérabilités sur Block IP (Bloquer les adresses IP), le pare-feu se sert d'abord du matériel pour bloquer les adresses IP. Si le trafic d'attaque dépasse la capacité de blocage du matériel, le pare-feu utilise alors des mécanismes de blocage par logiciel pour bloquer les adresses IP restantes.*
4. Définissez **Category (Catégorie)** sur **brute-force (force-brute)**.
5. (Facultatif) Si le blocage est sélectionné, précisez le **Host Type (Type d'hôte)** sur lequel effectuer le blocage : **server (serveur)** ou **client** (par défaut **any [indifférent]**).
6. Consultez l'étape 3 pour personnaliser l'action pour une signature spécifique.
7. Consultez l'étape 4 pour personnaliser le seuil de déclenchement pour une signature parent.




8. Cliquez sur **OK (OK)** pour enregistrer la règle et le profil.

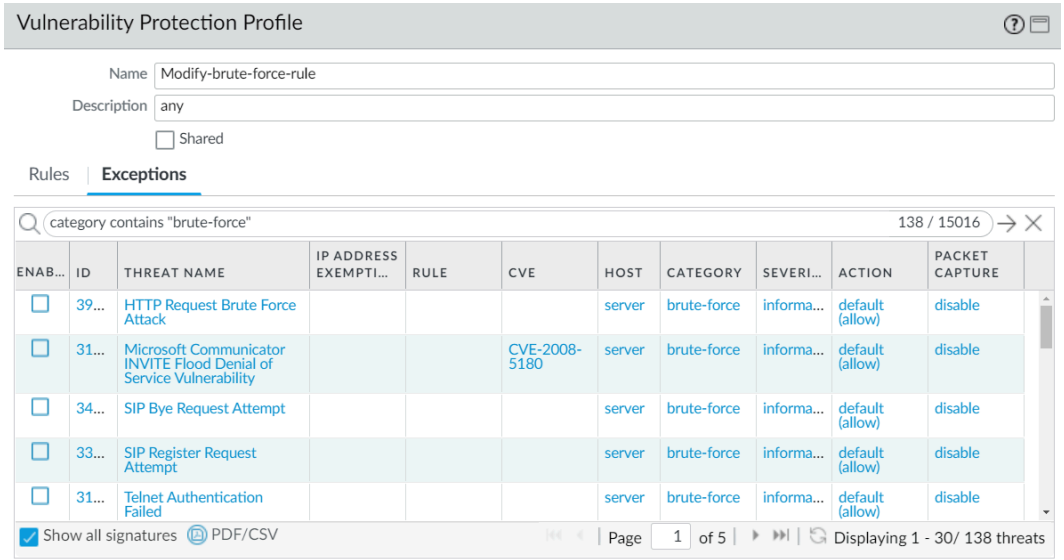
 

**STEP 3 |** (Facultatif) Personnalisez l'action d'une signature spécifique.

1. À l'onglet **Exceptions (Exceptions)**, cliquez sur **Show all signatures (Afficher toutes les signatures)** pour trouver la signature que vous souhaitez modifier.

   Pour afficher toute les signatures dans la catégorie force-brute, recherchez `category contains 'brute-force'`.

2. Pour modifier une signature spécifique, cliquez sur l'action par défaut prédéfinie dans la colonne Action (Action).




3. Définissez l'action : **Allow (Autoriser)**, **Alert (Alerter)**, **Block Ip (Bloquer les adresses IP)** ou **Drop (Abandonner)**. Si vous sélectionnez **Block Ip (Bloquer les adresses IP)**, exécutez les tâches suivantes :

   1. Indiquez le **Time (Délai)** (en secondes) au bout duquel l'action sera déclenchée.
   2. Indiquez s'il faut **Track By (Suivre en fonction de)** et bloque l'adresse IP à l'aide de la **IP source (Adresse IP source)** ou de la **IP source and destination (Adresse IP source et de destination)**.

4. Cliquez sur **OK**.
5. Pour chaque signature modifiée, cochez la case dans la colonne **Enable (Activer)**.
6. Cliquez sur **OK**.

**STEP 4 |** Personnalisation des conditions de déclenchement d'une signature parent.

Une signature parent modifiable affiche cette icône : .

Dans cet exemple, les critères de recherche étaient la catégorie force-brute et CVE-2008-1447.

1. Modifiez ( ) l'attribut « Délai » et le critère d'agrégation de la signature.
2. Pour modifier le seuil de déclenchement, indiquez le **Number of Hits (Nombre d'accès)** par nombre de **seconds (secondes)**.
3. Indiquez si vous souhaitez agréger le nombre d'accès (**Aggregation Criteria (Critère d'agrégation)**) par **source (source)**, **destination (destination)** ou par **source-and-destination (source et destination)**.
4. Cliquez sur **OK**.

**STEP 5 |** Associez ce nouveau profil à une règle de politique de sécurité.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et **Add (ajoutez)** ou modifiez une règle de politique de sécurité.
2. À l'onglet **Actions (Actions)**, sélectionnez **Profiles (Profils)** en tant que **Profile Type (Type de profil)** du paramètre Profil.
3. Sélectionnez votre profil de **Vulnerability Protection (Protection contre les vulnérabilités)**.
4. Cliquez sur **OK**.

**STEP 6 |** Validez vos modifications.

1. Cliquez sur **Commit (Valider)**.

# Activer les signatures d'évasion

Les signatures d'évasion Palo Alto Networks détectent des requêtes HTTPS ou TLS fabriquées et peuvent envoyer une alerte pour aviser des instances sur lesquelles un client se connecte à un domaine autre que celui qui est indiqué dans une requête DNS. Les signatures d'évasion sont en vigueur uniquement lorsque le pare-feu est également autorisé à agir en tant que proxy DMS et à résoudre des requêtes de noms de domaine. Il est recommandé de suivre les étapes suivantes pour activer les signatures d'évasion.

**STEP 1 |** Activez un pare-feu qui est intermédiaire des clients et serveurs pour qu'il agisse en tant que proxy DNS.

Configuration d'un objet proxy DNS, y compris :

- Précisez les interfaces sur lesquelles vous souhaitez que le pare-feu écoute les requêtes DNS.
- Définissez les serveurs DNS avec lesquels le pare-feu communique pour résoudre les requêtes DNS.
- Configurez des entrées FQDN à l'adresse IP statique que le pare-feu peut résoudre localement, sans avoir à contacter des serveurs DNS.
- Activez la mise en cache des mappages nom d'hôte/adresse IP résolus.

**STEP 2 |** Obtenez la version de contenu Applications et menaces la plus récente (au moins la version 579 ou toute version ultérieure).

1. Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**.
2. Cliquez sur **Check Now (Vérifier maintenant)** pour télécharger les dernières mises à jour du contenu Applications et Menaces.
3. Téléchargez et installez la version du contenu Applications et Menaces 579 (ou version ultérieure).

**STEP 3 |** Définissez la manière dont le pare-feu devrait mettre appliquer le trafic mis en correspondance avec des signatures d'évasion.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware (Antispyware)** et **Add (Ajoutez)** ou modifiez un profil antispyware.
2. Sélectionnez **Exceptions (Exceptions)** et sélectionnez **Show all signatures (Afficher toutes les signatures)**.
3. Filtrez les signatures selon le mot-clé `evasion`.
4. Pour toutes les signatures d'évasion, définissez l'**Action (Action)** sur n'importe quel paramètre autre que l'action par défaut ou autoriser (l'action définie par défaut pour les signatures d'évasion est Autoriser). Par exemple, définissez l'**Action (Action)** des ID de signature 14978 et 14984 sur **alert (alerter)** ou **drop (abandonner)**.
5. Cliquez sur **OK (OK)** pour enregistrer le profil antispyware mis à jour.
6. Associez le profil antispyware à une règle de politique de sécurité : Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis choisissez la politique que vous souhaitez modifier et cliquez sur l'onglet **Actions (Actions)**. Dans les Paramètres de profil, cliquez sur la liste déroulante en regard de **Anti-Spyware (Antispyware)** et sélectionnez le profil antispyware que vous venez de modifier pour appliquer les signatures d'évasion.

**STEP 4 |** Validez vos modifications.

Cliquez sur **Commit (Valider)**.

# Surveiller les adresses IP bloquées

Le pare-feu conserve une liste de blocage des adresses IP source qu'il bloque. Lorsque le pare-feu bloque une adresse IP source, par exemple lorsque vous configurez l'une des règles de politique suivantes, le pare-feu bloque le trafic dans le matériel avant que ces paquets n'utilisent des ressources du processeur ou de tampon de paquet :

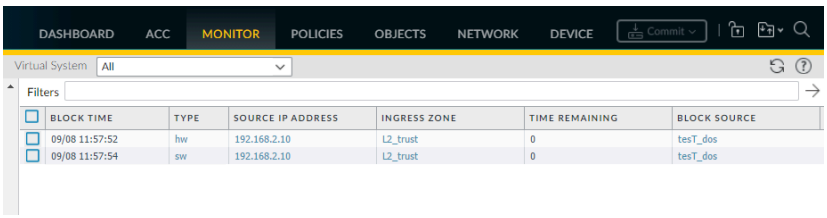
- Une règle classifiée de politique de Protection DoS avec l'action de **Protect (Protéger)** (une politique de Protection DoS classifiée spécifie que les connexions entrantes correspondent à une adresse IP source, une adresse IP de destination ou à une paire d'adresses IP source et de destination est associée à un profil de protection DoS classifié, comme décrit dans DoS Protection contre l'inondation de nouvelles sessions).
- Une règle de Politique de sécurité qui utilise un profil de protection contre les vulnérabilités

Le blocage des adresses IP matérielles est pris en charge sur les pare-feu PA-3200, PA-5200 et PA-7000.

Vous pouvez afficher la liste des blocs, obtenir des informations détaillées sur une adresse IP dans la liste des blocs ou afficher le nombre d'adresses bloquées par le matériel et le logiciel. Vous pouvez supprimer une adresse IP de la liste si vous pensez qu'elle ne devrait pas être bloquée. Vous pouvez modifier la source des informations détaillées sur les adresses de la liste. Vous pouvez également modifier la durée pendant laquelle le matériel bloque les adresses IP.

- Afficher les entrées de la liste d'interdiction.
  1. Sélectionnez **Monitor (Surveillance)** > **Block IP List (Bloquer la liste d'adresses IP)**.

     Les entrées de la liste d'interdiction indiquent dans la colonne Type si elles ont été bloquées par le matériel (hw) ou le logiciel (sw).
  2. Voir au bas de l'écran :
     - Le nombre **Total Blocked IPs (Total des adresses IP bloquées)** sur le nombre d'adresses IP bloquées prises en charge par le pare-feu.
     - Pourcentage de la liste d'interdiction utilisée par le pare-feu.
  3. Pour filtrer les entrées affichées, sélectionnez une valeur dans une colonne (qui crée un filtre dans le champ **Filters (Filtres)**) et Appliquez le filtre (→). Sinon, le pare-feu affiche les 1 000 premières entrées.
  4. Entrez un numéro de **Page** ou cliquez sur les flèches en bas de l'écran pour avancer dans les pages des entrées.
  5. Pour afficher les détails d'une adresse dans la liste des blocs, passez la souris sur une adresse IP source et cliquez sur le lien vers le bas. Cliquez sur le lien **Who is (Qui est...)** qui affiche l'information Network Solutions Who Is sur l'adresse.



- Supprimer les entrées de la liste d'interdiction.

  *Supprimez une entrée si vous déterminez que l'adresse IP ne devrait pas être bloquée. Révisez ensuite la règle de politique qui a provoqué le blocage de l'adresse par le pare-feu.*

  1. Sélectionnez **Monitor (Surveillance)** > **Block IP List (Bloquer la liste d'adresses IP)**.
  2. Sélectionnez une ou plusieurs entrées et cliquez sur **Delete (Supprimer)**.
  3. (Facultatif) Sélectionnez **Clear All (Tout effacer)** pour supprimer toutes les entrées de la liste.

- Désactivez ou réactivez le blocage de l'adresse IP matérielle à des fins de dépannage.

  *Bien que le blocage de l'adresse IP matérielle soit désactivé, le pare-feu effectue toujours le blocage logiciel de toute adresse IP que vous avez configuré.*

  ```
  > set system setting hardware-acl-blocking [enable | disable]
  ```

  *Pour préserver ressources du processeur ou de la mémoire tampon des paquets, gardez le blocage matériel de l'adresse IP activé sauf si le support technique de Palo Alto Networks vous demande de le désactiver, par exemple, si un débogage d'un flux de trafic est en cours.*

- Réglez le nombre de secondes pendant lesquelles les adresses IP bloquées par le matériel restent sur la liste d'interdiction (la plage est comprise entre 1 et 3600 ; La valeur par défaut est 1).

  ```
  > set system setting hardware-acl-blocking duration <seconds>
  ```

  *Maintenez une durée plus courte pour les entrées de liste d'interdiction matérielle que pour les entrées de liste d'interdiction logicielle afin de réduire la probabilité de dépasser la capacité de blocage du matériel.*

- Modifier le site Web par défaut pour trouver plus d'informations sur une adresse IP de Solutions réseau Qui est à un site Web différent.

  ```
  # set deviceconfig system ip-address-lookup-url <url>
  ```

- Afficher les nombres d'adresses IP sources bloquées par le matériel et le logiciel, par exemple pour afficher le taux d'une attaque.

  Afficher la somme totale des entrées d'adresse IP dans la liste des blocs et la table des blocs matériels (bloqués par le matériel et le logiciel) :

  ```
  > show counter global name flow_dos_blk_num_entries
  ```

  Afficher le nombre d'entrées d'adresses IP sur la table des blocs matériels bloquées par le matériel :

  ```
  > show counter global name flow_dos_blk_hw_entries
  ```

  Afficher le nombre d'entrées d'adresses IP dans la liste d'interdiction qui ont été bloquées par le logiciel :

  ```
  > show counter global name flow_dos_blk_sw_entries
  ```

- Afficher les informations de liste d'interdiction par emplacement sur un pare-feu de la série PA-7000.

  ```
  > show dos-block-table software filter slot <slot-number>
  ```

# Catégories de signatures de menace

Il existe trois types de signatures de menace Palo Alto Networks, chacune conçue pour détecter différents types de menaces lorsque le pare-feu balaye le trafic réseau :

- Signatures antivirus: détectez les virus et les logiciels malveillants détectés dans les exécutables et les types de fichiers.
- Signatures anti-spyware : détecte les activités de commande-et-contrôle (C2), dans le cadre desquelles un logiciel espion installé sur un client infecté collecte des données sans le consentement de l'utilisateur et/ou entre en communication avec un pirate à distance.
- Signatures de vulnérabilité : détecte les failles du système qu'un pirate pourrait autrement tenter d'exploiter.

La gravité d'une signature indique le risque de l'événement détecté, et l'action par défaut d'une signature (par exemple, bloquer ou transmettre une alerte) correspond à la façon dont Palo Alto Networks vous recommande d'appliquer le trafic correspondant.

Vous devez Configurer la protection antivirus, antispyware et antivirus pour indiquer au pare-feu quelle action entreprendre lorsqu'il détecte une menace, vous pouvez facilement utiliser les profils de sécurité par défaut pour bloquer les menaces en fonction des recommandations de Palo Alto Networks. Pour chaque type de signature, de catégorie et même de signature spécifique, vous pouvez continuer à modifier ou à créer de nouveaux profils pour appliquer plus efficacement les menaces éventuelles.

Le tableau suivant répertorie toutes les catégories de signatures possibles par type (antivirus, logiciels espions et vulnérabilités) et inclut la mise à jour du contenu (applications et menaces, antivirus ou WildFire) fournissant les signatures de chaque catégorie. Vous pouvez aussi aller sur les réseaux Palo Alto Coffre de Menaces à En savoir plus sur les signatures de menaces.

| Catégorie de menaces | Mises à jour de contenu fournissant ces signatures | Description |
|---|---|---|
| **Signatures antivirus** | | |
| apk | Antivirus<br>WildFire ou WildFire privé | Fichiers malveillants d'application Android (APK). |
| dmg | Antivirus<br>WildFire ou WildFire privé | Fichiers d'image de disque Apple malveillants (DMG) utilisés avec MacOS X. |
| flash | Antivirus<br>WildFire ou WildFire privé | Applets Adobe Flash et contenu Flash intégré à des pages Web. |

| Catégorie de menaces | Mises à jour de contenu fournissant ces signatures | Description |
|---|---|---|
| java-class | Antivirus | Applets Java (types de fichiers JAR/Class). |
| macho | Antivirus<br>WildFire ou WildFire privé | Les fichiers objet Mach (Mach-O) sont des fichiers exécutables, des bibliothèques et du code objet natifs de MacOS X. |
| office | Antivirus<br>WildFire ou WildFire privé | Fichiers Microsoft Office, y compris les documents (DOC, DOCX, RTF), les cahiers de travail (XLS, XLSX) et les présentations PowerPoint (PPT, PPTX). |
| openoffice | Antivirus<br>WildFire ou WildFire privé | Documents Office Open XML (OOXML) 2007+. |
| pdf | Antivirus<br>WildFire ou WildFire privé | Fichiers Portable Document Format (PDF). |
| pe | Antivirus<br>WildFire ou WildFire privé | Les fichiers exécutables portatifs (PE) peuvent s'exécuter automatiquement sur un système Windows de Microsoft et ne devraient être autorisés que lorsqu'ils sont autorisés. Ces types de fichiers comprennent ce qui suit :<br>• Code d'objet.<br>• Polices (FON).<br>• Fichiers système (SYS).<br>• Fichiers lecteur (DRV).<br>• Éléments du panneau de configuration Windows (CPL).<br>• DLL (bibliothèque à liaisons dynamiques)<br>• OCX (bibliothèques des contrôles personnalisés OLE ou des contrôles ActiveX).<br>• SCR (scripts pouvant être utilisés pour exécuter d'autres fichiers).<br>• Fichiers EFI (Extensible Firmware Interface), qui s'exécutent entre un système d'exploitation et un microprogramme afin de faciliter les mises à jour de périphériques et les opérations de démarrage.<br>• Fichiers d'informations sur le programme (PIF). |

| Catégorie de menaces | Mises à jour de contenu fournissant ces signatures | Description |
|---|---|---|
| pkg | Antivirus<br>WildFire ou WildFire privé | Packages d'installation de logiciels Apple (PKG), utilisés avec MacOS X. |
| **Signature de logiciels espions** | | |
| adware | Applications et menaces | Détecte les programmes qui affichent des publicités potentiellement indésirables. Certains logiciels publicitaires modifient les navigateurs pour mettre en évidence et créer des liens hypertextes à partir des mots-clés les plus recherchés sur les pages Web. Ces liens redirigent les utilisateurs vers des sites Web publicitaires. Les logiciels publicitaires peuvent également récupérer des mises à jour à partir d'un serveur C2 (commande-et-contrôle) et les installer dans un navigateur ou sur un système client.<br>Les protections nouvellement lancées dans cette catégorie sont rares. |
| autogen | Antivirus | Ces signatures basées sur la charge détectent le trafic de commande et de contrôle (C2) et sont générées automatiquement. Il est important de souligner que les signatures de l'autogène peuvent détecter le trafic C2 même lorsque l'hôte C2 est inconnu ou change rapidement. |
| backdoor | Applications et menaces | Détecte un programme qui permet à un pirate d'obtenir un accès distant non autorisé à un système. |
| Réseau de robots (Botnet) | Applications et menaces | Indique une activité de botnet. Un botnet est un réseau d'ordinateurs infectés par des logiciels malveillants (« bots ») qui sont contrôlés par un pirate. Le pirate peut ordonner, de manière centralisée, à chaque ordinateur d'un réseau de botnets d'effectuer simultanément une action coordonnée (par exemple, le lancement d'une attaque par déni de service). |
| browser-hijack | Applications et menaces | Détecte la présence d'un plugin ou d'un logiciel qui modifie les paramètres du navigateur. Un pirate de navigateur peut prendre en charge la recherche automatique ou suivre l'activité Web des utilisateurs et envoyer cette information à un serveur C2. |

| Catégorie de menaces | Mises à jour de contenu fournissant ces signatures | Description |
|---|---|---|
| | | Les protections nouvellement lancées dans cette catégorie sont rares. |
| cryptominer | Applications et menaces | (Parfois connu sous le nom de cryptojacking ou de mineurs) Détecte la tentative de téléchargement ou le trafic réseau généré par des programmes malveillants conçus pour utiliser des ressources informatiques afin de miner des cryptomonnaies à l'insu de l'utilisateur. Les binaires Cryptominer sont souvent livrés par un téléchargeur de script shell qui tente de déterminer l'architecture du système et de tuer d'autres processus de mineurs sur le système. Certains mineurs s'exécutent dans le cadre d'autres processus, tels qu'un navigateur web rendant une page web malveillante. |
| data-theft | Applications et menaces | Détecte un système qui envoie des informations à un serveur C2 connu.<br>Les protections nouvellement lancées dans cette catégorie sont rares. |
| dns | Antivirus | Détecte les requêtes DNS visant la connexion à des domaines malveillants.<br>Les signatures DNS et DNS-Wildfire détectent les mêmes domaines malveillants. Cependant, les signatures DNS sont incluses dans la mise à jour quotidienne du contenu antivirus et les signatures dns-wildfire sont incluses dans les mises à jour WildFire qui fournissent des protections toutes les 5 minutes. |
| dns-security | Antivirus | Détecte les requêtes DNS visant la connexion à des domaines malveillants.<br>dns-security comprend les signatures dns et dns-wildire, en plus des signatures uniques générées par le service de sécurité DNS. |
| dns-wildfire | WildFire ou WildFire privé | Détecte les requêtes DNS visant la connexion à des domaines malveillants.<br>Les signatures DNS et DNS-Wildfire détectent les mêmes domaines malveillants. Cependant, les signatures DNS sont incluses dans la mise à jour quotidienne du contenu antivirus et les signatures dns-wildfire sont incluses dans |

| Catégorie de menaces | Mises à jour de contenu fournissant ces signatures | Description |
|---|---|---|
| | | les mises à jour WildFire qui fournissent des protections toutes les 5 minutes. |
| téléchargeur | Applications et menaces | (Aussi connu sous le nom de droppers, stagers ou loaders) Détecte les programmes qui utilisent une connexion Internet pour se connecter à un serveur distant afin de télécharger et d'exécuter des logiciels malveillants sur le système compromis. Le cas d'utilisation le plus courant est celui d'un téléchargeur déployé comme point culminant de la ***première étape*** d'une cyber-attaque, où l'exécution de la charge utile récupérée par le téléchargeur est considérée comme la ***deuxième étape***. Les scripts shell (Bash, PowerShell, etc.), les chevaux de Troie et les documents de leurre malveillants (également appelés maldocs) tels que les fichiers PDF et Word sont des types de téléchargeurs courants. |
| fraude | Applications et menaces | (y compris le détournement de formulaires, le hameçonnage et les escroqueries) Détecte l'accès à des sites web compromis dont il a été déterminé qu'ils ont été injectés avec du code JavaScript malveillant pour recueillir des informations sensibles sur les utilisateurs. (par exemple, nom, adresse, e-mail, numéro de carte de crédit, CVV, date d'expiration) à partir des formulaires de paiement qui sont saisis sur les pages de paiement des sites de commerce électronique. |
| outil de piratage | Applications et menaces | Détecte le trafic généré par des outils logiciels qui sont utilisés par des acteurs malveillants pour effectuer une reconnaissance, attaquer ou accéder à des systèmes vulnérables, exfiltrer des données, ou créer un canal de commande et de contrôle pour contrôler subrepticement un système informatique sans autorisation. Ces programmes sont fortement associés aux logiciels malveillants et aux cyber-attaques. Les outils de piratage peuvent être déployés de manière bénigne lorsqu'ils sont utilisés dans les opérations de l'Équipe rouge et bleue, les tests de pénétration et la R&D. L'utilisation ou la possession de ces outils peut être illégale dans certains pays, quelle que soit l'intention. |
| Keylogger | Applications et menaces | Détecte les programmes qui permettent aux pirates de suivre secrètement l'activité des utilisateurs en enregistrant les touches de clavier et en enregistrant des captures d'écran. |

| Catégorie de menaces | Mises à jour de contenu fournissant ces signatures | Description |
|---|---|---|
| | | Les enregistreurs de frappe utilisent diverses méthodes C2 pour envoyer périodiquement des journaux et des rapports à une adresse électronique prédéfinie ou à un serveur C2. Par la surveillance des enregistreurs de frappe, un pirate pourrait récupérer des informations d'identification qui lui permettraient d'accéder au réseau. |
| networm | Applications et menaces | Détecte un programme qui se réplique et se propage automatiquement d'un système à l'autre. Les « net-worms » peuvent utiliser des ressources partagées ou exploiter les défaillances de sécurité pour accéder aux systèmes cibles. |
| Hameçonnage | Applications et menaces | Détecte une situation où un utilisateur tente de se connecter à une page d'hameçonnage (probablement après avoir reçu un email contenant un lien vers le site malveillant). Un site Web d'hameçonnage incite les utilisateurs à soumettre des informations d'identification qu'un pirate peut voler pour accéder au réseau.<br><br>***En plus de bloquer l'accès aux pages d'hameçonnage, activez*** Authentification multi-facteurs ***et*** Prévention contre l'hameçonnage ***pour prévenir les attaques d'hameçonnage à tous les stades.*** |
| post-exploitation | Applications et menaces | Détecte des activités qui indiquent la phase post-exploitation d'une attaque, dans le cadre de laquelle un pirate tente d'évaluer la valeur d'un système compromis. Cela peut inclure l'évaluation de la sensibilité des données stockées sur le système et de l'utilité du système pour compromettre davantage le réseau. |
| webshell | Applications et menaces | Détecte les shells web et le trafic des shells web, y compris la détection des implants et l'interaction de commande et de contrôle. Les shells web doivent d'abord être implantés par un acteur malveillant sur l'hôte compromis, le plus souvent en ciblant un serveur ou un cadre web. La communication ultérieure avec le fichier shell web permet souvent à un acteur malveillant de prendre pied dans le système, d'effectuer le dénombrement des services et du réseau, l'exfiltration des données et l'exécution du code à distance dans le contexte de l'utilisateur du serveur web. Les types de |

| Catégorie de menaces | Mises à jour de contenu fournissant ces signatures | Description |
|---|---|---|
| | | shells web les plus courants sont les scripts PHP, .NET et les scripts de balisage Perl. Les attaquants peuvent également utiliser des serveurs web infectés par un shell (les serveurs web peuvent être à la fois orientés vers Internet ou des systèmes internes) pour cibler d'autres systèmes internes. |
| spyware | Applications et menaces | Détecte la communication C2 sortante. Ces signatures sont générées automatiquement ou créées manuellement par les chercheurs de Palo Alto Networks.<br><br>***Les signatures de spyware et d'autogen détectent toutes les deux la communication C2 sortante ; cependant, les signatures autogènes sont basées sur la charge utile et peuvent détecter de manière unique les communications C2 avec des hôtes C2 inconnues ou qui changent rapidement.*** |
| **Signatures de vulnérabilités** | | |
| brute force | Applications et menaces | Une signature de force brute détecte plusieurs occurrences d'une condition au cours d'une période donnée. Bien que l'activité isolée puisse être bénigne, la signature de force brute indique que la fréquence et le taux auxquels l'activité s'est produite sont suspects. Par exemple, un échec de connexion FTP unique n'indique pas une activité malveillante. Cependant, de nombreux échecs de connexion FTP sur une courte période de temps indiquent la probabilité qu'un pirate tente de combiner des mots de passe pour accéder à un serveur FTP.<br><br>Vous pouvez régler l'action et les conditions de déclenchement pour les signatures de force brute. |
| code execution | Applications et menaces | Détecte une vulnérabilité d'exécution de code qu'un pirate peut exploiter pour exécuter du code sur un système disposant des privilèges de l'utilisateur connecté. |
| Occultation de code | Applications et menaces | Détecte le code qui a été transformé pour dissimuler certaines données tout en conservant sa fonction. Le code occulté est difficile ou impossible à lire, il est donc difficile de savoir quelles commandes le code est en train d'exécuter ou avec quels programmes il |

| Catégorie de menaces | Mises à jour de contenu fournissant ces signatures | Description |
|---|---|---|
| | | est conçu pour interagir. Le plus souvent, des acteurs malveillants dissimulent du code pour dissimuler des logiciels malveillants. Plus rarement, les développeurs légitimes peuvent dissimuler du code pour protéger la confidentialité ou la propriété intellectuelle ou pour améliorer l'expérience utilisateur. Par exemple, certains types de dissimulation (tels que la minification) réduisent la taille du fichier, ce qui diminue les temps de chargement sur le site Web et l'utilisation de la bande passante. |
| dos | Applications et menaces | Détecte une attaque par déni de service, dans le cadre de laquelle un pirate tente de rendre indisponible un système ciblé en interrompant temporairement le système et les applications et services dépendants. Pour effectuer une attaque par déni de service, un pirate peut inonder un système cible de trafic ou envoyer des informations qui entraînent son échec. Les attaques par déni de service privent les utilisateurs légitimes (tels que les employés, les membres et les titulaires de compte) du service ou de la ressource auquel ils souhaitent accéder. |
| exploit-kit | Applications et menaces | Détecte une page de renvoi d'un kit d'attaques. Les pages de renvoi d'un kit d'attaques contiennent souvent plusieurs exploits qui ciblent une ou plusieurs vulnérabilités et expositions (CVE) communes, pour plusieurs navigateurs et plugins. Étant donné que les CVE ciblés changent rapidement, les signatures des kits d'attaques se déclenchent en fonction de la page de renvoi du kit d'attaques et non des CVE.<br><br>Lorsqu'un utilisateur visite un site Web avec un kit d'attaques, ce dernier cherche les CVE ciblés et tente de fournir en mode silencieux une charge malveillante à l'ordinateur de la victime. |
| info-leak | Applications et menaces | Détecte une vulnérabilité logicielle qu'un pirate pourrait exploiter pour dérober des informations sensibles ou propriétaires. Souvent, une fuite d'informations peut se produire, car les contrôles complets n'existent pas pour protéger les données et les pirates peuvent exploiter les fuites d'informations en envoyant des requêtes spécialement construites. |

| Catégorie de menaces | Mises à jour de contenu fournissant ces signatures | Description |
|---|---|---|
| identifiants non sécurisés | Applications et menaces | Détecte l'utilisation de mots de passe faibles, compromis et par défaut du fabricant pour les logiciels, les appareils réseau et les dispositifs IdO. |
| Dépassement de capacité | Applications et menaces | Détecte une vulnérabilité de débordement dans le cadre de laquelle un pirate pourrait exploiter le manque de contrôles adéquats des requêtes. Une attaque réussie pourrait entraîner l'exécution de code à distance avec les privilèges de l'application, du serveur ou du système d'exploitation. |
| phishing | Applications et menaces | Détecte une situation où un utilisateur tente de se connecter à une page d'hameçonnage (probablement après avoir reçu un email contenant un lien vers le site malveillant). Un site Web d'hameçonnage incite les utilisateurs à soumettre des informations d'identification qu'un pirate peut voler pour accéder au réseau.<br><br>***En plus de bloquer l'accès aux pages d'hameçonnage, activez*** Authentification multi-facteurs ***et*** Prévention contre l'hameçonnage ***pour prévenir les attaques d'hameçonnage à tous les stades.*** |
| protocol-anomaly | Applications et menaces | Détecte les anomalies de protocole, lorsque le comportement d'un protocole s'écarte de l'utilisation standard et conforme. Par exemple, un paquet malformé, une application mal conçue ou une application qui s'exécute sur un port non standard sont des exemples d'anomalies de protocole et pourraient servir de techniques d'évasion. Il est recommandé de bloquer les anomalies de protocole, peu importe leur niveau de gravité. |
| sql-injection | Applications et menaces | Détecte une technique de piratage courante dans le cadre de laquelle un pirate insère des requêtes SQL dans les requêtes d'une application, afin de lire ou de modifier une base de données. Ce type de technique est souvent utilisé sur des sites Web qui ne suppriment pas complètement les données saisies par l'utilisateur. |

# Créer des exceptions de menace

Palo Alto Networks définit une action recommandée par défaut (comme bloquer ou alerter) pour les signatures de menaces. Vous pouvez utiliser un ID de menace pour exclure une signature de menaces de la mise en œuvre ou pour modifier l'action que le pare-feu applique relativement à cette signature de menaces. Par exemple, vous pouvez modifier l'action relative aux signatures de menaces qui entraînent de faux positifs sur votre réseau.

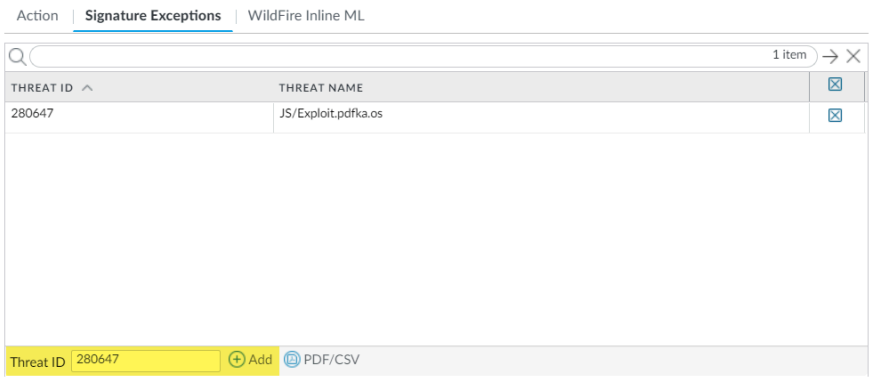
Configurez les exceptions de menace des signatures antivirus, des signatures de vulnérabilités, des signatures antispyware et des signatures DNS pour changer l'action appliquée par le pare-feu relativement à une menace. Cependant, avant de commencer, assurez-vous que le pare-feu supprime et applique les menaces selon les paramètres des signatures par défaut :

- Obtenez les dernières mises à jour des signatures antivirus, des menaces, d'applications et de WildFire.
- Effectuez le paramétrage des profils Antivirus, Antispyware et Protection contre les vulnérabilités et appliquez ces profils de sécurité à votre politique de sécurité.

**STEP 1 |** Excluez les signatures antivirus de l'application.

> ***Bien que vous puissiez utiliser un profil antivirus pour exclure des signatures antivirus de l'application, vous ne pouvez modifier l'action que le pare-feu applique relativement à une signature antivirus donnée. Vous pouvez toutefois définir l'action que le pare-feu doit appliquer sur les virus détectés dans divers types de trafic en modifiant les décodeurs (Objects (Objets) > Security Profiles (profils de sécurité) > Antivirus (Antivirus) > <antivirus-profile (profil antivirus)> > Antivirus (Antivirus)).***

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Antivirus (Antivirus)**.
2. **Add (Ajoutez)** ou modifiez un profil antivirus existant duquel vous souhaitez exclure une signature de menace, puis sélectionnez **Signature Exception (Exception de signature)**.
3. **Add (Ajoutez)** le **Threat ID (ID de menace)** de la signature de menaces que vous souhaitez exclure de l'application.

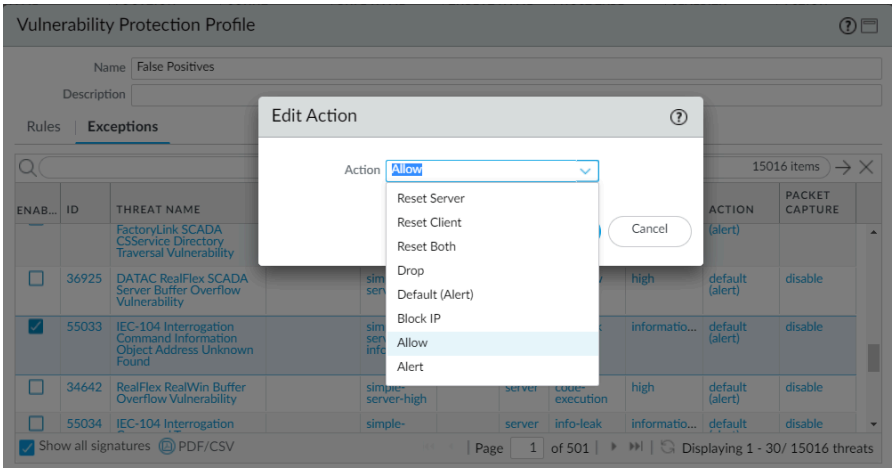



4. Cliquez sur **OK (OK)** pour enregistrer le profil antivirus.

**STEP 2 |** Modifiez l'application des signatures de protection contre les logiciels malveillants ou contre les vulnérabilités (à l'exception des signatures DNS ; passez à l'option suivante pour modifier l'application des signatures DNS, qui sont un type de signature antispyware).

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware (Antispyware)** ou **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Vulnerability Protection (Protection contre les vulnérabilités)**.
2. **Add (Ajoutez)** ou modifiez un profil antispyware ou de protection contre les vulnérabilités existant duquel vous souhaitez exclure la signature de menace, puis sélectionnez **Signature Exceptions (Exceptions de signature)** pour les profils de protection antispyware ou **Exceptions** pour les profils de protection contre les vulnérabilités.
3. **Show all signatures (Affichez toutes les signatures)**, puis appliquer un filtre pour sélectionner la signature dont vous souhaitez modifier les règles d'application.
4. Cochez la case qui se situe sous la colonne **Enable (Activer)** correspondant à la signature dont vous souhaitez modifier l'application.
5. Sélectionnez l'**Action (Action)** que vous souhaitez que le pare-feu applique relativement à cette signature de menaces.




Dans le cas des signatures que vous souhaitez exclure de l'application parce qu'elles produisent des faux positifs, définissez l'**Action (Action)** sur **Allow (Autoriser)**.

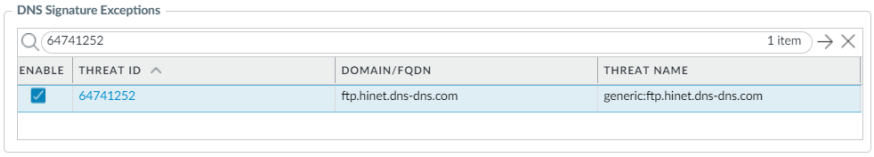
6. Cliquez sur **OK (OK)** pour enregistrer votre profil antispyware ou votre profil de protection contre les vulnérabilités, qu'il soit nouveau ou modifié.

**STEP 3 |** Modifiez l'application des signatures DNS.

Par défaut, les recherches DNS vers des noms d'hôte malveillants qui contiennent des signatures DNS sont détectées et mises en entonnoir.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware (Antispyware)**.
2. **Add (Ajoutez)** ou modifiez le profil antispyware duquel vous souhaitez exclure la signature de menaces, puis sélectionnez **DNS Exceptions (Exceptions de DNS)**.
3. Recherchez l'ID de menace DNS pour la signature de DNS que vous souhaitez exclure de l'application et cochez la case de la signature applicable :




4. Cliquez sur **OK (OK)** pour enregistrer votre profil antispyware, qu'il soit nouveau ou modifié.

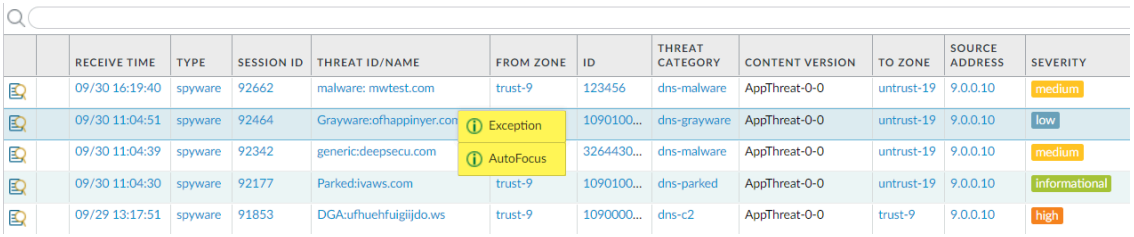
 

# Signatures personnalisées

Vous pouvez créer des signatures de menaces personnalisées pour détecter et bloquer du trafic spécifique. Lorsque le pare-feu est géré par un serveur de gestion Panorama, le ThreatID est mappé avec la menace personnalisée correspondante sur le pare-feu pour permettre au pare-feu de générer un journal des menaces rempli avec le ThreatID personnalisé configuré. Pour en savoir plus, consultez notre guide Application personnalisée et signatures de menace.

# Surveillance et obtention des rapports de menaces

Les fonctionnalités d'Archivage sécurisé des menaces et AutoFocus sont intégrées dans le pare-feu pour fournir une visibilité sur la nature des menaces détectées par le pare-feu et pour rendre une image plus complète de la façon dont un artefact s'intègre au trafic réseau de votre organisation (un artefact est une propriété, une activité ou un comportement associé à un fichier, un lien de courriel, ou une session). Vous pouvez obtenir des informations contextuelles immédiates sur une menace ou transférer votre enquête sur menaces de manière transparente du pare-feu à l'Archivage sécurisé des menaces et à AutoFocus.



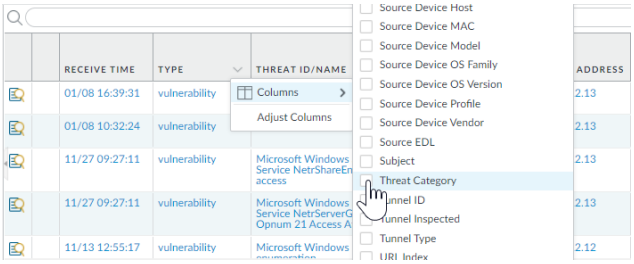

En outre, vous pouvez utiliser les Catégories de signatures de menace, qui répertorient les types d'événements de menace, pour restreindre votre vue à un certain type d'activité de menace ou pour créer des rapports personnalisés.

- Surveiller l'activité et créer des rapports personnalisés en fonction des catégories de menaces
- En savoir plus sur les signatures de menaces
- Renseignements sur les menaces pour le trafic réseau

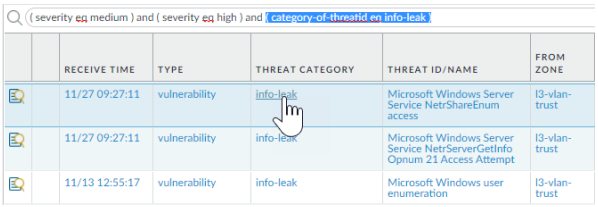
## Surveiller l'activité et créer des rapports personnalisés en fonction des catégories de menaces

Les catégories de menaces classent différents types de signatures de menaces pour vous aider à comprendre et à établir des liens entre les événements détectés par les signatures de menaces. Les catégories de menaces sont des sous-ensembles des types de signatures de menaces les plus larges: spyware, vulnérabilité, antivirus et signatures DNS. Les entrées du journal des menaces affichent la **catégorie de menace** pour chaque événement enregistré.

- Filtrer les journaux des menaces par catégorie de menace.
  1. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menace)**.
  2. Ajoutez la colonne Threat Category (Catégorie de menace) pour pouvoir afficher la Catégorie de menace pour chaque entrée de journal :

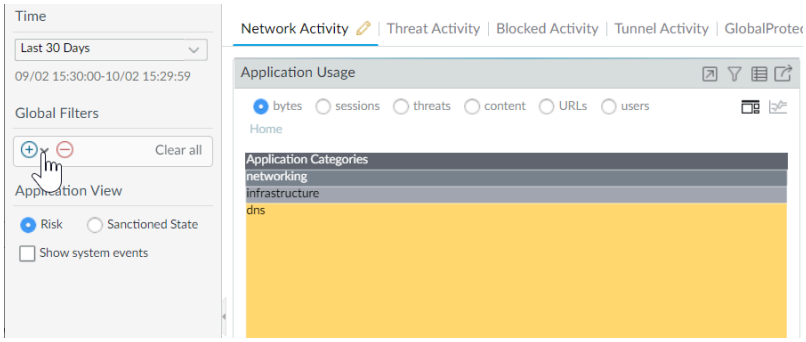



  3. Pour filtrer en fonction de la catégorie de menace :
     - Utilisez le constructeur de requête de journal pour ajouter un filtre avec l'**Attribute (Attribut)** catégorie de menace et dans le champ **Value (Valeur)**, entrez une catégorie de menace.
     - Sélectionnez la catégorie de menace de toute entrée de journal pour ajouter cette catégorie au filtre :

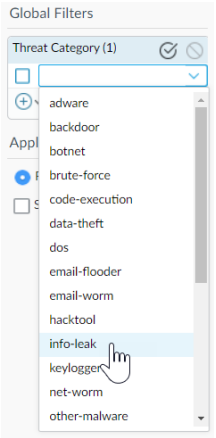


- Filtrer l'activité ACC par catégorie de menace.
  1. Sélectionnez **ACC** et ajoutez une catégorie de menace en tant que filtre général :




  2. Sélectionnez la catégorie de menace pour filtrer tous les onglets ACC.




- Créez des rapports personnalisés basés sur les catégories de menaces pour recevoir des informations sur les types spécifiques de menaces détectées par le pare-feu.
  1. Sélectionner **Monitor (Surveillance)** > **Manage Custom (Gestion Personnalisée)** des rapports pour ajouter un nouveau rapport personnalisé ou modifier un rapport existant.
  2. Choisissez la **base de données** à utiliser comme source pour le rapport personnalisé. Dans ce cas, sélectionnez **Menace** dans l'un des deux types de sources de base de données, dans les bases de données récapitulatives et dans les journaux détaillés. Les données de la base de données de synthèse sont condensées pour permettre un temps de réponse plus rapide lors de la génération de rapports. Les journaux détaillés prennent plus de temps à générer, mais fournissent un ensemble détaillé et détaillé de données pour chaque entrée de journal.
  3. Dans le Constructeur de requêtes, ajoutez un filtre de rapport avec l'attribut **Threat Category (Catégorie de menace)** et dans le champ Valeur, sélectionnez une catégorie de menace sur laquelle baser votre rapport.
  4. Pour tester les paramètres de rapport, sélectionnez **Run Now (Lancer l'exécution)**.
  5. Cliquez sur **OK** pour enregistrer le rapport.

# En savoir plus sur les signatures de menaces

Les journaux de menaces du pare-feu enregistrent toutes les menaces détectées par le pare-feu en fonction des signatures de menaces (Set Up Antivirus, Anti-Spyware, and Vulnerability Protection) et l'ACC affiche un aperçu des principales menaces sur votre réseau. Chaque événement que le pare-feu enregistre inclut un ID qui identifie la signature de menace associée.

Vous pouvez utiliser l'ID de menace trouvé avec un journal de menaces ou une entrée ACC pour :

- Vérifier facilement si une signature de menace est configurée comme une exception à votre politique de sécurité (Create Threat Exceptions).
- Trouvez les dernières informations sur le coffre-fort des menaces concernant une menace spécifique. Étant donné que l'Archivage sécurisé des menaces est intégré au pare-feu, vous pouvez visualiser les détails des menaces directement dans le contexte du pare-feu ou lancer une recherche d'Archivage sécurisé des menaces dans une nouvelle fenêtre de navigateur pour une menace enregistrée par le pare-feu.

*Si une signature a été désactivée, l'UTID de la signature pourrait être réutilisé pour une nouvelle signature.*

*Passez en revue les notes de mise à jour de contenu pour prendre connaissance des notifications concernant de nouvelles signatures et les signatures désactivées. Les signatures peuvent être désactivées dans les cas suivants : l'activité que la signature détecte n'est plus utilisée par les pirates, la signature générait un nombre considérable de faux positifs ou la signature a été regroupée avec d'autres signatures en une seule signature (optimisation de signatures).*

**STEP 1 |** Vérifier que le pare-feu est connecté à l'Archivage sécurisé des menaces.

Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifier le paramètre **Logging and Reporting (Journalisation et génération de rapports)** sur **Enable Threat Vault Access (Activer l'accès à l'archivage sécurisé des menaces)**. L'accès au coffre de menaces est activé par défaut.

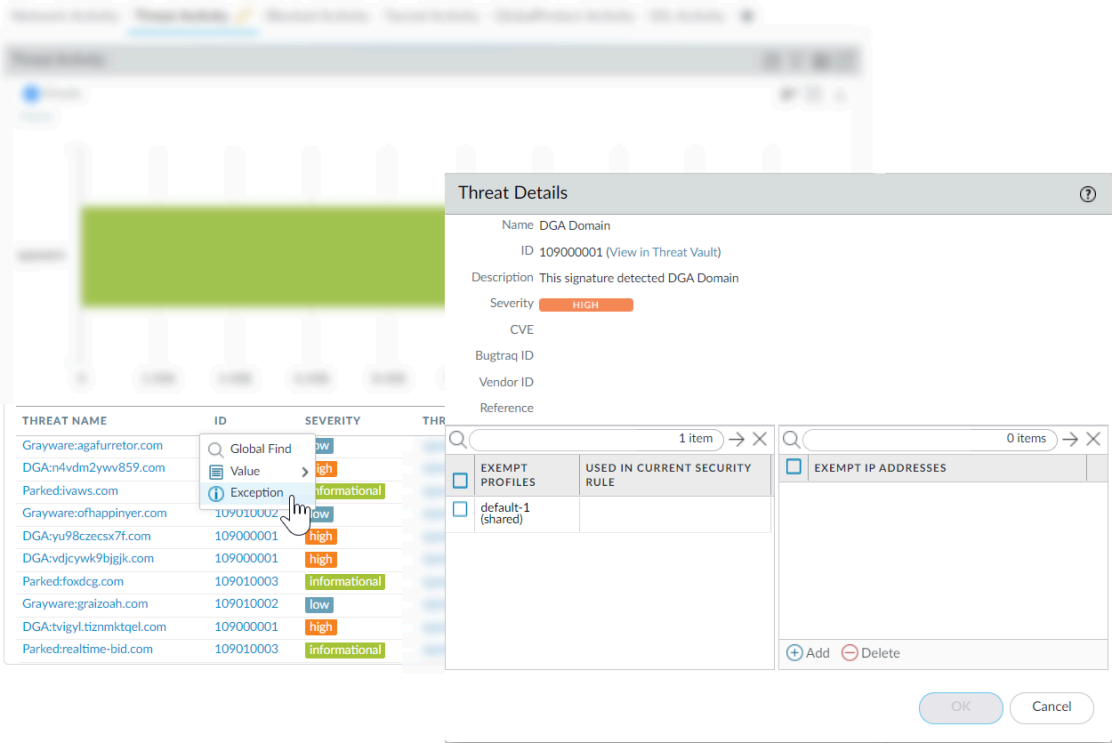
**STEP 2 |** Recherchez l'ID de menace pour les menaces détectées par le pare-feu.

- Pour voir chaque événement de menace détecté par le pare-feu en fonction des signatures de menaces, sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menaces)**. Vous pouvez trouver l'ID d'une entrée de menace répertoriée dans la colonne ID ou sélectionner l'entrée de journal pour afficher les détails du journal, y compris l'ID de menace.
- Pour afficher un aperçu des principales menaces sur le réseau, sélectionnez **ACC** > **Threat Activity (Activité de menace ACC)** et jetez un coup d'œil au widget Activité de la menace. La colonne ID affiche l'ID de menace pour chaque menace affichée.
- Pour afficher les détails des menaces que vous pouvez configurer en tant qu'exceptions de menace (le pare-feu applique la menace différemment de l'action par défaut définie pour la signature de menace), sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware/Vulnerability Protection (Protection contre les vulnérabilités Antispyware)**. **Ajoutez** ou modifiez un profil et cliquez sur l'onglet **Exceptions** pour afficher les exceptions configurées. Si aucune exception n'est configurée, vous pouvez filtrer les signatures de menaces ou sélectionner **Afficher toutes les signatures**.

**STEP 3 |** Survolez un **Threat Name (Nom de menace)** ou l'**ID** de la menace pour ouvrir la liste déroulante et cliquez sur **Exception (Exception)** pour examiner les détails de la menace et la manière dont le pare-feu est configuré pour appliquer la menace.

Par exemple, renseignez-vous sur l'une des principales menaces répertoriées sur l'ACC :




**STEP 4 |** Examiner les derniers **Threat Details (Détails de la Menace)** pour la menace et lancez une recherche dans l'Archivage sécurisé des menaces en fonction de l'ID de menace.

- Les détails sur les menaces affichées incluent les dernières informations dans l'Archivage sécurisé des menaces sur la menace, les ressources que vous pouvez utiliser pour en savoir plus sur la menace et les CVEs associés à la menace.
- Sélectionnez **View in Threat Vault (Afficher dans l'Archivage sécurisé des menaces)** pour ouvrir une recherche d'Archivage sécurisé des menaces dans une nouvelle fenêtre et rechercher les dernières informations que la base de données des menaces de Palo Alto Networks détient pour cette signature de menace.

**STEP 5 |** Vérifier si une signature de menace est configurée comme une exception à votre politique de sécurité.

- Si la colonne **Used in current security rule (Utilisé dans la règle de sécurité actuelle)** est vide, le pare-feu applique la menace en fonction de l'action de signature par défaut recommandée (par exemple, blocage ou alerte).
- Une coche dans la colonne **Used in current security rule (Utilisé dans la règle de sécurité actuelle)** indique qu'une règle de politique de sécurité est configurée pour appliquer une

action autre que la valeur par défaut pour la menace (par exemple, autoriser), en fonction des paramètres liés **Exempt Profiles (Profils exemptés)**.

*La **colonne Utilisé dans la règle de sécurité** n'indique pas si la règle de politique de sécurité est activée, uniquement si la règle de politique de sécurité est configurée avec l'exception de menace. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** pour vérifier si une règle de stratégie de sécurité indiquée est activée.*

**STEP 6 |** **Ajouter** une adresse IP sur laquelle filtrer l'exception de menace ou afficher les **Exempt IP Addresses (Adresses IP d'exemption)** existantes.

Configurez une adresse IP d'exemption pour appliquer une exception de menace uniquement lorsque la session associée a une adresse IP source ou de destination correspondante ; Pour toutes les autres sessions, la menace est appliquée en fonction de l'action de signature par défaut.

# Renseignements sur les menaces pour le trafic réseau

En détenant un abonnement valide à AutoFocus, vous pouvez comparer l'activité sur votre réseau aux plus récents renseignements sur les menace disponibles sur le portail AutoFocus. En connectant votre pare-feu à AutoFocus, vous pouvez profiter des fonctions suivantes :

- Voir un récapitulatif des renseignements sur les menaces AutoFocus pour les artefacts des sessions consignés dans les journaux du pare-feu.
- Ouvrir une recherche AutoFocus pour les artefacts des journaux du pare-feu.

Le récapitulatif des renseignements sur les menaces AutoFocus révèle la présence d'un artefact sur votre réseau et à plus grand échelle. Les verdicts WildFire et les étiquettes AutoFocus présentés pour l'artefact indiquent si ce dernier constitue un risque à la sécurité.

- Récapitulatif d'AutoFocus Intelligence
- Activation des données de renseignement sur les menaces AutoFocus
- Afficher et agir sur les données de résumé des renseignements d'AutoFocus

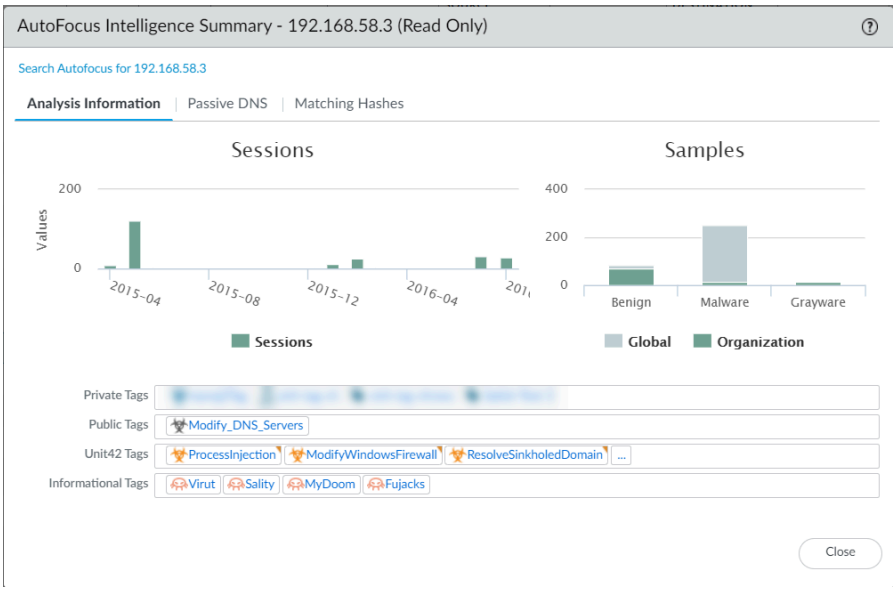
*Vous pouvez également appliquer la politique en fonction des résultats AutoFocus :*

- Exporter les artefacts AutoFocus (adresses IP, URL et domaines) et les utiliser dans une liste dynamique externe.
- Utiliser un mineur AutoFocus en tant que source de la liste dynamique externe.

## Récapitulatif d'AutoFocus Intelligence

Le récapitulatif d'AutoFocus Intelligence offre une vue centralisée des renseignements sur un artefact qu'AutoFocus a extraits des renseignements sur les menaces recueillis des autres utilisateurs d'AutoFocus, de WildFire, de la base de données de filtrage PAN-DB URL, de l'Unité 42 et des renseignements de source ouverte.




| Récapitulatif d'AutoFocus Intelligence | |
|---|---|
| Analysis information | L'onglet Analysis Information (Informations tirées de l'analyse) présente les renseignement suivants :<br>• Sessions : le nombre de sessions journalisées dans votre ou vos pare-feu pour lesquelles le pare-feu a détecté des échantillons associés à l'artefact.<br>• Échantillons : une comparaison des échantillons de l'organisation et des échantillons globaux qui sont associés à l'artefact et regroupés selon le verdict de WildFire verdict (bénin, malveillant ou indésirable). ***Global*** fait référence à des échantillons provenant de tous les envois WildFire, alors que ***organisation*** se réfère uniquement aux échantillons soumis à WildFire par votre organisation.<br>• Étiquettes correspondantes : les étiquettes AutoFocus qui correspondent à l'artefact. Les Étiquettes AutoFocus indiquent si un artefact est lié à des logiciels malveillants ou à des attaques ciblées. |
| DNS passif | L'onglet DNS passif affiche l'historique du DNS passif qui inclut l'artefact. L'historique du DNS passif se fonde sur les renseignement DNS mondiaux qui se trouvent dans AutoFocus ; il ne se limite pas à l'activité DNS de votre réseau. L'historique du DNS passif comprend :<br>• la demande de domaine;<br>• le type de demande DNS;<br>• l'adresse IP ou le domaine dont la requête DNS a pris la forme (les adresses IP privées ne s'affichent pas);<br>• le nombre de fois que la requête a été soumise; |

| Récapitulatif d'AutoFocus Intelligence | |
|---|---|
| | • la date et l'heure auxquelles la requête a été vue pour la première fois et pour la dernière fois. |
| Hachages correspondants | L'onglet Matching Hashes (Hachages correspondants) présentent les cinq échantillons correspondants qui ont été détectés le plus récemment. Parmi les informations sur les échantillons figurent :<br>• le hachage SHA256 de l'échantillon;<br>• le type de fichier échantillon;<br>• la date et l'heure auxquelles WildFire a analysé un échantillon et lui a affecté un verdict de WildFire;<br>• le verdict de WildFire affecté à l'échantillon;<br>• la date et l'heure auxquelles WildFire a mis à jour le verdict de WildFire pour l'échantillon (le cas échéant). |

## Activation des données de renseignement sur les menaces AutoFocus

Activez la licence AutoFocus et activez la communication entre le pare-feu et AutoFocus. Une fois que vous êtes prêt, vous serez en mesure d'afficher le Récapitulatif d'AutoFocus Intelligence d'un journal ou d'un artefact ACC afin d'évaluer sa présence dans votre réseau et les menaces connexes.

**STEP 1 |** Vérifiez que la licence AutoFocus est activée sur le pare-feu.

1. Sélectionnez **Device (Périphérique)** > **Licenses (Licences)** pour vous assurer que la licence AutoFocus du périphérique est installée et valide (vérifiez la date d'expiration).
2. Si le pare-feu n'affiche pas la licence, reportez-vous à la section Activation des licences d'abonnement.

**STEP 2 |** Connectez le pare-feu à AutoFocus.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les AutoFocus Settings (Paramètres d'AutoFocus).
2. Saisissez la **AutoFocus URL (URL AutoFocus)** :

   **`https://autofocus.paloaltonetworks.com:10443`**
3. Servez-vous du **Query Timeout (Délai d'expiration des requêtes)** pour régler la durée pendant laquelle le pare-feu peut tenter d'effectuer une requête auprès d'AutoFocus pour obtenir les renseignement sur les menaces. Si le portail AutoFocus ne répond pas avant la fin de la période spécifiée, le pare-feu met fin à la connexion.

   *Il est recommandé de définir le délai d'expiration des requêtes sur la valeur par défaut de 15 secondes. Les requêtes AutoFocus sont optimisées de sorte à être effectuées au cours de ce délai.*
4. Sélectionnez **Enabled (Activé)** pour permettre au pare-feu de se connecter à AutoFocus.
5. Cliquez sur **OK**.
6. **Commit (Validez)** les changements que vous avez apportés pour conserver les paramètres d'AutoFocus lors du redémarrage.

**STEP 3 |** Connectez AutoFocus au pare-feu.

1. Connectez-vous au portail AutoFocus : https://autofocus.paloaltonetworks.com
2. Sélectionnez **Settings (Paramètres)**.
3. **Add new (Ajoutez de nouveaux)** systèmes distants.
4. Saisissez un **Name (Nom)** descriptif pour identifier le pare-feu.
5. Sélectionnez **PanOS (PanOS)** comme System Type (Type de système).
6. Saisissez l'**Address (Adresse) IP** du pare-feu.
7. Cliquez sur **Save changes (Enregistrer les changements)** pour ajouter le système distant.
8. Cliquez de nouveau sur **Save changes (Enregistrer les changements)** à la page Settings (Paramètres) pour vous assurer que le pare-feu est ajouté avec succès.

**STEP 4 |** Testez la connexion entre le pare-feu et AutoFocus.

1. Sur la pare-feu, sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)**.
2. Vérifiez que vous pouvez Évaluer les artefacts de pare-feu avec AutoFocus.

## Afficher et agir sur les données de résumé des renseignements d'AutoFocus

Interagissez avec le résumé des renseignements d'AutoFocus pour afficher plus d'informations sur un artefact, ou étendez votre recherche d'artefacts à AutoFocus. Les étiquettes AutoFocus révèlent si l'artefact est associé à certains types de logiciels ou comportements malveillants.

**STEP 1 |** Confirmez que le pare-feu est connecté à AutoFocus.

Activez les renseignements sur les menaces d'AutoFocus sur le pare-feu (abonnement AutoFocus actif requis).

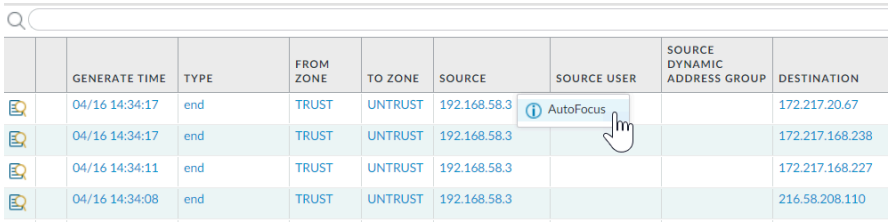
**STEP 2 |** Trouvez des artefacts sur lesquels enquêter.

Vous pouvez afficher un résumé de renseignements d'AutoFocus pour des artefacts lorsque vous :

- Affichez des journaux (le Trafic, les Menaces, le Filtrage des URL, les Envois WildFire, le Filtrage des données et les Journaux unifiés uniquement).
- Affichez les entrées de la liste dynamique externe.

**STEP 3 |** Placez le curseur sur un artefact pour ouvrir le menu déroulant, puis cliquez sur **AutoFocus**.




Le résumé des renseignements d'AutoFocus est uniquement disponible pour les types d'artefacts suivants :

Adresse IP

URL

Domain (Domaine)

User-Agent

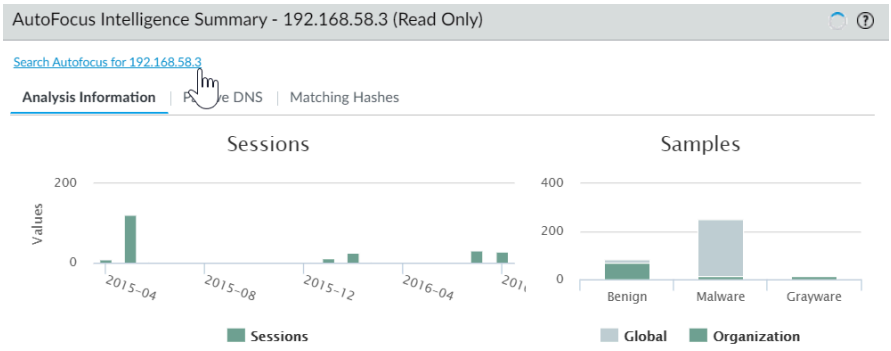
nom de la menace (uniquement pour les menaces des sous-types de virus et du virus détectés par WildFire) ;

Nome de fichier

Hachage SHA-256

**STEP 4 |** Lancez une recherche AutoFocus pour l'artefact pour lequel vous avez ouvert le résumé des renseignements d'AutoFocus.

Cliquez sur le lien **Search AutoFocus for... (Rechercher sur AutoFocus...)** au sommet de la fenêtre de résumé des renseignements d'AutoFocus. Les résultats de la recherche comprennent tous les échantillons associés à l'artefact. Basculez entre les onglets **My Samples (Mes échantillons)** et **All Samples (Tous les échantillons)** et comparez le nombre d'échantillons pour déterminer le niveau de présence de l'artefact dans votre organisation.



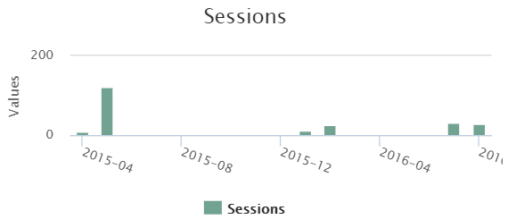
**STEP 5 |** Lancez une recherche AutoFocus pour les autres artefacts dans le résumé des renseignements d'AutoFocus.

Cliquez sur les artefacts suivants pour déterminer leur niveau de présence dans votre organisation :

- Les verdicts WildFire dans l'onglet Informations d'analyse
- Les URL et adresses IP dans l'onglet DNS passif
- Les hachages SHA256 dans l'onglet Hachages correspondants

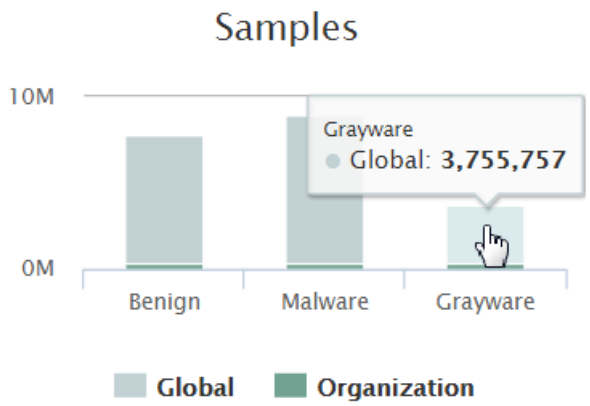
**STEP 6 |** Affichez le nombre de sessions associées à l'artefact dans votre organisation par mois.

Survolez les barres de session.




**STEP 7 |** Affichez le nombre d'échantillons associés à l'artefact par portée et verdict WildFire.

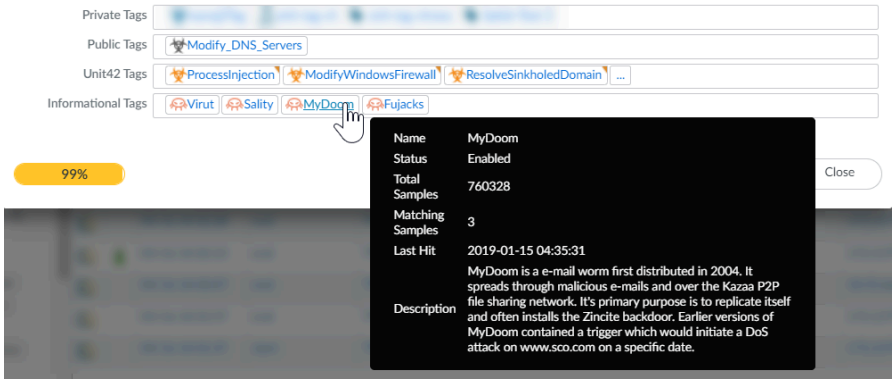
Survolez les barres d'échantillon.



**STEP 8 |** Affichez plus de détails sur la correspondance avec les tags AutoFocus.

Placez le curseur sur un tag correspondant pour afficher la description du tag et d'autres détails concernant le tag.




**STEP 9 |** Affichez les autres échantillons associés à un tag correspondant.

Cliquez sur un tag correspondant pour lancer une recherche AutoFocus pour ce tag. Les résultats de la recherche comprennent tous les échantillons correspondant au tag.

Les tags de l'Unité 42 identifient les menaces et les campagnes constituant un risque direct relatif à la sécurité. Cliquez sur un tag de correspondance de l'Unité 42 pour voir combien d'échantillons de votre réseau sont associés à la menace que le tag identifie.

**STEP 10 |** Trouvez plus de tags correspondants pour un artefact.

Cliquez sur le symbole de points de suspension ( ... ) pour lancer une recherche AutoFocus pour l'artefact. La colonne Tags dans les résultats de recherche affiche plus de tags correspondants pour l'artefact, ce qui vous donne une idée des autres logiciels malveillants, comportements malveillants, acteurs de menace, exploits ou campagnes pour lesquels l'artefact est souvent détecté.

# Partage de Données de Prévention des Menaces avec Palo Alto Networks

La télémétrie est le processus de collecte et de transmission des données à analyser. Lorsque vous activez la télémétrie sur le pare-feu, le pare-feu collecte et transmet régulièrement les données qui contiennent des informations sur les applications, les menaces, et l'état des périphériques vers Palo Alto Networks. Partager des données de prévention des menaces apporte les bénéfices suivants :

- Des signatures de surveillance de logiciels espion et de vulnérabilités renforcées sont fournies à tous ses clients à échelle mondiale. Par exemple, lorsqu'une menace particulière déclenche des signatures de surveillance de vulnérabilité ou de logiciel espion, le pare-feu partage les URL associés avec cette menace avec l'équipe de recherche de menaces Palo Alto Networks, pour qu'elle puisse classer ces URL comme malveillantes.
- L'exécution de tests rapides et d'évaluation de signatures de surveillance de menaces, sans impact sur votre réseau, afin que les signatures de surveillance de menaces critiques soient rendues accessibles à tous les clients de Palo Alto Networks plus rapidement.
- Précision et détection des codes malveillants accrues au sein du Filtrage des URL PAN-DB, des signatures (C2) de commande et de contrôle basées sur DNS, et de Wildfire.

Palo Alto Networks utilise les données de prévention des menaces issues de la télémétrie pour les rendre accessibles à tous les utilisateurs de Palo Alto Networks. Tous les utilisateurs de Palo Alto Networks bénéficient des données que chaque participant à la télémétrie partage, ce qui fait de la télémétrie une approche communautaire pour la prévention des menaces. Palo Alto Networks ne partage pas vos données de télémétrie avec d'autres clients ou d'autres organisations tierces.

Pour en savoir plus sur la télémétrie, y compris ses avantages, ses utilisations et sa configuration, consultez la section Télémétrie du périphérique.

# Ressources de prévention des menaces

Pour plus d'informations sur les meilleures pratiques de prévention des menaces, reportez-vous aux sources suivantes :

- Création de signatures de menaces personnalisées
- Meilleures pratiques pour sécuriser votre réseau contre les fuites au niveau des couches 4 et 7
- Bonnes pratiques en matière de filtrage des URL
- Meilleures pratiques du Zero Trust
- Protection DoS et Protection de Zones Respectant les Bonnes Pratiques

Pour afficher une liste des menaces et applications que les produits Palo Alto Networks peuvent identifier, consultez les liens ci-dessous :

- Applipedia : fournit des informations sur les applications que Palo Alto Networks peut identifier.
- Archivage sécurisé des menaces: répertorie les menaces que les produits Palo Alto Networks peuvent identifier. Vous pouvez rechercher des menaces par vulnérabilité, logiciel espion ou virus. Cliquez sur l'icône Détails en regard du numéro d'identification pour plus d'informations sur une menace.

# Déchiffrement

Les pare-feu Palo Alto Networks peuvent déchiffrer et inspecter le trafic pour procurer une visibilité des menaces et pour contrôler les protocoles, la vérification des certificats et la gestion des échecs. Le déchiffrement pour appliquer des politiques sur le trafic chiffré pour que le pare-feu gère le trafic chiffré conformément aux paramètres de sécurité que vous avez configurés. Déchiffrez le trafic pour empêcher des contenus malveillants chiffrés d'entrer sur votre réseau et des contenus sensibles de sortir de votre réseau, en étant dissimulés dans un trafic crypté. L'activation du décryptage peut inclure la préparation des clés et des certificats nécessaires pour le décryptage, la création de profils et de politiques de décryptage et la configuration du miroir du port de décryptage.

# Présentation du décryptage

Les protocoles de chiffrement Secure Sockets Layer (SSL) et Secure Shell (SSH) sont utilisés pour sécuriser le trafic entre deux entités, telles qu'un serveur Web et un client. SSL et SSH encapsulent le trafic, en cryptant les données de manière à ce qu'elles soient insignifiantes pour des entités autres que le client et le serveur avec les certificats pour affirmer la confiance entre les périphériques et les clés pour décoder les données. Déchiffrez le trafic SSL et SSH pour :

- Empêcher les logiciels malveillants dissimulés dans le trafic crypté de s'introduire à l'intérieur de votre réseau. Par exemple, un pirate compromet un site Web qui utilise le chiffrement SSL. Les employés visitent ce site Web et, sans le savoir, télécharge une exploitation ou un fichier malveillant. Le fichier malveillant utilise ensuite le terminal infecté de l'employé pour se déplacer latéralement à l'intérieur du réseau et compromettre d'autres systèmes.
- Empêcher les informations sensibles de transiter à l'extérieur du réseau.
- Garantir que les applications appropriées fonctionnent sur un réseau sécurisé.
- Déchiffrer le trafic de manière sélective. Par exemple, créez une politique et un profil de déchiffrement pour exclure le trafic des sites financiers ou relatifs à la santé du déchiffrement.

Le décryptage du pare-feu Palo Alto Networks est basé sur une politique et peut décrypter, inspecter et contrôler les connexions SSL et SSH entrantes et sortantes. Une politique de déchiffrement vous permet de préciser le trafic selon la destination, la source, le service ou la catégorie d'URL et de bloquer, de restreindre ou de transmettre le trafic précisé selon les paramètres de sécurité du profil de déchiffrement associé. Un profil de déchiffrement contrôle les protocoles SSL, la vérification des certificats et les vérifications des échecs pour empêcher le trafic qui utilise des algorithmes faibles ou des modes non pris en charge d'accéder au réseau. Le pare-feu utilise les certificats et les clés pour décrypter le trafic en texte brut, puis applique App-ID et les paramètres de sécurité au trafic de texte brut, y compris les profils Décryptage, Antivirus, Vulnérabilité, Antispyware, Filtrage des URL, WildFire et Blocage des fichiers. Une fois que le trafic est décrypté et inspecté, le pare-feu chiffre de nouveau le trafic en texte brut dès sa sortie du pare-feu pour garantir la confidentialité et la sécurité.

Le pare-feu fournit trois types de règle de stratégie de décryptage : Proxy de transfert SSL pour contrôler le trafic SSL sortant, Inspection SSL entrante pour contrôler le trafic SSL entrant et Proxy SSH pour contrôler le trafic par tunnel SSH. Vous pouvez associer un profil de déchiffrement à une règle de politique pour appliquer des paramètres d'accès granulaires au trafic, comme les vérifications des certificats du serveur, les modes non pris en charge et les échecs.

Le déchiffrement SSL (du proxy de transfert et inspection entrante) exige des certificats pour établir le pare-feu comme un tiers de confiance et pour établir la confiance entre un client et un service afin de sécuriser la connexion SSL/TLS. Vous pouvez également utiliser des certificats lors de l'exclusion des serveurs du déchiffrement SSL pour des raisons techniques (le site interrompt le déchiffrement pour des raisons telles que l'épinglage des certificats, des suites de chiffrement non prises en charge ou l'authentification mutuelle). Le décryptage SSH ne nécessite pas de certificats.

***Utilisez la** liste de contrôle des meilleures pratiques en matière de déchiffrement **pour planifier, mettre en œuvre et préserver votre déploiement de déchiffrement.***

Vous pouvez intégrer un module de sécurité matériel avec un pare-feu pour activer la sécurité renforcée pour les clés privées utilisées dans le décryptage du proxy de transfert SSL et l'inspection

SSL entrante. Pour en savoir plus sur le stockage et la génération des clés en utilisant un module de sécurité matériel et en intégrant un module de sécurité matériel à votre pare-feu, reportez-vous à la section Sécurisation des clés avec un module de sécurité matériel.

Vous pouvez également utiliser la mise en miroir du déchiffrement pour transférer le trafic déchiffré vers une solution tierce en vue d'une analyse supplémentaire et de l'archivage.

***Si vous activez la mise en miroir du déchiffrement, soyez au fait des lois et des règlements locaux qui précisent le trafic que vous mettre en miroir et l'endroit et la manière de stocker le trafic, car tout le trafic mis en miroir, y compris les informations sensibles, est transmis en texte clair.***

# Concepts du décryptage

Passez en revue les rubriques suivantes pour en apprendre davantage sur le support et les caractéristiques de déchiffrement :

- Clés et certificats pour les politiques de décryptage
- Proxy de transfert SSL
- Profil de décryptage du proxy de transfert SSL
- Inspection SSL entrante
- Profil de décryptage d'inspection entrante SSL
- Paramètre des profil de décryptage SSL
- Proxy SSH
- Profil de décryptage SSL
- Profil SSL pour le non décryptage
- Décryptage SSL avec certificats ECC (Elliptical Curve Cryptography, cryptographie à courbe elliptique).
- Prise en charge de Perfect Forward Secrecy (Confidentialité de transmission parfaite ; PFS) pour le décryptage SSL
- Déchiffrement SSL et Subject Alternative Names (Autres noms de l'objet ; SAN)
- Décryptage TLSv1.3
- Support haute disponibilité pour les sessions déchiffrées
- Mise en miroir du décryptage

## Clés et certificats pour les politiques de décryptage

Les clés sont des chaînes de nombres qui sont normalement générés en utilisant une opération mathématique impliquant des nombres aléatoires et des grands nombres premiers. Les clés transforment des chaînes, telles que les mots de passe et les secrets partagés, à partir d'un texte brut non chiffré en un cryptogramme chiffré et à partir d'un cryptogramme chiffré en un texte brut déchiffré. Les clés peuvent être symétriques (la même clé est utilisée pour crypter et décrypter) ou asymétriques (une clé est utilisée pour le cryptage et une clé mathématiquement liée est utilisée pour le décryptage). N'importe quel système peut générer une clé.

Les certificats X.509 établissent une relation de confiance entre un client et un serveur afin d'établir une connexion SSL. Un client qui tente d'authentifier un serveur (ou un serveur authentifiant un client) connaît la structure du certificat X 509 et sait par conséquent comment extraire des informations d'identification concernant le serveur à partir des champs du certificat, telles que son nom de domaine complet (FQDN) ou adresse IP (appelé ***nom commun*** ou ***CN*** du certificat) ou le nom de l'organisation, du département, ou de l'utilisateur pour qui le certificat a été généré. Une Certificate Authority (autorité de certification - CA) doit émettre tous les certificats. Une fois que l'AC a vérifié un client ou un serveur, l'AC génère le certificat et le signe en utilisant sa clé privée.

*Si vous avez deux CA (**Device (Périphérique) > Certificate Management (Gestion des certificats) > Device Certificates (Certificats du périphérique)**) ayant le même objet et la même clé et que l'une des CA expire, supprimez (option personnalisée) ou désactivez (option prédéfinie) la CA expirée. Si vous décidez de ne pas supprimer ou désactiver une CA expirée, le pare-feu peut bâtir une chaîne vers la CA expirée si elle est activée dans la chaîne de confiance, ce qui entraîne une page de blocage.*

Lorsque vous appliquez une politique de déchiffrement au trafic, une session entre le client et le serveur est établie uniquement si le pare-feu approuve l'AC qui a signé le certificat du serveur. Pour établir une relation de confiance, le pare-feu doit comprendre le certificat AC racine du serveur dans sa liste d'approbation de certificats (CTL) et utiliser la clé publique contenue dans ce même certificat AC racine pour vérifier la signature. Le pare-feu présente ensuite une copie du certificat du serveur signé par le certificat d'approbation de transfert pour que le client s'authentifie. Vous pouvez aussi configurer le pare-feu pour utiliser une AC d'entreprise comme certificat d'approbation de transfert pour le proxy de transfert SSL. Si le pare-feu ne comprend pas le certificat AC racine du serveur dans sa liste CTL, le pare-feu présente une copie du certificat du serveur signé par le certificat de non-approbation de transfert au client. Le certificat de non-approbation de transfert garantit que les clients sont informés par un avertissement de certificat lors des tentatives d'accès aux sites hébergés par un serveur avec des certificats non approuvés.

Pour plus d'informations sur les certificats, reportez-vous à la section Gestion des certificats.

*Pour contrôler les autorités de certification (AC) de confiance que votre périphérique approuve, utilisez l'onglet **Device (Périphérique) > Certificate Management (Gestion des certificats) > Certificates (Certificats) > Default Trusted Certificate Authorities (Autorités de certification de confiance par défaut)** sur l'interface Web du pare-feu.*

Le tableau suivant répertorie les différents certificats utilisés par les pare-feu Palo Alto Networks pour le déchiffrement.

| Certificats utilisés avec le décryptage | Description |
|---|---|
| Approbation de transfert (Utilisée pour le déchiffrement de proxy de transfert SSL) | Il s'agit du certificat que le pare-feu présente aux clients durant le décryptage si le site auquel le client tente de se connecter dispose d'un certificat qui est signé par une AC que le pare-feu approuve. Pour configurer le certificat d'approbation de transfert que le pare-feu pourra présenter aux clients lorsque le certificat du serveur est signé par une CA approuvée, reportez-vous à la section Configuration du proxy de transfert SSL.<br><br>Par défaut, le pare-feu détermine la taille de clé à utiliser pour le certificat client en fonction de la taille de clé du certificat du serveur de destination. Cependant, vous pouvez configurer la taille de la clé pour les certificats de serveur proxy de transfert SSL. Pour plus de sécurité, songez à stocker la clé privée associée au certificat d'approbation de transfert sur un module de sécurité matériel (reportez-vous à la section Stocker les clés privées sur un HSM). |

| Certificats utilisés avec le décryptage | Description |
|---|---|
| | *Sauvegardez la clé privée associée au certificat CA d'approbation de transfert du pare-feu (pas la clé principale du pare-feu) dans un registre sécuritaire. Ainsi, si un problème se produit avec le pare-feu, vous pouvez toujours accéder au certificat CA d'approbation de transfert. Pour plus de sécurité, songez à stocker la clé privée associée au certificat d'approbation de transfert sur un module de sécurité matériel (reportez-vous à la section* Stocker les clés privées sur un HSM*).* |
| Non-approbation de transfert (Utilisée pour le déchiffrement de proxy de transfert SSL) | Il s'agit du certificat que le pare-feu présente aux clients durant le décryptage si le site auquel le client tente de se connecter dispose d'un certificat qui est signé par une AC que le pare-feu n'approuve pas. Pour configurer un certificat de non-approbation de transfert sur le pare-feu, reportez-vous à la section Configuration du proxy de transfert SSL. |
| Inspection SSL entrante | Les certificats des serveurs sur votre réseau pour lesquels vous voulez effectuer l'inspection SSL entrante de n'importe quel serveur si vous chargez le certificat du serveur sur le pare-feu). Importez les certificats du serveur sur le pare-feu. |

| Certificats utilisés avec le décryptage | Description |
| --- | --- |
| | *À compter de PAN-OS 8.0, les pare-feu utilisent l'algorithme Elliptic-Curve Diffie-Hellman Ephemeral (Diffie-Hellman basé sur les courbes elliptiques éphémères ; ECDHE) pour effectuer une vérification stricte des certificats. C'est donc dire que si le pare-feu utilise un certificat intermédiaire, vous devez réimporter le certificat sur le pare-feu à partir du site Web après avoir effectué la mise à niveau vers PAN-OS 8.0 ou une version ultérieure et associer le certificat du serveur avec le certificat intermédiaire (installation d'un certificat en chaîne). Autrement, les sessions d'inspection SSL entrante qui possède un certificat intermédiaire dans la chaîne échoueront. Pour installer un certificat en chaîne :*<br>**1.** *Ouvrez chaque fichier de certificat (.cer) dans éditeur de texte, tel que le Bloc-notes.*<br>**2.** *Collez chaque certificat de bout en bout avec le certificat du serveur au haut et chaque signataire inclus au bas.*<br>**3.** *Enregistrez le fichier en tant que texte (.txt) ou certificat (.cer) (le nom du fichier ne peut pas contenir d'espaces).*<br>**4.** *Importez le certificat combiné (en chaîne) sur le pare-feu.* |

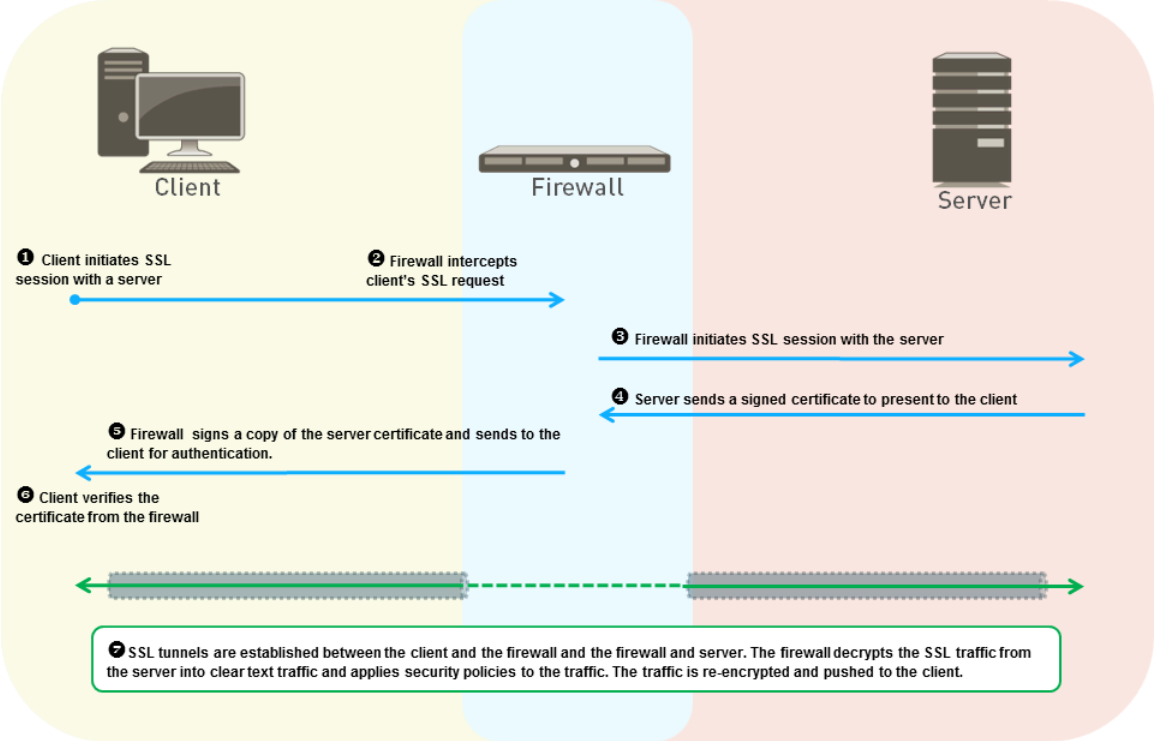
## Proxy de transfert SSL

Lorsque vous configurez le pare-feu pour qu'il déchiffre le trafic SSL destiné à des sites externes, il fonctionne comme un serveur de proxy de transfert SSL. Utilisez une politique de décryptage de proxy de transfert SSL pour décrypter et inspecter le trafic SSL/TLS des utilisateurs internes vers le Web. Le déchiffrement de proxy de transfert SSL empêche le fichier malveillant dissimulé en tant que trafic chiffré SSL d'entrer dans votre réseau d'entreprise en le déchiffrant de sorte que le pare-feu puisse appliquer des profils de décryptage, des stratégies de sécurité et des profils au trafic.

Avec le déchiffrement de proxy de transfert SSL, le pare-feu est un homme au milieu entre le client interne et le serveur externe. Le pare-feu utilise des certificats pour présenter de nouveau le client au serveur de manière transparente et pour présenter de nouveau le serveur au client de manière transparente, de sorte que le client pense communiquer directement avec le serveur (même si la session du client s'effectue avec le pare-feu) et le serveur croit qu'il communique directement avec le client (même si la session du serveur s'effectue également avec le pare-feu). Le pare-feu utilise des certificats pour s'établir comme tierce partie de confiance (personne au milieu) pour la session client-serveur (pour des détails sur les certificats, voir les politiques de déchiffrement des clés et des certificats).

La figure suivante illustre ce processus en détail. Reportez-vous à la section Configuration du proxy de transfert SSL pour plus d'informations sur la configuration du proxy de transfert SSL.




1. Le client interne de votre réseau tente de lancer une session TLS avec un serveur externe.
2. Le pare-feu intercepte la demande de certificat SSL du client. Pour le client, le pare-feu joue le rôle de serveur externe, même si la session sécurisée en cours d'établissement se fait avec le pare-feu et non avec le serveur réel.
3. Le pare-feu transmet ensuite la demande de certificat SSL du client au serveur pour lancer une session distincte avec le serveur. Pour le serveur, le pare-feu ressemble au client, le serveur ne sait pas qu'il y a un intermédiaire et le serveur vérifie le certificat.
4. Le serveur envoie au pare-feu un certificat signé qui est destiné au client.
5. Le pare-feu analyse le certificat du serveur. Si le certificat de serveur est signé par une autorité de certification approuvée par le pare-feu et qu'il respecte les politiques et les profils que vous avez configurés, le pare-feu génère une copie d'approbation SSL du certificat de serveur et l'envoie au client. Si le certificat du serveur est signé par un AC auquel le pare-feu ne fait pas confiance, le pare-feu génère une copie SSL Untrust du certificat du serveur et l'envoie au client. La copie de certificat que le pare-feu génère et envoie au client contient les extensions du certificat de serveur d'origine et est appelée ***imitation*** de certificat car ce n'est pas le certificat réel du serveur. Si le pare-feu ne fait pas confiance au serveur, le client voit un message d'avertissement sur la page de bloc indiquant que le site auquel il tente de se connecter n'est pas fiable, et si vous permettez aux utilisateurs de se désabonner du décryptage SSL, le client peut choisir d'aller de l'avant ou de mettre fin à la session.
6. Le client vérifie le certificat d'emprunt d'identité du pare-feu. Le client initie ensuite un échange de clés de session avec le serveur, auquel le pare-feu envoie un proxy de la même manière que les certificats. Le pare-feu transmet la clé client au serveur et crée une copie d'emprunt d'identité pour le client, de sorte que le pare-feu reste un proxy « invisible ». Le client et le serveur croient que leurs sessions sont établies entre eux, mais deux sessions séparées demeurent, l'une entre le client et le pare-feu et l'autre entre le pare-feu et le serveur. Désormais, toutes les parties disposent des certificats et des clés nécessaires et le pare-feu peut déchiffrer le trafic.

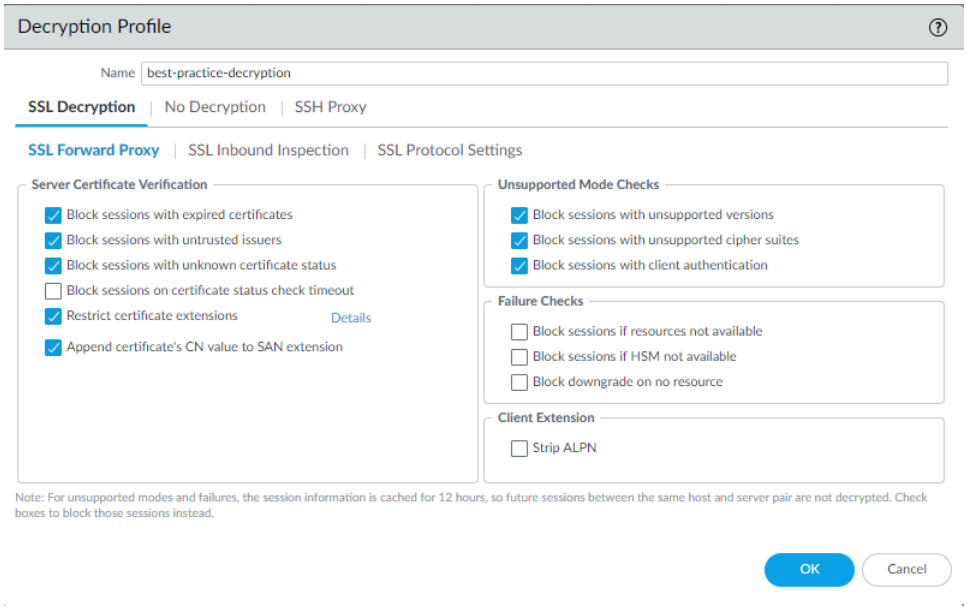
 

7. Tout le trafic de session SSL passe par le pare-feu de manière transparente entre le client et le serveur. Le pare-feu déchiffre le trafic SSL, applique des politiques de sécurité, des profils et des profils de déchiffrement au trafic, chiffre de nouveau le trafic, puis le transmet.

*Lorsque vous configurez le proxy de transfert SSL, le trafic proxy ne prend pas en charge les points de code DSCP ou QoS.*

## Profil de décryptage du proxy de transfert SSL

Le profil de décryptage de transfert SSL (**Objects (Objets)** > **Decryption Profile (Profil de décryptage)** > **SSL Decryption (Décryptage SSL)** > **SSL Forward Proxy (Proxy de transfert SSL)**) contrôle la vérification du serveur, les vérifications en mode session et les vérifications d'échec pour le trafic SSL/TLS sortant défini dans les stratégies de décryptage du proxy de transfert auxquelles vous associez le profil. La figure suivante illustre les recommandations générales en matière de meilleures pratiques pour les paramètres du profil de décryptage de proxy de transfert, mais les paramètres que vous utilisez dépendent également des règles de conformité de la sécurité de votre entreprise, ainsi que des lois et réglementations locales. Il existe également des meilleures pratiques spécifiques pour le périmètre des profils de décryptage de passerelle Internet et des profils de décryptage de centre de données.

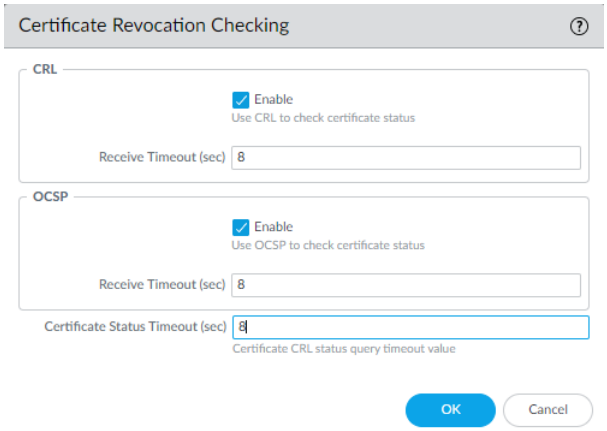



### Vérification des certificats du serveur

- **Bloquer les sessions avec des certificats expirés** : cochez toujours cette case pour bloquer des sessions comportant des serveurs dont les certificats sont expirés et pour empêcher l'accès à des sites potentiellement peu sûrs. Si vous ne cochez pas cette case, les utilisateurs peuvent se connecter à des sites malveillants et transiger avec eux de même que voir des messages d'avertissement lorsqu'ils tentent de se connecter. Rien n'empêche alors la connexion de se produire.
- **Block les sessions avec des émetteurs non approuvés** : cochez toujours cochez cette case pour bloquer les sessions avec des serveurs qui possèdent des émetteurs de certificats non approuvés. Un émetteur non approuvé peut indiquer une attaque d'homme au milieu, une attaque par répétition, ou autre attaque.

- **Bloquer les sessions dont l'état du certificat est inconnu** : bloque la session SSL/TLS lorsque l'état de révocation de certificat du serveur est renvoyé avec la mention « inconnu ». Étant donné que plusieurs raisons peuvent expliquer que l'état du certificat soit inconnu, pour assurer la sécurité générale du déchiffrement, le fait de cocher la case renforce généralement la sécurité. Toutefois, dans les zones de sécurité plus élevées du réseau, telles que le centre de données, cochez cette case.
- **Bloquer les sessions lorsque le délai de vérification de l'état du certificat est dépassé** : la décision de bloquer les sessions si la vérification de l'état expire dépend de la positon de votre entreprise à l'égard de la conformité de la sécurité, car il s'agit d'un compromis entre une sécurité renforcée et une meilleure expérience utilisateur. La vérification du statut du certificat examine la liste de révocations de certificat (CRL) sur un serveur de révocation ou utilise un Online Certificate Status Protocol (OCSP) pour savoir si l'autorité de certification émettrice (CA) a révoqué le certificat et si le certificat n'est pas digne de confiance. Toutefois, les serveurs de révocation peuvent tarder à répondre, pouvant occasionner l'expiration de la session et le blocage de la session par le pare-feu même si le certificat est valide. Si vous **Bloquez les sessions à expiration du délai de vérification du certificat** et que le serveur de révocation tarde à répondre, vous pouvez utiliser **Device (Périphérique)** > **Setup (Configuration)** > **Session** > **Decryption Settings (Paramètres de Décryptage)** et la **Vérification de Révocation de Certificat** pour changer le délai d'expiration de cinq secondes par défaut pour une autre valeur. Par exemple, vous pouvez augmenter la valeur du délai d'attente à huit secondes, comme indiqué dans la figure suivante. Autorisez aussi bien la vérification de révocation de certificat par CRL que par OCSP car les serveurs de certificats peuvent contenir l'URL CRL dans l'extension du point de distribution CRL (CDP) ou l'URL OCSP dans l'extension de certificat Authority Information Access (AIA).




- **Restreindre les extensions de certificat** : cochez cette case limite les extensions de certificat du certificat de serveur à l'utilisation de la clé et à l'utilisation de la clé étendue et bloque les certificats comportant d'autres extensions. Toutefois, dans certains déploiements, d'autres extensions de certificat peuvent être nécessaires. Cochez seulement cette case si votre déploiement ne nécessite aucune autre extension de certificat.
- **Ajouter la valeur CN du certificat à l'extension SAN** : cochez cette case pour garantir que lorsqu'un navigateur requiert un certificat de serveur pour utiliser un nom de substitution d'objet (SAN) et ne prend pas en charge la correspondance de certificat basée sur le nom commun (CN), si le certificat n'a pas d'extension SAN, les utilisateurs peut toujours accéder aux ressources Web demandées car le pare-feu ajoute l'extension SAN (basée sur le CN) au certificat d'emprunt d'identité.

Vérifications des modes non pris en charge Si vous ne bloquez pas les sessions avec des modes non pris en charge, les utilisateurs reçoivent un message d'avertissement s'ils se connectent à des serveurs potentiellement non sécurisés. Ils peuvent cliquer sur ce message pour accéder à un site potentiellement dangereux. Le blocage de ces sessions vous protège des serveurs qui utilisent des versions de protocole et des algorithmes faibles et risqués :

- **Bloquer les sessions avec des versions non prises en charge** — Lorsque vous configurez le Paramètre des profil de décryptage SSL, vous spécifiez la version minimale du protocole SSL à autoriser sur votre réseau pour réduire la surface d'attaque en bloquant les protocoles faibles. Cochez toujours cette case pour bloquer les sessions comportant des versions de protocole SSL/TLS faibles que vous avez décidé de ne pas prendre en charge.
- **Bloquer les sessions avec des suites de chiffrement non prises en charge** : cochez toujours cette case pour bloquer les sessions si le pare-feu ne prend pas en charge la suite de chiffrement spécifiée dans la communication. Vous configurez les algorithmes pris en charge par le pare-feu sur l'onglet **SSL Protocol Settings (Paramètres du protocole SSL)** du profil de décryptage.
- **Bloquer les sessions avec l'authentification du client** — Si vous n'avez aucune application critique nécessitant une authentification client, bloquez-la car le pare-feu ne peut pas déchiffrer les sessions nécessitant une authentification client. Le pare-feu a besoin des certificats du client et du serveur pour effectuer le décryptage bidirectionnel, mais avec l'authentification du client, le pare-feu ne connaît que le certificat du serveur. Cela met un terme au décryptage de sessions avec authentification client. Lorsque vous cochez cette case, le pare-feu bloque toutes les sessions avec authentification client, à l'exception des sessions des sites de la liste d'exclusion de décryptage SSL (**Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **SSL Decryption Exclusion (Exclusion de décryptage SSL)**).

  Si vous ne **Bloquez pas les sessions avec l'authentification du client**, lorsque le pare-feu tente de décrypter une session utilisant l'authentification du client, le pare-feu autorise la session et ajoute une entrée dans son cache d'exclusion de décryptage local contenant l'URL/adresse IP du serveur, l'application et le profil de décryptage à son Cache d'exclusion du décryptage local.

  *Vous devrez peut-être autoriser le trafic sur votre réseau à partir de sites qui utilisent l'authentification des clients et ne figurent pas dans les sites prédéfinis de la liste d'exclusion de décryptage SSL. Créez un profil de Décryptage autorisant des sessions avec authentification client. Ajoutez-le à une règle de politique de décryptage qui s'applique uniquement aux serveurs qui hébergent l'application. Pour renforcer encore plus la sécurité, vous pouvez exiger une Authentification Multifactorielle pour compléter le processus de connexion de l'utilisateur.*

Vérification des échecs :

- **Bloquer des sessions si les ressources ne sont pas disponibles** : si vous bloquez des sessions alors qu'aucune ressource de traitement du pare-feu n'est disponible, le pare-feu abandonne le trafic lorsqu'il ne dispose pas des ressources nécessaires pour le décrypter. Si vous ne bloquez pas les sessions lorsque le pare-feu ne peut pas traiter le décryptage en raison d'un manque de ressources, le trafic que vous souhaitez décrypter entre alors dans le réseau toujours crypté et n'est donc pas inspecté. Cependant, le blocage des sessions lorsque les ressources ne sont pas disponibles peut affecter l'expérience de l'utilisateur en rendant temporairement inaccessibles des sites que les utilisateurs peuvent normalement atteindre. La mise en œuvre de ce contrôle d'échec dépend de la position de votre entreprise en matière de conformité à la sécurité et de l'importance de l'expérience de l'utilisateur, mises en balance avec un renforcement de la sécurité.

Vous pouvez également utiliser des modèles de pare-feu avec une plus grande puissance de traitement afin de pouvoir décrypter plus de trafic.

- **Bloquer les sessions si HSM n'est pas disponible** — Si vous utilisez un module de sécurité matérielle (HSM) pour stocker vos clés privées, votre utilisation dépend des règles de conformité relatives à l'origine de la clé privée et de la manière dont vous souhaitez gérer le trafic chiffré si le HSM n'est pas disponible. Par exemple, si votre entreprise impose l'utilisation d'un HSM pour la signature de clé cryptographique, vous devez bloquer les sessions si le HSM n'est pas disponible. En revanche, si votre entreprise est moins stricte sur ces questions, vous pouvez envisager de ne pas bloquer de session lorsque le HSM n'est pas disponible. (Si le HSM est en panne, le pare-feu peut traiter le décryptage de sites pour lesquels des réponses du HSM sont dans le cache, mais pas pour les autres sites.) La meilleure pratique, dans ce cas, dépend des politiques de votre entreprise. Si le HSM est essentiel pour votre entreprise, exécutez-le dans une paire haute disponibilité (PAN-OS 8.1 prend en charge deux membres d'une paire HSM HA).
- **Blocage du déclassement en l'absence de ressource** : empêche le pare-feu de déclasser TLSv1.3 en TLSv1.2 si le pare-feu n'a pas de ressources de traitement TLSv1.3 disponibles. Si vous bloquez le déclassement, alors lorsque le pare-feu manque de ressources TLSv1.3, il abandonne le trafic qui utilise TLSv1.3 au lieu de le déclasser en TLSv1.2. Si vous ne bloquez pas le déclassement, alors lorsque le pare-feu manque de ressources TLSv1.3, il déclasse à TLSv1.2. Cependant, le blocage du déclassement lorsque les ressources de traitement du pare-feu ne sont pas disponibles peut affecter l'expérience utilisateur en rendant les sites que les utilisateurs peuvent normalement atteindre temporairement inaccessibles. La mise en œuvre de ce contrôle d'échec dépend de la position de votre entreprise en matière de conformité à la sécurité et de l'importance de l'expérience de l'utilisateur, mises en balance avec un renforcement de la sécurité. Vous pourriez vouloir créer une politique et un profil de décryptage distincts pour régir le décryptage du trafic sensible pour lequel vous ne voulez pas déclasser la version TLS.

## Inspection SSL entrante

Utilisez l'inspection SSL entrant pour déchiffrer et inspecter le trafic entrant SSL/TLS d'un client vers un serveur réseau ciblé (tout serveur pour lequel vous avez le certificat et que vous pouvez importer sur le pare-feu) et bloquer les sessions suspectes. Par exemple, si un employé est connecté à distance à un serveur Web hébergé sur le réseau d'entreprise et tente d'ajouter des documents internes dont l'accès est restreint à son dossier Dropbox (qui utilise SSL pour la transmission des données), l'inspection SSL entrante peut être utilisée pour s'assurer que les données sensibles ne quittent pas le réseau sécurisé de l'entreprise en bloquant ou limitant la session.

Sur le pare-feu, vous devez installer le certificat et la clé privée pour chaque serveur pour lequel vous voulez effectuer une Inspection entrante SSL. Vous devez également installer le certificat de clé publique ainsi que la clé privée sur chaque pare-feu qui effectue une Inspection entrante SSL. La manière dont le pare-feu effectue l'inspection entrante SSL dépend du type de clé négociée : Rivest, Shamir, Adleman (RSA) ou Perfect Forward Secrecy (Confidentialité de transmission parfaite ; PFS).

Pour les clés RSA, le pare-feu effectue une Inspection entrante SSL sans mettre fin à la connexion. Lorsque la session chiffrée traverse le pare-feu, le pare-feu en fait une copie de manière transparente et le déchiffre afin que le pare-feu puisse appliquer la politique appropriée au trafic.

*Lorsque vous configurez les* Paramètre des profil de décryptage SSL *pour le trafic d'inspection SSL entrante, créez des profils distincts pour les serveurs ayant des capacités de sécurité différentes. Par exemple, si un ensemble de serveurs ne prend en charge que RSA, les paramètres de protocole SSL doivent uniquement prendre en charge RSA. Toutefois, les paramètres de protocole SSL pour les serveurs prenant en charge PFS doivent prendre en charge PFS. Configurez les paramètres de protocole SSL pour obtenir le niveau de sécurité maximal pris en charge par le serveur, mais vérifiez les performances pour vous assurer que les ressources de pare-feu peuvent gérer la charge de traitement supérieure requise par les protocoles et algorithmes de sécurité élevés.*

Pour les clés PFS utilisant l'échange DHE (Diffie-Hellman) ou l'échange ECDHE (Elliptic Curve Diffie-Hellman exchange), le pare-feu fait office de proxy intermédiaire entre le client externe et le serveur interne. Étant donné que PFS génère une nouvelle clé à chaque session, le pare-feu ne peut pas se contenter de copier et de déchiffrer le flux SSL entrant lorsqu'il traverse, le pare-feu doit faire office de périphérique proxy.

*Si vous avez activé l'inspection entrante SSL à l'aide d'algorithmes d'échange de clés PFS, vous devez* upload a certificate bundle (télécharger un ensemble de certificats) *(un seul fichier) dans le pare-feu avec vos certificats organisés comme suit :*

1. *Certificat d'entité finale (feuille)*
2. *Certificats intermédiaires (dans l'ordre d'émission)*
3. *(Optional (Facultatif))* *Certificat racine*

*Le téléchargement du fichier garantit que les clients reçoivent la chaîne de certificats complète pendant les négociations SSL, évitant ainsi les problèmes d'authentification des certificats de serveur côté client.*

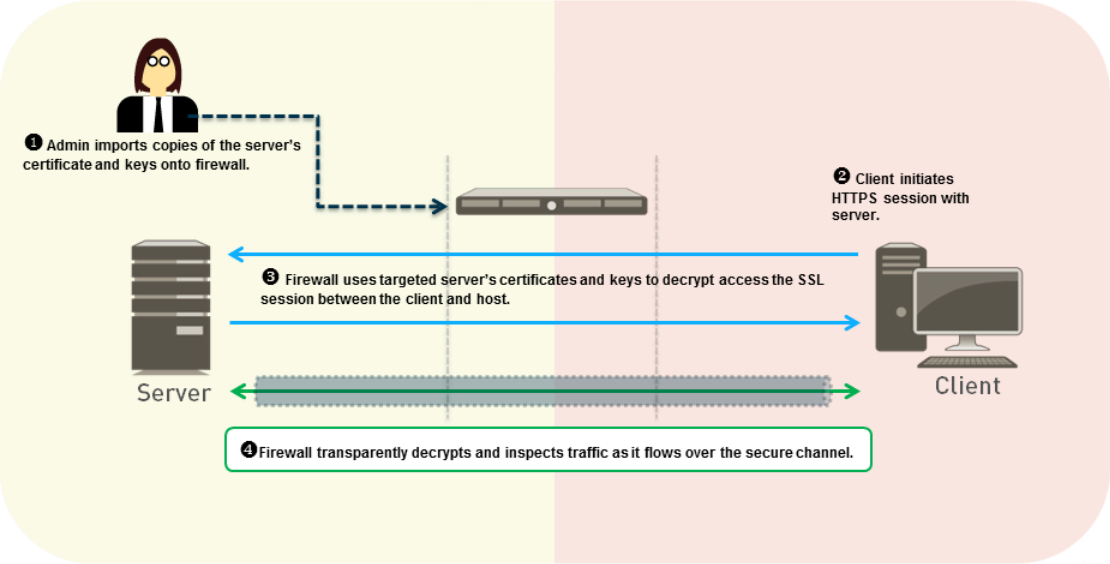
La figure suivante montre le fonctionnement de l'inspection SSL entrante lorsque l'algorithme d'échange de clé est RSA. Lorsque l'algorithme d'échange de clé est PFS, le pare-feu fonctionne comme un proxy (il crée une session sécurisée entre le client et le pare-feu et une autre session sécurisée entre le pare-feu et le serveur) et doit générer une nouvelle clé de session pour chaque session sécurisée.

*Lorsque vous configurez l'inspection entrante SSL et utilisez un chiffrement PFS, la reprise de session n'est pas prise en charge.*

Reportez-vous à la section Configuration de l'inspection SSL entrante pour plus d'informations sur sa mise en place.

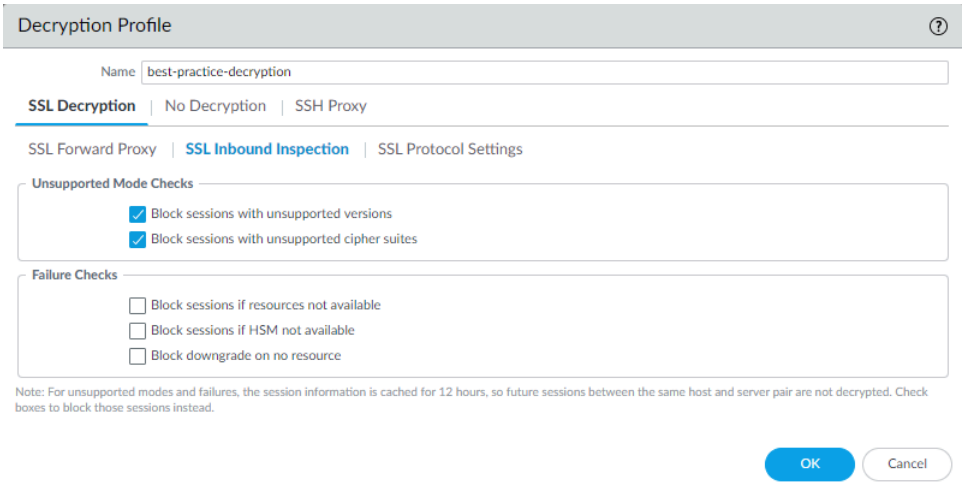
*Lorsque vous configurez l'inspection entrante SSL, le trafic proxy ne prend pas en charge les points de code DSCP ou QoS.*




# Profil de décryptage d'inspection entrante SSL

Le profil de décryptage de l'inspection SSL entrante (**Objects (Objets)** > **Decryption Profile (Profil de décryptage)** > **SSL Decryption (Décryptage SSL)** > **SSL Inbound Inspection (Inspection SSL entrante)**) contrôle les vérifications en mode session et les vérifications d'échec pour le trafic entrant SSL/TLS défini dans les politiques de décryptage de l'inspection entrante auxquelles vous joignez le profil. La figure suivante présente les recommandations générales de bonnes pratiques pour les paramètres du profil de décryptage de l'inspection entrante, mais les paramètres que vous utilisez dépendent également des règles de conformité de votre entreprise en matière de sécurité et des lois et réglementations locales.




Vérifications des modes non pris en charge Si vous ne bloquez pas les sessions avec des modes non pris en charge, les utilisateurs reçoivent un message d'avertissement s'ils se connectent à des serveurs potentiellement non sécurisés. Ils peuvent cliquer sur ce message pour accéder à un site potentiellement dangereux. Le blocage de ces sessions vous protège des serveurs qui utilisent des versions de protocole et des algorithmes faibles et risqués :

1. **Bloquer les sessions avec des versions non prises en charge** : lorsque vous configurez le Paramètre des profil de décryptage SSL, vous spécifiez la version minimale du protocole TLS à

autoriser sur votre réseau pour réduire la surface d'attaque en bloquant les protocoles faibles. Cochez toujours cette case pour bloquer les sessions comportant des versions de protocole SSL et TLS faibles que vous avez décidé de ne pas prendre en charge.

2. **Bloquer les sessions avec des suites de chiffrement non prises en charge** : cochez toujours cette case pour bloquer les sessions si le pare-feu ne prend pas en charge la suite de chiffrement spécifiée dans la communication. Vous configurez les algorithmes pris en charge par le pare-feu sur l'onglet **SSL Protocol Settings (Paramètres du protocole SSL)** du profil de décryptage.

Vérification des échecs :

- **Bloquer des sessions si les ressources ne sont pas disponibles** : si vous bloquez des sessions alors qu'aucune ressource de traitement du pare-feu n'est disponible, le pare-feu abandonne le trafic lorsqu'il ne dispose pas des ressources nécessaires pour le décrypter. Si vous ne bloquez pas les sessions lorsque le pare-feu ne peut pas traiter le décryptage en raison d'un manque de ressources, le trafic que vous souhaitez décrypter entre alors dans le réseau toujours crypté et n'est donc pas inspecté. Cependant, le blocage des sessions lorsque les ressources ne sont pas disponibles peut affecter l'expérience de l'utilisateur en rendant temporairement inaccessibles des sites que les utilisateurs peuvent normalement atteindre. La mise en œuvre de ce contrôle d'échec dépend de la position de votre entreprise en matière de conformité à la sécurité et de l'importance de l'expérience de l'utilisateur, mises en balance avec un renforcement de la sécurité. Vous pouvez également utiliser des modèles de pare-feu avec une plus grande puissance de traitement afin de pouvoir décrypter plus de trafic.
- **Bloquer les sessions si HSM n'est pas disponible** — Si vous utilisez un module de sécurité matérielle (HSM) pour stocker vos clés privées, votre utilisation dépend des règles de conformité relatives à l'origine de la clé privée et de la manière dont vous souhaitez gérer le trafic chiffré si le HSM n'est pas disponible. Par exemple, si votre entreprise impose l'utilisation d'un HSM pour la signature de clé cryptographique, vous devez bloquer les sessions si le HSM n'est pas disponible. En revanche, si votre entreprise est moins stricte sur ces questions, vous pouvez envisager de ne pas bloquer de session lorsque le HSM n'est pas disponible. (Si le HSM est en panne, le pare-feu peut traiter le décryptage de sites pour lesquels des réponses du HSM sont dans le cache, mais pas pour les autres sites.) La meilleure pratique, dans ce cas, dépend des politiques de votre entreprise. Si le HSM est essentiel pour votre entreprise, exécutez-le dans une paire haute disponibilité (PAN-OS 8.1 prend en charge deux membres d'une paire HSM HA).
- **Blocage du déclassement en l'absence de ressource** : empêche le pare-feu de déclasser TLSv1.3 en TLSv1.2 si le pare-feu n'a pas de ressources de traitement TLSv1.3 disponibles. Si vous bloquez le déclassement, alors lorsque le pare-feu manque de ressources TLSv1.3, il abandonne le trafic qui utilise TLSv1.3 au lieu de le déclasser en TLSv1.2. Si vous ne bloquez pas le déclassement, alors lorsque le pare-feu manque de ressources TLSv1.3, il déclasse à TLSv1.2. Cependant, le blocage du déclassement lorsque les ressources de traitement du pare-feu ne sont pas disponibles peut affecter l'expérience utilisateur en rendant les sites que les utilisateurs peuvent normalement atteindre temporairement inaccessibles. La mise en œuvre de ce contrôle d'échec dépend de la position de votre entreprise en matière de conformité à la sécurité et de l'importance de l'expérience de l'utilisateur, mises en balance avec un renforcement de la sécurité. Vous pourriez vouloir créer une politique et un profil de décryptage distincts pour régir le décryptage du trafic sensible pour lequel vous ne voulez pas déclasser la version TLS.

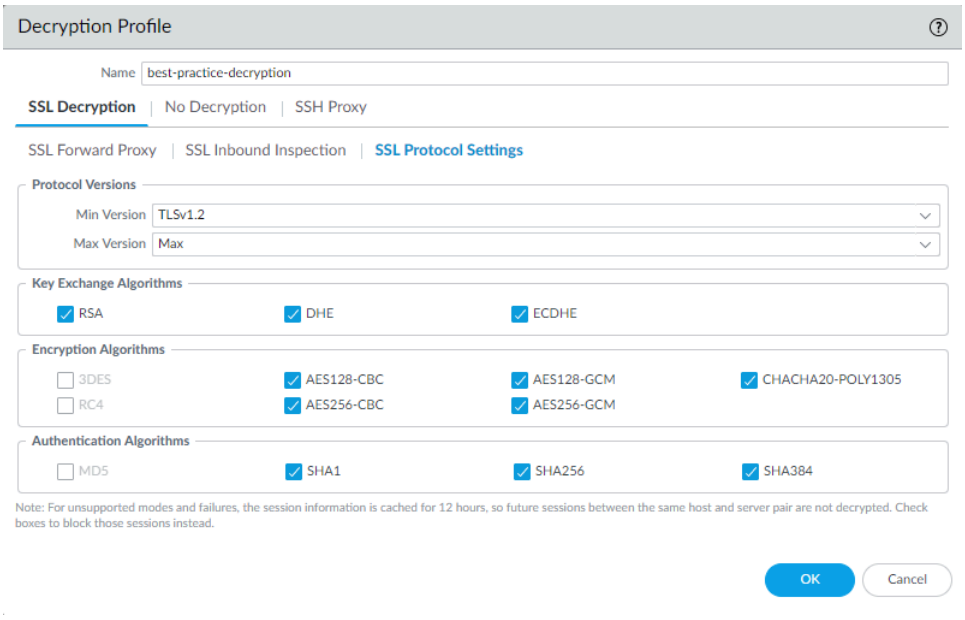
 

# Paramètre des profil de décryptage SSL

Les paramètres du protocole SSL (**Objects (Objets)** > **Decryption Profile (Profil de décryptage)** > **SSL Decryption (Décryptage SSL)** > **SSL Protocole Settings (Paramètres du protocole SSL)**) contrôlent si vous autorisez les versions de protocole SSL / TLS vulnérables, les algorithmes de cryptage faibles et les algorithmes d'authentification faibles. Les paramètres de protocole SSL s'appliquent au proxy de transfert SSL sortant et au trafic d'inspection SSL entrante. Ces paramètres ne s'appliquent pas au trafic de proxy SSH ni au trafic que vous ne décryptez pas.

La figure suivante illustre les recommandations générales concernant les meilleures pratiques pour les paramètres de protocole SSL. Il existe également des meilleures pratiques spécifiques pour le périmètre des profils de décryptage de passerelle Internet et des profils de décryptage de centre de données.

*Lorsque vous configurez les paramètres du protocole SSL pour le trafic d'inspection SSL entrante, créez des profils distincts pour les serveurs ayant des capacités de sécurité différentes. Par exemple, si un ensemble de serveurs ne prend en charge que RSA, les paramètres de protocole SSL doivent uniquement prendre en charge RSA. Toutefois, les paramètres de protocole SSL pour les serveurs prenant en charge PFS doivent prendre en charge PFS. Configurez les paramètres du protocole SSL pour le plus haut niveau de sécurité que le serveur cible que vous protégez prend en charge, mais vérifiez la performance pour vous assurer que les ressources du pare-feu peuvent gérer la charge de traitement supérieure dont les protocoles et algorithmes de sécurité accrue ont besoin.*




Versions du protocole :

- Fixez la **Min Version** sur **TLSv1.2** afin d'apporter le plus fort niveau de Sécurité —les sites commerciaux qui accordent de l'importance à la sécurité prennent en charge TLSv1.2. Si un site (ou une catégorie de sites) ne prend en charge que des chiffrements plus faibles, examinez le site et déterminez s'il héberge une application commerciale légitime. Si tel est le cas, créez une exception pour ce site uniquement en configurant un profil de décryptage comportant une **Min Version (Version Min.)** qui correspond à la suite la plus forte prise en charge par le site, puis en appliquant le profil à une règle de stratégie de déchiffrement qui limite l'autorisation du

chiffrement faible au site ou aux sites en question. Si le site n'abrite pas d'application commerciale légitime, n'affaiblissez pas votre posture de sécurité en renforçant ce site—des protocoles (ainsi que des chiffrement) faibles contiennent des vulnérabilités connues que les pirates informatiques peuvent exploiter.

Si le site appartient à une catégorie de sites dont vous n'avez pas besoin à des fins commerciales, utilisez la fonction de Filtrage des URL pour bloquer l'accès à l'ensemble de la catégorie. Ne prenez pas en charge les algorithmes de cryptage ou d'authentification faibles, sauf si vous devez prendre en charge d'anciens sites importants, et lorsque vous faites des exceptions, créez un profil de décryptage distinct qui autorise le protocole le plus faible uniquement pour ces sites. Ne déclarez pas le profil de déchiffrement principal que vous appliquez à la plupart des sites à TLSv1.1 simplement pour quelques exceptions.

*La page Qeb Qualys SSL Labs SSL Pulse fournit des statistiques à jour sur les pourcentages des différents chiffrements et protocoles utilisés sur les 150 000 sites les plus populaires du monde. Vous pouvez ainsi suivre les tendances et comprendre à quel point le support mondial est étendu pour des chiffrements et des protocoles plus sûrs.*

- Définissez la **Max Version** sur **Max** plutôt que sur une version en particulier afin que, au gré des améliorations apportées aux protocoles, le pare-feu prenne en charge les protocoles les meilleurs et les plus récents. Que vous souhaitiez appliquer un profil de Décryptage à une règle de politique de Décryptage régissant du trafic entrant (Inspection SSL Entrante) ou sortant (Proxy de transfert SSL), évitez d'autoriser des algorithmes faibles.

  *Si votre politique de décryptage est compatible avec des applications mobiles, dont beaucoup utilisent des certificats épinglés, réglez la **Max Version (Version max)** sur **TLSv1.2**. Parce que TLSv1.3 crypte les informations du certificat qu n'étaient pas cryptées dans les versions TLS antérieures, le pare-feu ne peut pas ajouter automatiquement des exclusions de décryptage sur la base des informations du certificat, ce qui affecte certaines applications mobiles. Par conséquent, si vous activez TLSv1.3, le pare-feu peut annuler certains trafics d'application mobile sauf si vous créez une Politique de non déchiffrement pour ce trafic.*

  *Si vous connaissez les applications mobiles que vous utilisez pour votre entreprise, envisagez de créer une politique et un profil de déchiffrement séparés pour ces applications afin de pouvoir activer TLSv1.3 pour le reste du trafic de l'application.*

Algorithmes d'échange de clés Laissez les trois cases cochées (par défaut) pour prendre en charge les échanges de clés RSA et PFS (DHE et ECDHE), sauf si la version minimale est fixée à TLSv1.3, qui ne prend en charge que l'ECDHE.

*Pour prendre en charge le trafic HTTP/2, vous devez laisser la case ECDHE cochée.*

Algorithmes de chiffrement : Lorsque vous définissez la version minimale du protocole sur TLSv1.2, les algorithmes 3DES et RC4 les plus anciens et les plus faibles sont automatiquement décochés (bloqués). Lorsque vous définissez la version minimale du protocole sur TLSv1.3, les algorithmes 3DES, RC4, AES128-CBC et AES256-CBC sont automatiquement bloqués. Pour tout trafic pour lequel vous devez autoriser un protocole TLS plus faible, créez un profil de décryptage distinct et appliquez-le uniquement au trafic de ce site, puis désélectionnez les cases appropriées pour autoriser l'algorithme. Autoriser le trafic qui utilise les algorithmes 3DES ou RC4 expose votre réseau à un

risque excessif. Si le blocage de 3DES ou RC4 vous empêche d'accéder à un site que vous devez utiliser à des fins professionnelles, créez un profil et une politique de décryptage distincts pour ce site. N'affaiblissez pas le déchiffrement pour aucun autre site.

Algorithmes d'authentification : Le pare-feu bloque automatiquement l'algorithme MD5, plus ancien et plus faible. Lorsque TLSv1.3 est la version minimale, le pare-feu bloque également SHA1. N'autorisez pas le trafic authentifié MD5 sur votre réseau ; SHA1 est l'algorithme d'authentification le plus faible que vous devriez autoriser. Si aucun site nécessaire n'utilise le SHA1, bloquez le trafic du SHA1 pour réduire davantage la surface d'attaque.

## Proxy SSH

Dans une configuration de proxy SSH, le pare-feu se trouve entre un client et un serveur. La session SSH permet au pare-feu de déchiffrer les connexions SSH entrantes et sortantes et de s'assurer que les attaquants n'utilisent pas SSH pour tunnel les applications et le contenu indésirables. Le déchiffrement SSH ne nécessite pas de certificat et le pare-feu génère automatiquement la clé utilisée pour le déchiffrement SSH lors du démarrage du pare-feu. Durant la procédure de démarrage, le pare-feu vérifie s'il existe une clé. Sinon, le pare-feu génère une clé. Le pare-feu utilise la clé pour déchiffrer les sessions SSH de tous les systèmes virtuels configurés sur le pare-feu et de toutes les sessions SSH v2.

SSH permet la tunnellisation, ce qui peut masquer le trafic malveillant du déchiffrement. Le pare-feu ne peut pas déchiffrer le trafic à l'intérieur d'un tunnel SSH. Vous pouvez bloquer tout le trafic du tunnel SSH en configurant une règle de politique de sécurité pour l'application **ssh-tunnel** avec l'**action** mise sur **Deny (Refuser)** (avec une règle de politique de sécurité pour autoriser le trafic de l'application **ssh**).

Des sessions utilisant des SSH peuvent tunnelliser des paquets Windows X11 et des paquets TCP. Une connexion SSH peut contenir plusieurs canaux. Lorsque vous appliquez un profil de Décryptage SSH à du trafic, le pare-feu examine l'App-ID du trafic et identifie le type de canal pour chaque canal de la connexion. Voici les différents types de canaux :

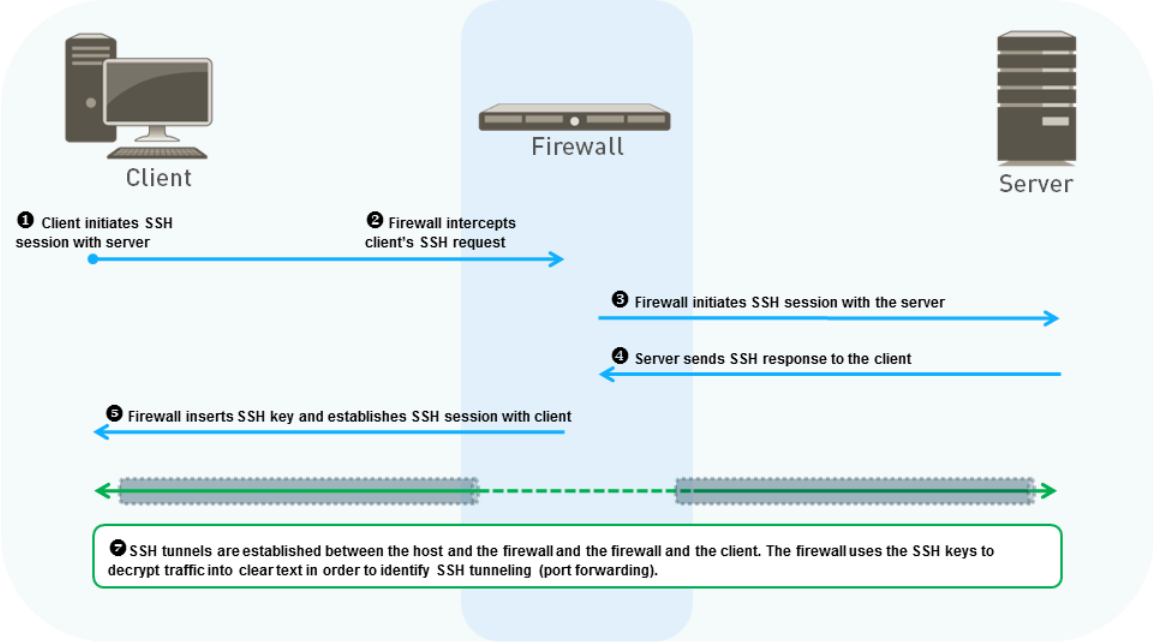
- session
- X11
- forwarded-tcpip
- direct-tcpip

Lorsque le type de canal est "session", le pare-feu identifie le trafic comme étant du trafic SSH autorisé, tels que SFTP ou SCP. Lorsque le type de canal est "X11", forwarded-tcpip ou direct-tcpip, le pare-feu identifie le trafic comme étant du trafic utilisant un tunnel SSH et le bloque.

***Limitez l'utilisation de SSH aux administrateurs qui doivent gérer des périphériques réseau, consigner tout le trafic SSH et envisager de configurer l'***Authentification multi-facteurs ***pour garantir que seuls des utilisateurs légitimes peuvent utiliser SSH pour accéder à des périphériques, ce qui réduit la surface d'attaque.***

La figure suivante montre le processus de décryptage SSH : Reportez-vous à la section Configuration du proxy SSH pour savoir comment activer le déchiffrement du proxy SSH.




Lorsque le client envoie une demande SSH au serveur pour lancer une session, le pare-feu intercepte la demande et l'achemine au serveur. Le pare-feu intercepte ensuite la réponse du serveur et la transmet au client. Ceci établit deux tunnels SSH distincts, l'un entre le pare-feu et le client et l'autre entre le pare-feu et le serveur, le pare-feu fonctionnant en tant que proxy. À mesure que le trafic circule entre le client et le serveur, le pare-feu vérifie si le trafic SSH est acheminé normalement ou s'il utilise la tunnellisation SSH (transfert de port). Le pare-feu n'effectue aucune inspection du contenu et des menaces sur les tunnels SSH ; toutefois, si le pare-feu identifie les tunnels SSH, il bloque le trafic par tunnel SSH et le restreint en fonction des politiques de sécurité configurées.

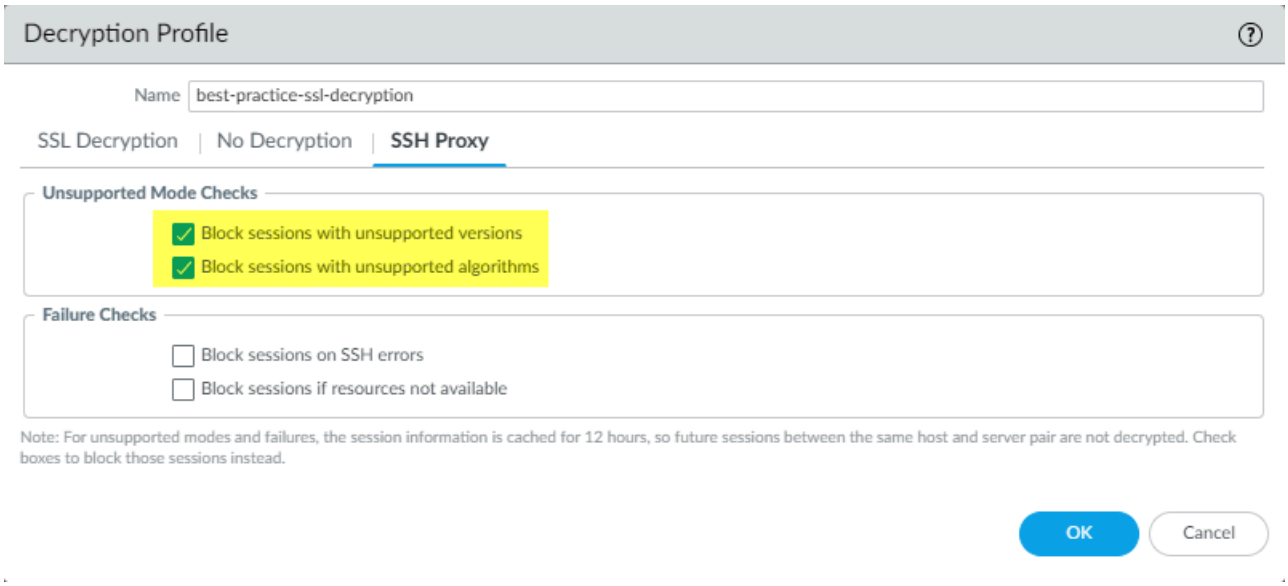
*Lorsque vous configurez le proxy SSH, le trafic proxy ne prend pas en charge les points de code DSCP ou la qualité de service.*

## Profil de décryptage SSL

Le profil SSL Forward Proxy Decryption **Objects (Objets)** > **Decryption Profile (Profil de décryptage)** > **SSH Proxy**) contrôle les vérifications de mode de session et les vérifications de défaillance pour le trafic SSH défini dans les politiques de déchiffrement de proxy SSH auxquelles vous associez le profil. La figure suivante montre les recommandations générales relatives aux pratiques exemplaires pour les paramètres de profil de déchiffrement de proxy SSH, mais les paramètres que vous utilisez dépendent également des règles de conformité en matière de sécurité de votre entreprise et des lois et règlements locaux.

*Le pare-feu n'effectue aucune inspection du contenu et des menaces sur les tunnels SSH (transfert de port). Cependant, le pare-feu fait la distinction entre l'application SSH et l'application du tunnel SSH. Si le pare-feu identifie des tunnels SSH, il bloque le trafic du tunnel SSH et le limite en fonction des stratégies de sécurité configurées.*




Vérifications des modes non pris en charge Le pare-feu prend en charge SSHv2. Si vous ne bloquez pas les sessions avec des modes non pris en charge, les utilisateurs reçoivent un message d'avertissement s'ils se connectent à des serveurs potentiellement non sécurisés. Ils peuvent cliquer sur ce message pour accéder à un site potentiellement dangereux. Le blocage de ces sessions vous protège des serveurs qui utilisent des versions de protocole et des algorithmes faibles et risqués :

1. **Bloquer les sessions comportant des versions non prises en charge** - Le pare-feu possède un ensemble de versions prises en charge qui sont prédéfinies. Cochez cette case pour bloquer le trafic comportant des versions faibles. Cochez toujours cette case pour bloquer les sessions comportant des versions de protocole faibles afin de réduire la surface d'attaque.
2. **Bloquer les sessions comportant des algorithmes non pris en charge** – Le pare-feu comporte un ensemble d'algorithmes pris en charge qui sont prédéfinis. En cochant cette case, vous bloquez le trafic avec des algorithmes faibles. Cochez toujours cette case pour bloquer les sessions avec des algorithmes non pris en charge afin de réduire la surface d'attaque.

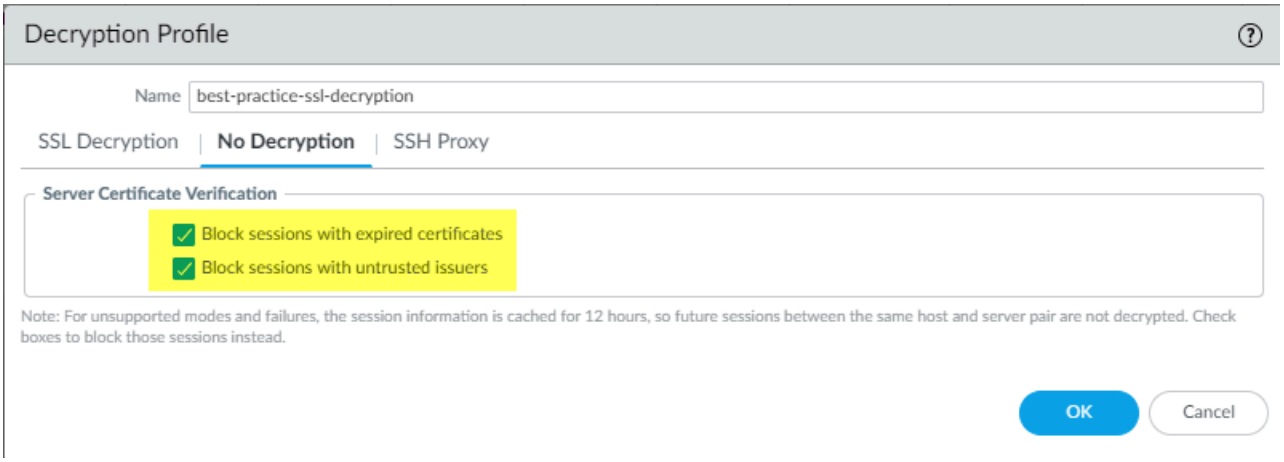
Vérification des échecs :

- **Bloquer les sessions sur les erreurs SSH** — Cochez cette case pour mettre fin à la session si des erreurs SSH se produisent.
- **Bloquer les sessions si les ressources ne sont pas disponibles** : si vous ne bloquez pas les sessions lorsque les ressources de traitement du pare-feu ne sont pas disponibles, le trafic chiffré que vous souhaitez déchiffrer entre sur le réseau toujours chiffré, ce qui risque de permettre des connexions potentiellement dangereuses. Cependant, le blocage de sessions lorsque les ressources de traitement du pare-feu ne sont pas disponibles peut affecter l'expérience utilisateur en rendant les sites que les utilisateurs peuvent normalement atteindre temporairement inaccessibles. La mise en place de contrôles de défaillance dépend de la position de votre entreprise concernant les règles de conformité et concernant l'importance accordée à l'expérience utilisateur, comparée à une sécurité plus stricte. Vous pouvez également utiliser des modèles de pare-feu avec une plus grande puissance de traitement afin de pouvoir décrypter plus de trafic.

# Profil pour l'absence de déchiffrement

Les profils de non décryptage (**Objects (Objets)** > **Decryption Profile (Profil de décryptage)** > **No Decryption (Non décryptage)**) effectuent des contrôles de vérification du serveur pour le trafic que vous choisissez de ne pas décrypter. Vous joignez un profil de non décryptage politique de décryptage « non décryptage » qui définit le trafic à exclure du décryptage. (N'utilisez pas la politique pour exclure le trafic que vous ne pouvez pas décrypter parce qu'un site interrompt le décryptage pour des raisons techniques, comme un certificat épinglé ou une authentification mutuelle. Ajoutez plutôt le nom d'hôte à la liste d'exclusion du de déchiffrement.) La figure suivante montre les recommandations de meilleures pratiques générales pour les paramètres de profil d'absence de déchiffrement, mais les paramètres que vous utilisez dépendent également des règles de conformité de sécurité de votre entreprise et des lois et règlements locaux.




- **Bloquer les sessions avec des certificats expirés** : cochez cette case pour bloquer des sessions comportant des serveurs dont les certificats sont expirés et pour empêcher l'accès à des sites potentiellement peu sûrs. Si vous ne cochez pas cette case, les utilisateurs peuvent se connecter à des sites malveillants et transiger avec eux de même que voir des messages d'avertissement lorsqu'ils tentent de se connecter. Rien n'empêche alors la connexion de se produire.
- **Block les sessions avec des émetteurs non approuvés** : cochez cette case pour bloquer les sessions avec des serveurs qui possèdent des émetteurs de certificats non approuvés. Un émetteur non approuvé peut indiquer une attaque d'homme au milieu, une attaque par répétition, ou autre attaque.

*Ne joignez pas un profil de non-décryptage aux politiques de décryptage pour le trafic TLSv1.3 que vous ne décryptez pas. Contrairement aux versions précédentes, TLSv1.3 crypte les informations des certificats, de sorte que le pare-feu n'a aucune visibilité sur les données des certificats et ne peut donc pas bloquer les sessions avec des certificats expirés ou des émetteurs non fiables, donc le profil n'a aucun effet. (Le pare-feu peut effectuer des contrôles de certificats avec TLSv1.2 et antérieurs car ces protocoles ne chiffrent pas les informations de certificats et vous devez appliquer un profil de non décryptage à leur trafic). Cependant, vous devez créer une politique de décryptage pour le trafic TLSv1.3 que vous ne décryptez pas, car le pare-feu n'*enregistre *pas le trafic non décrypté à moins qu'une politique de décryptage ne contrôle ce trafic.*

*(S'applique à TLSv1.2 et aux versions antérieures) Si vous décidez d'autoriser les sessions avec des émetteurs non approuvés (non recommandé) et de **bloquer les sessions avec un certificat expiré** uniquement, il se peut qu'une session avec un émetteur approuvé expiré soit bloquée par mégarde. Lorsque le magasin de certificats du pare-feu contient une CA approuvée auto-signée valide et que le serveur envoie un CA expiré dans la chaine de certification, le pare-feu ne vérifie pas son magasin de certificats A la place, le pare-feu bloque la session basée sur le CA expiré, alors qu'il devrait trouver l'ancre de confiance alternative valide et autoriser la session basée sur le certificat de confiance auto-signé*

*Pour éviter ce scénario, en plus de **bloquer les sessions avec des certificats expirés**, activez **bloquer les sessions avec les émetteurs non approuvés**. Cela oblige le pare-feu à vérifier son magasin de certificat, trouver le CA de confiance auto-signé et autoriser la session*

## Décryptage SSL avec certificats ECC (Elliptical Curve Cryptography, cryptographie à courbe elliptique).

Le pare-feu décrypte automatiquement le trafic SSL entrant depuis des sites web ou des applications à l'aide de certificats ECC, dont des certificats ECDSA (Elliptic Curve Digital Signature Algorithm). À mesure que les organisations font la transition vers une utilisation de certificats ECC afin de bénéficier de clés plus fortes et de tailles de certificats plus courtes, vous pouvez maintenir une visibilité sur des applications sécurisées par ECC et du trafic web, et en autoriser un accès en toute sécurité.

*Le décryptage de sites web et applications avec certificats ECC n'est pas disponible pour le trafic mis en miroir sur le pare-feu ; le trafic crypté utilisant des certificats ECC doit passer directement par le pare-feu pour que le pare-feu puisse le décrypter.*

*Vous pouvez utiliser un Hardware Security Module (module de sécurité matériel - HSM) pour enregistrer les clés privées associées aux certificats ECDSA. Pour le trafic TLSv1.3, PAN-OS prend en charge les HSM uniquement pour le proxy de transfert SSL. Il ne prend pas en charge les HSM pour l'inspection SSL entrante.*

## Prise en charge de Perfect Forward Secrecy (Confidentialité de transmission parfaite ; PFS) pour le décryptage SSL

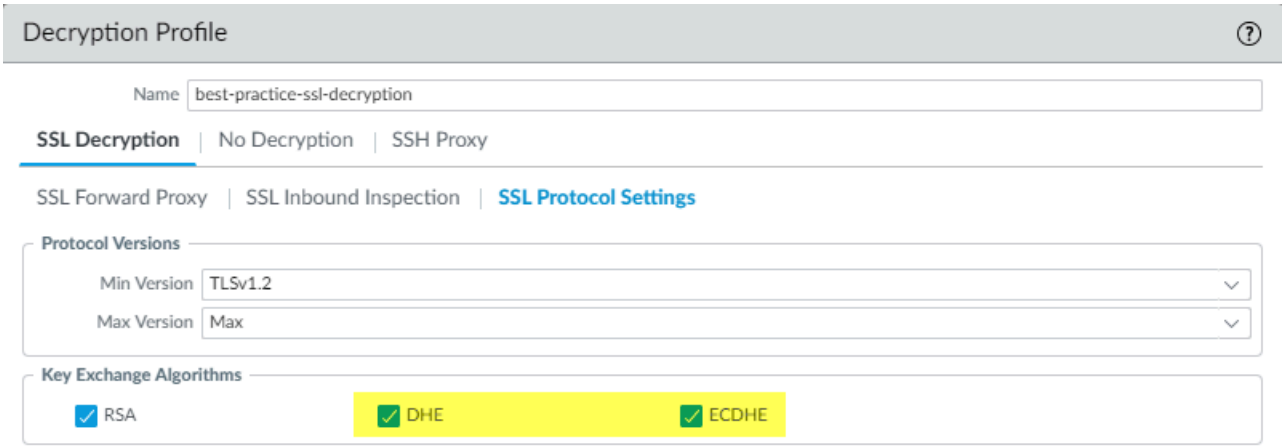
PGS est un protocole de communication sécurisé qui empêche l'infection d'une session chiffrée d'entraîner l'infection de plusieurs sessions chiffrées. Avec PFS, un serveur génère des clés privées uniques pour chaque session sécurisée qu'il établit avec un client. Si une clé privée d'un serveur est compromise, seule la session établie au moyen de cette clé est vulnérable : un pirate ne peut récupérer les données des sessions antérieures et postérieures, car le serveur établit chaque connexion au moyen d'une clé générée de manière unique. Le pare-feu déchiffre des sessions SSL avec des algorithmes d'échange de clés PFS et conserve la protection PFS pour les sessions antérieures et postérieures.

La prise en charge de PFS basé sur Diffie-Hellman (DHE) et de PFS basé sur la courbe elliptique Diffie-Hellman (ECDHE) est activée par défaut (**Objects (Objets)** > **Decryption Profile (Profil de décryptage)** > **SSL Decryption (Décryptage SSL)** > **SSL Protocol Settings (Paramètres de protocole SSL)**.

*Si vous utilisez les algorithmes d'échange de clés DHE ou ECDHE pour activer la Prise en charge de Perfect Forward Secrecy (Confidentialité de transmission parfaite ; PFS) pour le décryptage SSL, vous pouvez utiliser un* hardware security module (module de sécurité matérielle ; HSM)< *pour stocker les clés privées pour l'Inspection Entrante SSL.*

*Lorsque vous configurez l'inspection entrante SSL et utilisez un chiffrement PFS, la reprise de session n'est pas prise en charge.*

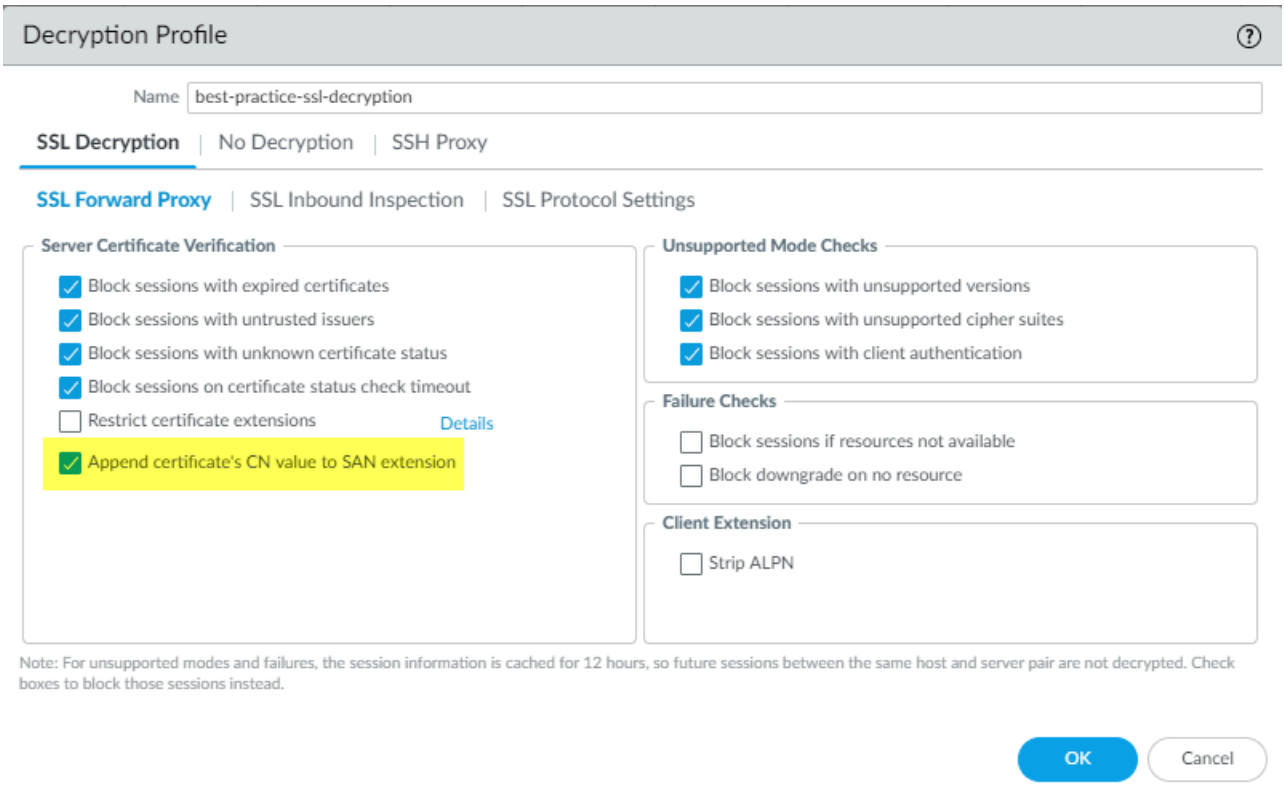



# Déchiffrement SSL et Subject Alternative Names (Autres noms de l'objet ; SAN)

Certains navigateurs exigent que les certificats du serveur utilisent un Subject Alternative Name (Autre nom de l'objet ; SAN) pour spécifier les domaines que le certificat protège et ne prennent plus en charge la mise en correspondance de certificats en fonction du Common Name (nom commun ; CN) du certificat du serveur. Les SAN permettent à un certificat de serveur unique de protéger plusieurs noms ; les CN sont moins bien définis que les SAN et ne peuvent protéger qu'un seul domaine ou que les sous-domaines de premier niveau d'un domaine. Cependant, si un certificat du serveur ne contient qu'un CN, les navigateurs qui exigent un SAN n'autoriseront pas les utilisateurs finaux à se connecter à la ressource Web demandée. Le pare-feu peut ajouter un SAN au certificat d'emprunt qu'il génère pour s'établir en tant que tiers de confiance lors du déchiffrement SSL. Lorsqu'un certificat du serveur ne contient qu'un CN, un pare-feu qui effectue le déchiffrement SSL copie ce CN au SAN du certificat d'emprunt. Le pare-feu présente le certificat d'emprunt contenant le SAN au client, et le navigateur peut alors prendre en charge la connexion. Les utilisateurs finaux peuvent continuer d'accéder aux ressources dont ils ont besoin, et le pare-feu peut déchiffrer les sessions.

Pour activer la prise en charge du SAN pour le trafic SSL déchiffré, mettez à jour le profil de déchiffrement associé à la politique de déchiffrement pertinente : sélectionnez **Objects (Objets)** > **Decryption Profile (Profil de déchiffrement)** > **SSL Decryption (Déchiffrement SSL)** > **SSL Forward Proxy (Proxy de transfert SSL)** > **Append Certificate's CN Value to SAN Extension (Ajouter la valeur CN du certificat à l'extension SAN)**.




# Décryptage TLSv1.3

Vous pouvez décrypter, obtenir une visibilité totale et prévenir les menaces connues et inconnues dans le trafic TLSv1.3. TLSv1.3 est la dernière version du protocole TLS, qui apporte des améliorations en matière de sécurité et de performances des applications. Vos politiques de décryptage existantes fonctionnent avec TLSv1.3 lorsque vous configurez le profil de décryptage associé pour utiliser TLSv1.3 comme version de protocole minimale ou pour utiliser TLSv1.3 ou Max comme version de protocole maximale. Le pare-feu prend en charge le décryptage TLSv1.3 pour le proxy de transfert, l'Inspection entrante, le trafic du Broker de paquets de réseau décrypté et la mise en miroir du port de décryptage.

Pour utiliser TLSv1.3, le client et le serveur doivent être capables de négocier les chiffrements TLSv1.3. Pour les sites web qui ne prennent pas en charge TLSv1.3, le pare-feu sélectionne une version plus ancienne du protocole TLS que le serveur prend en charge.

Le pare-feu prend en charge les algorithmes de décryptage suivants pour TLSv1.3 :

- TLS13-AES-128-GCM-SHA256
- TLS13-AES-256-GCM-SHA384
- TLS13-CHACHA20-POLY1305-SHA256

Si le profil de décryptage que vous appliquez au trafic décrypté indique que la **Max version (Version max)** du protocole est **Max**, alors le profil prend en charge TLSv1.3 et utilise automatiquement TLSv1.3 avec les sites qui prennent en charge TLSv1.3. Sinon, pour prendre en charge TLSv1.3, réglez **Max Version (Version max)** sur **Max**. Lorsque vous passez à PAN-OS 10.0, tous les profils de décryptage dont la **Max version (Version max)** est réglée sur **Max** sont réinitialisés sur **TLSv1.2**

afin de fournir une prise en charge automatique des applications mobiles qui utilisent des certificats épinglés et d'éviter que le trafic ne soit interrompu.

Toutes les applications ne prennent pas en charge le protocole TLSv1.3. Suivez les meilleures pratiques de décryptage, réglez le **Min Version (Version min)** du protocole TLS sur **TLSv1.2** et laissez le réglage de **Max Version (Version max)** sur **Max**. Si les besoins professionnels exigent d'autoriser un protocole TLS plus faible, créez un profil de décryptage SSL distinct avec une **Min Version (Version min)** qui autorise le protocole plus faible et joignez-le à une politique de décryptage qui définit le trafic que vous devez autoriser avec le protocole TLS plus faible.

Si votre politique de décryptage est compatible avec des applications mobiles, dont beaucoup utilisent des certificats épinglés, réglez la **Max Version (Version max)** sur **TLSv1.2**. Parce que TLSv1.3 crypte les informations du certificat qu n'étaient pas cryptées dans les versions TLS antérieures, le pare-feu ne peut pas ajouter automatiquement des exclusions de décryptage sur la base des informations du certificat, ce qui affecte certaines applications mobiles. Par conséquent, si vous activez TLSv1.3, le pare-feu peut annuler certains trafics d'application mobile sauf si vous créez une Politique de non déchiffrement pour ce trafic. Si vous connaissez les applications mobiles que vous utilisez pour votre entreprise, envisagez de créer une politique et un profil de déchiffrement séparés pour ces applications afin de pouvoir activer TLSv1.3 pour le reste du trafic.

*N'attachez pas de No Decryption profile (profil de non-déchiffrement) aux Decryption policies (politiques de déchiffrement) pour le trafic TLSv1.3 que vous ne déchiffrez pas si vous savez qu'une stratégie particulière contrôle uniquement le trafic TLSv1.3. Un changement par rapport aux versions précédentes de TLS est que TLSv1.3 crypte les informations des certificats, de sorte que le pare-feu n'a plus de visibilité sur ces données et ne peut donc pas bloquer les sessions avec des certificats expirés ou des émetteurs non approuvés, donc le profil n'a aucun effet. (Le pare-feu peut effectuer des contrôles de certificats avec TLSv1.2 et antérieurs car ces protocoles ne chiffrent pas les informations de certificats et vous devez appliquer un profil de non décryptage à leur trafic). Cependant, vous pouvez enregistrer le trafic non déchiffré de tous types en activant la journalisation des négociations TLS réussies et infructueuses dans la stratégie de décryptage (la journalisation des négociations TLS infructueuses est activée par défaut).*

Lorsque vous autorisez des modes non pris en charge dans le Paramètre des profil de décryptage SSL, le pare-feu ajoute automatiquement le trafic au Cache d'exclusion du décryptage local. Le pare-feu décrypte et inspecte toujours le trafic qui est déclassé de TLSv1.3 à TLSv1.2 et le **Reason (Motif)** indiqué dans le cache pour ajouter le serveur au cache est TLS13_UNSUPPORTED.

Si vous passez de PAN-OS 10.1 à une version antérieure, tout profil de décryptage qui spécifie TLSv1.3 comme **Min Version (Version min)** ou **Max Version (Version max)** passe à la version la plus élevée prise en charge. Par exemple, le déclassement de PAN-OS 10.1 à PAN-OS 9.1 remplacerait TLSv1.3 par TLSv1.2. Si un périphérique Panorama sur PAN-OS 10.1 pousse la configuration vers des périphériques qui exécutent des versions plus anciennes de PAN-OS, tout profil de décryptage qui a spécifié TLSv1.3 comme la **Min Version (Version min)** ou la **Max Version (Version max)** passe également à la version la plus élevée prise en charge.

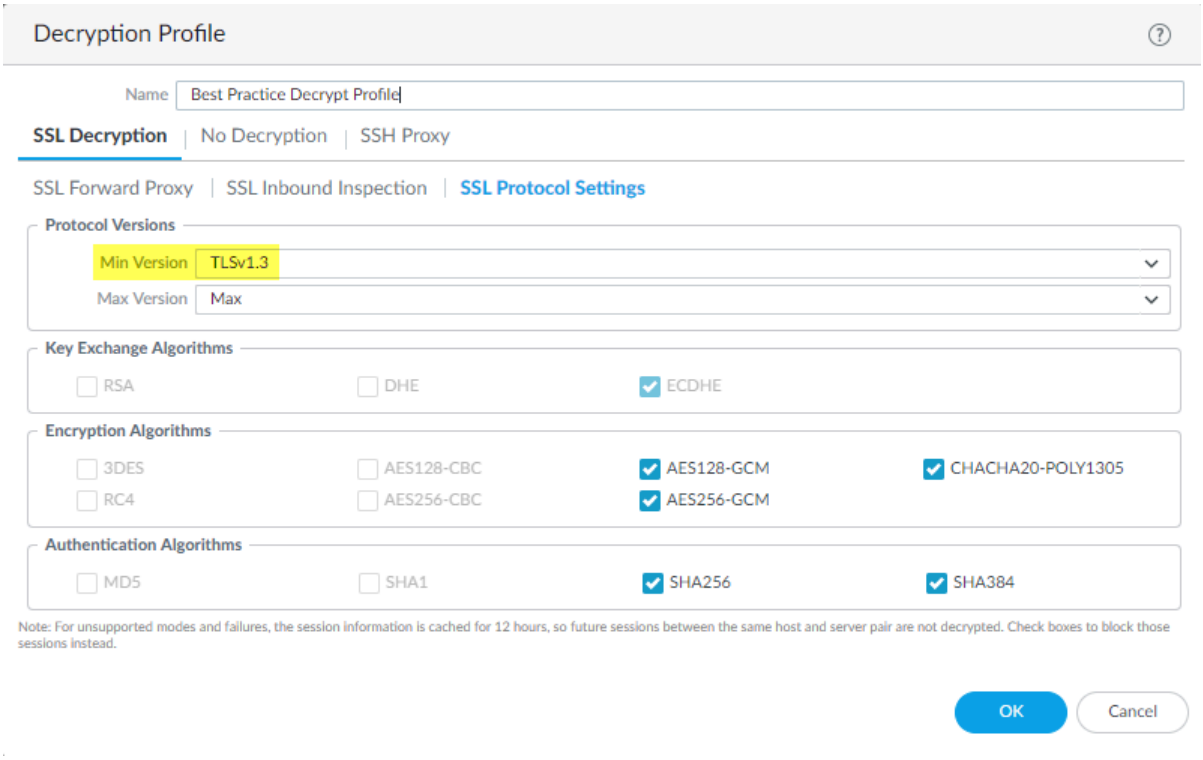
*Pour les clients qui utilisent des modules de sécurité matériels (HSM), PAN-OS prend en charge TLSv1.3 uniquement pour proxy de transfert SSL. Il ne prend pas en charge les HSM pour l'inspection SSL entrante.*

Vous pouvez configurer un profil de décryptage SSL qui définit TLSv1.3 comme la version de protocole minimale autorisée pour obtenir la sécurité la plus stricte. Cependant, certaines applications ne prennent pas en charge TLSv1.3 et peuvent ne pas fonctionner si TLSv1.3 est le protocole minimum autorisé. Appliquez un profil qui définit TLSv1.3 comme la version minimale uniquement au trafic d'applications qui ne prennent en charge que TLSv1.3.

1. Créez un nouveau profil de décryptage SSL ou modifiez un profil existant (**Objects (Objets)** > **Decryption (Décryptage)** > **Decryption Profile (Profil de décryptage)**).

   S'il s'agit d'un nouveau profil, spécifiez le **Name (Nom)** du profil.
2. Sélectionnez **SSL Protocol Settings (Paramètres du protocole SSL)**.
3. Changez la **Min Version (Version min)** en **TLSv1.3**.




   L'utilisation de **Max** pour la **Max Version (Version max)** garantit que le trafic contrôlé par le profil peut utiliser la version de protocole la plus forte disponible. **Min Version (Version min)** définit la version la plus faible du protocole que le trafic peut utiliser. Le fait de régler la version minimale à **TLSv1.3** signifie que le trafic doit utiliser TLSv1.3 (ou plus) et que les versions de protocole plus faibles sont bloquées. (La règle de politique de décryptage définit le trafic que le profil contrôle).

   Lorsque vous configurez TLSv1.3 comme **Min Version (Version min)**, vous devez utiliser Perfect Forward Secrecy (PFS) et les algorithmes plus faibles d'échange de clés, de cryptage et d'authentification ne sont pas disponibles.
4. Configurez tous les autres paramètres du profil de décryptage que vous devez définir ou modifier.
5. Cliquez sur **OK** pour enregistrer le profil.
6. Attachez le profil à la règle de politique de décryptage appropriée pour l'appliquer au trafic approprié.

## Support haute disponibilité pour les sessions déchiffrées

Le pare-feu prend en charge la synchronisation haute disponibilité (HA) uniquement pour les sessions SSL entrantes et décryptées, et uniquement si les sessions ont été établies à l'aide d'algorithmes d'échange de clés non-PFS. Le pare-feu ne prend pas en charge la synchronisation HA pour tout autre trafic décrypté. Le pare-feu décrypte les nouvelles sessions qui démarrent après le basculement sur la base de la politique de décryptage.

Le tableau suivant montre la prise en charge de la synchronisation HA pour les sessions décryptées après un basculement :

| Type de session | Échange de clés PFS | Échange de clés non-PFS |
|---|---|---|
| Session SSL entrante (décryptage d'inspection entrante) | Pas de synchronisation HA, le pare-feu abandonne la session | La synchronisation HA a lieu, le pare-feu autorise la session mais ne décrypte pas la session |
| Sessions SSL sortantes (décryptage de proxy de transfert SSL) | Pas de synchronisation HA, le pare-feu abandonne la session | Pas de synchronisation HA, le pare-feu abandonne la session |

## Mise en miroir du décryptage

La mise en miroir du décryptage crée une copie du trafic décrypté provenant d'un pare-feu et l'envoie à un outil de collecte du trafic, tel que NetWitness ou Solera, qui peut recevoir des captures de paquets bruts, en vue de leur archivage et de leur analyse. Cette fonction est nécessaire pour les entreprises qui ont besoin de captures de données complètes à des fins de forensics ou d'archivage, ou de la fonctionnalité de prévention des fuites de données (DLP).

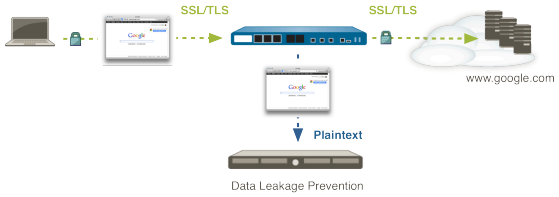
Après avoir installé la licence, connectez l'outil de collection de trafic directement à une interface Ethernet sur le pare-feu et réglez **Interface Type (Type d'interface)** sur **Decrypt Mirror (Mise en miroir du décryptage)**. Le pare-feu simule une initialisation TCP avec l'outil de collection et ensuite, envoie chaque paquet de données au travers de l'interface, déchiffré (en texte clair).

*La Mise en miroir du port de déchiffrement n'est pas offerte sur les pare-feu VM-Series pour plateformes de cloud public (AWS, Azure, Google Cloud Platform) et VMware NSX.*

N'oubliez pas que le décryptage, le stockage, l'inspection et/ou l'utilisation du trafic SSL sont régis par la législation dans certains pays et que le consentement des utilisateurs peut être exigé afin d'utiliser la fonction Miroir du décryptage. En outre, l'utilisation de cette fonction pourrait accorder à des utilisateurs malveillants un accès administrateur au pare-feu leur permettant de récolter des noms d'utilisateur, des mots de passe, des numéros de sécurité sociale, des numéros de carte de crédit, ou d'autres informations sensibles envoyées via un canal crypté. Palo Alto Networks vous recommande de consulter la direction de votre entreprise avant d'activer et d'utiliser cette fonction dans un environnement de production.

Le graphique suivant illustre le processus de mise en miroir du trafic déchiffré et la section Configuration de la mise en miroir du port de décryptage explique comment activer la licence et utiliser cette fonction.



# Préparation au déploiement du déchiffrement

La partie du déploiement du déchiffrement qui demande le plus de temps n'est pas la configuration des politiques et des profils de déchiffrement, c'est plutôt la préparation du déploiement en travaillant avec les parties prenantes pour décider du trafic à déchiffrer et à ne pas déchiffrer, en informant votre population d'utilisateurs des changements apportés à l'accès au site Web, en développant une stratégie relative à l'infrastructure de clés privées et en planifiant un déploiement graduel et hiérarchisé.

Définissez les objectifs du déchiffrement et passez en revue la liste de vérification des pratiques exemplaires en matière de déploiement de déchiffrement pour vous assurer de comprendre les pratiques exemplaires recommandées. L'objectif visé devrait être de déchiffrer le plus grand nombre de trafic que les ressources de votre pare-feu permet et de déchiffrer le trafic le plus important en premier.

***Passez de règles de politique de sécurité basées sur des portes à des règles de politique de sécurité basées sur des applications avant de créer et de déployer des règles de politique de déchiffrement. Si vous créez des règles de déchiffrement basées sur une politique de sécurité basée sur des ports, puis que vous passez à une politique de sécurité basée sur les applications, le changement pourrait pousser les règles de déchiffrement à bloquer le trafic que vous cherchez à autoriser, car les règles de politique de sécurité risquent d'utiliser les ports par défaut des applications pour empêcher le trafic d'application d'utiliser des ports non standard. Par exemple, le trafic identifié en tant que trafic d'applications de navigation web (port 80 par défaut) pourrait comporter des applications sous-jacentes qui possèdent des ports par défaut différents, comme le trafic HTTPS (port par défaut 443). La règle par défaut de l'application bloque le trafic HTTPS, car il voit le trafic déchiffré au moyen d'un port « non standard » (443 plutôt que 80). En migrant vers des règles basées sur l'App-ID avant de déployer le déchiffrement, vous permettra, lorsque vous testerez votre déploiement de déchiffrement dans les POC, de découvrir les mauvaises configurations de la politique de sécurité et de les régler avant de procéder au déploiement à la population d'utilisateurs générale.***

Pour vous préparer au déploiement du déchiffrement :

- Travailler avec les parties prenantes au développement d'une stratégie de déploiement du déchiffrement
- Concevoir un plan de déploiement PKI
- Dimensionnez le déploiement du pare-feu de décryptage
- Prévoir un déploiement hiérarchisé et organisé

## Travailler avec les parties prenantes au développement d'une stratégie de déploiement du déchiffrement

Travaillez avec les parties prenantes, comme les services juridiques, les finances, les ressources humaines, les cadres supérieurs, la sécurité, les technologies de l'information et le soutien pour développer une stratégie de déploiement du déchiffrement. Commencez par obtenir les approbations nécessaires pour déchiffrer le trafic et ainsi sécuriser la société. Le déchiffrage du trafic

passe par la compréhension de l'incidence que les règlements juridiques et les besoins de l'entreprise ont sur ce que vous pouvez et ne pouvez pas déchiffrer.

Identifiez et hiérarchisez le trafic à déchiffrer. Il est recommandé de déchiffrer le plus de trafic possible pour obtenir une visibilité des menaces potentielles dans le trafic chiffré et prévenir ces menaces. Si le mauvais dimensionnement des pare-feu vous empêche de déchiffrer tout le trafic que vous souhaitez déchiffrer, hiérarchisez les serveurs les plus critiques, les catégories de trafic les plus risquées et les segments les moins fiables et les sous-réseaux IP. Pour faciliter la hiérarchisation, posez-vous des questions comme, « Que se passe-t-il si ce serveur est compromis ? » et « Quel niveau de risque suis-je prêt à assumer en ce qui concerne le niveau de rendement que je veux atteindre ? »

Ensuite, identifiez le trafic que vous ne pouvez pas déchiffrer parce qu'un site interrompt le déchiffrement pour des raisons techniques, comme un certificat épinglé, une chaîne de certificats incomplètes, des suites de chiffrement non prises en charge ou une authentification mutuelle. Les sites de déchiffrement qui interrompent le déchiffrement de manière technique finissent par bloquer ce trafic. Évaluez les sites Web qui interrompent le déchiffrement techniquement et demandez-vous si vous avez besoin d'accéder à ces sites pour des raisons d'affaires. Si vous n'avez pas besoin d'accéder à ces sites, autorisez le déchiffrement à les bloquer. Si vous avez besoin d'accéder à l'un de ces sites pour des raisons d'affaires, ajoutez-les à la liste d'exclusion du déchiffrement SSL pour les exclure du déchiffrement. La liste d'exclusion du déchiffrement SSL est destinée exclusivement aux sites qui interrompent le déchiffrement techniquement.

Identifiez le trafic sensible que vous ***choisissez*** de ne pas décrypter pour des raisons juridiques, réglementaires, personnelles ou autres, comme le trafic relatif aux services financiers, à la santé ou au gouvernement, ou encore le trafic de certains dirigeants. Il ne s'agit pas de trafic qui interrompt le déchiffrement techniquement. Vous ne devez donc pas utiliser la liste d'exclusion du déchiffrement SSL pour exclure ce trafic du déchiffrement. Créez plutôt une exclusion de déchiffrement basée sur une politique pour identifier et contrôler le trafic que vous choisissez de ne pas déchiffrer et appliquez le profil d'absence de déchiffrement à la politique pour empêcher les serveurs présentant des problèmes de certificats d'accéder au réseau. Les exclusions de déchiffrement basées sur les politiques visent unique le trafic que vous choisissez de ne pas déchiffrer.

Lorsque vous planifier une politique de déchiffrement, tenez compte des règles de conformité de la sécurité de votre entreprise, de la politique d'utilisation de l'ordinateur et des objectifs de votre entreprise. Des contrôles extrêmement stricts peuvent avoir une incidence sur l'expérience utilisateur en empêchant l'accès à des sites non commerciaux auxquels l'utilisateur pouvait anciennement accédé. Ils peuvent toutefois être requis pour des institutions gouvernementales ou financières. Il y a toujours un compromis à faire entre l'exploitabilité, les activités de gestion et la sécurité. Plus la politique de déchiffrement est stricte, plus il est probable qu'un site Web devienne inaccessible, ce qui peut entraîner des plaintes des utilisateur et modifier la base de règles.

***Bien qu'une politique de déchiffrement stricte puisse initialement entraîner quelques plaintes d'utilisateurs, ces plaintes peuvent attirer votre attention sur les sites Web non autorisés ou indésirables qui sont bloqués parce qu'ils utilisent des algorithmes faibles ou qu'ils présentent des problèmes de certificat. Utilisez les plaintes comme des outils pour avoir une meilleure compréhension du trafic sur votre réseau.***

Il se peut que différents groupes d'utilisateurs, et même différents utilisateurs individuels, doivent faire l'objet de politiques de déchiffrement différentes. Vous pourriez également souhaiter appliquer la même politique de déchiffrement pour tous les utilisateurs. Par exemple, les dirigeants peuvent être exemptés des politiques de déchiffrement qui s'appliquent à d'autres employés. Et vous pourriez

souhaiter appliquer différentes politiques de déchiffrement aux groupes d'employés, aux contrats, aux partenaires et aux invités. Préparez les politiques relatives à l'utilisation des ordinateurs par les RH et les services juridiques pour les distribuer à tous les employés, sous-traitants, partenaires, invités et les autres utilisateurs du réseau. Ainsi, lorsque vous déployez le déchiffrement, les utilisateurs comprennent que leurs données peuvent être déchiffrées et qu'elles peuvent faire l'objet d'une analyse visant à y déceler des menaces.

*Votre façon de gérer les utilisateurs invités dépend de l'accès dont ils ont besoin. Isolez les invités du reste de votre réseau en les plaçant sur un VLAN séparé et sur un SSID séparé pour l'accès sans fil. Si les invités n'ont pas à accéder à votre réseau d'entreprise, ne les laissez pas y pénétrer, et vous n'aurez pas besoin de déchiffrer leur trafic. Si les invités ont besoin d'accéder à votre réseau d'entreprise, déchiffrez leur trafic :*

- *Les entreprises ne contrôlent pas les périphériques des invités. Déchiffrez le trafic des invités et soumettez-le à votre politique de sécurité relative aux invités afin que le pare-feu puisse inspecter le trafic et prévenir les menaces. Pour ce faire, redirigez les utilisateurs invités via un portail d'authentification, montrez-leur comment télécharger et installer le certificat de l'autorité de certification et informez-les clairement que leur trafic sera déchiffré. Incluez le processus dans la politique d'utilisation des ordinateurs et dans la politique de confidentialité de votre société.*
- *Créez des règles de politique de déchiffrement et des règles de politique de sécurité pour contrôler étroitement l'accès des invités afin que ces derniers ne puissent accéder qu'aux zones de votre réseau auxquelles ils doivent accéder.*

Comme c'est le cas pour différents groupes d'utilisateurs, décidez quels périphériques vous souhaitez déchiffrer et quelles applications vous souhaitez déchiffrer. Les réseaux d'aujourd'hui prennent non seulement en charge les périphériques d'entreprise, mais également les périphériques BYOD, mobiles, distants, etc., y compris les périphériques des entrepreneurs, des partenaires et des invités. De nos jours, les utilisateurs tentent d'accéder à de nombreux sites, qu'ils soient approuvés ou non approuvés, et vous devez décider quelle proportion de ce trafic vous voulez déchiffrer.

*Les entreprises ne contrôlent pas les périphériques BYOD. Si vous autorisez les périphériques BYOD sur votre réseau, déchiffrez leur trafic et soumettez-le à la même règle de sécurité que vous appliquez à tout autre trafic sur le réseau, de sorte que le pare-feu puisse inspecter le trafic et prévenir les menaces. Pour ce faire, redirigez les utilisateurs BYOD via un portail d'authentification, montrez-leur comment télécharger et installer le certificat de l'autorité de certification et informez-les clairement que leur trafic sera déchiffré. Informez les utilisateurs BYOD du processus et incluez-le dans la politique d'utilisation des ordinateurs et dans la politique de confidentialité de votre société.*

Décidez le trafic que vous souhaitez journaliser et enquêtez sur le trafic que vous pouvez journaliser. Soyez au courant des lois locales concernant le type de données que vous pouvez journaliser et stocker ainsi que l'endroit où journaliser et stocker les données. Par exemple, les lois locales peuvent empêcher la journalisation et le stockage des informations personnelles, comme les données financières et relatives à la santé.

Décidez comment vous souhaitez gérer les mauvais certificats. Par exemple, souhaitez-vous bloquer ou autoriser les sessions dont l'état du certificat est inconnu ? Lorsque vous comprenez comment vous voulez gérer les mauvais certificats, cela vous permet de détermine la manière dont vous

configurez les profils de déchiffrement que vous associez aux politiques de déchiffrement pour contrôler les sessions que vous autorisez selon l'état de vérification du certificat du serveur.

## Concevoir un plan de déploiement PKI

Planifiez le déploiement de votre Public Key Infrastructure (infrastructure à clé publique ; ICP). Les périphériques réseau ont besoin d'un certificat CA d'approbation de transfert SSL pour les sites approuvés et d'un certificat CA de non-approbation de transfert SSL pour les sites non approuvés. Générez les certificats d'approbation de transfert et les certificats de non-approbation de transfert distincts (ne signez pas le certificat d'approbation de transfert avec la CA racine d'entreprise, car vous voulez que le certificat de non-approbation avertisse les utilisateurs qu'ils essaient d'accéder à des sites potentiellement dangereux). Les pare-feu de nouvelle génération Palo Alto Networks offrent deux façons de générer des certificats CA pour le déchiffrement SSL :

- **Générez les certificats CA SSL de votre CA racine d'entreprise en tant que certificats subordonnés** : si vous disposez d'une PKI d'entreprise existante, c'est la meilleure pratique à suivre. La génération d'un certificat subordonné d'une CA racine d'entreprise facilite le déploiement et le rend plus fluide, car les périphériques réseau approuvent déjà la CA racine d'entreprise, vous évitez donc tout problème de certificat lorsque vous commencez la phase de déploiement. Si vous ne disposez pas d'une CA racine d'entreprise, songez à en obtenir une.
- **Générez un certificat CA racine auto-signé sur le pare-feu et créez des certificats CA subordonnés sur ce pare-feu** : si vous n'avez pas une CA racine d'entreprise, cette méthode vous fournit un certificat CA racine auto-signé et les certificats d'approbation de transfert et de non-approbation de transfert subordonnés. Avec cette méthode, vous devez installer les certificats auto-signés sur tous vos périphériques réseau afin que ces périphériques reconnaissent les certificats auto-signés du pare-feu. Puisque les certificats doivent être déployés sur tous les périphériques, cette méthode convient mieux aux petits déploiements et aux tests de preuve de concept (POC) qu'aux grands déploiements.

*N'exportez pas le certificat de non-approbation de transfert dans les listes d'approbation de certificats des périphériques de votre réseau! C'est essentiel, car lorsque vous installez le certificat de non-approbation dans la liste de confiance, les périphériques approuvent des sites Web qui ne le pare-feu n'approuve pas. De plus, les utilisateurs ne voient pas les avertissements de certificat pour les sites non approuvés, ils ne sauront donc pas que les sites ne sont pas approuvés et pourront y accéder, ce qui pourrait exposer votre réseau aux menaces.*

*Que vous génériez des certificats d'approbation de transfert depuis votre CA racine d'entreprise ou que vous utilisiez un certificat auto-signé généré sur le pare-feu, générez un certificat d'autorité de confiance d'approbation de transfert subalterne distinct pour chaque pare-feu. La souplesse d'utiliser des CA subordonnées distincts vous permet de* révoquer *un certificat lorsque vous mettez un périphérique (ou une paire de périphériques) hors service sans affecter le reste du déploiement et réduit l'impact dans toutes les situations où vous avez besoin de révoquer un certificat. Les CA d'approbation de transfert distincts sur chaque pare-feu aident également à résoudre les problèmes, parce que le message d'erreur de la CA que l'utilisateur voit comprend des informations sur le trafic qui traverse le pare-feu. Si vous utilisez la même CA d'approbation de transfert sur chaque pare-feu, vous perdez la granularité de l'information.*

L'utilisation de différents certificats de non-approbation de transfert sur différents pare-feu ne procurent aucun avantage. Vous pouvez donc utiliser le même certificat de non-approbation de transfert sur tous les pare-feu. Si vous avez besoin d'une sécurité supplémentaire pour vos clés privées, envisagez de les stocker sur un HSM.

Vous pouvez prendre des dispositions spéciales pour les utilisateurs invités. Si les utilisateurs invités n'ont pas besoin d'accéder à votre réseau d'entreprise, n'autorisez pas l'accès. Ainsi, vous n'aurez pas à déchiffrer leur trafic ni à créer l'infrastructure pour soutenir l'accès des invités. Si vous devez soutenir les utilisateurs invités, discutez avec votre service juridique afin de savoir si vous pouvez déchiffrer le trafic des invités.

Si vous pouvez déchiffrer le trafic des invités, traitez les invités de la même façon que vous traiter les périphériques BYOD. Déchiffrez le trafic des invités et soumettez-le à la même politique de sécurité que vous appliquez à tout autre trafic sur le réseau. Pour ce faire, il faut rediriger les utilisateurs invités vers un portail d'authentification, leur indiquer comment télécharger et installer le certificat CA et les informer clairement que leur trafic sera décrypté. Incluez le processus dans la politique d'utilisation des ordinateurs et dans la politique de confidentialité de votre société. De plus, restreignez le trafic des invités uniquement aux zones auxquelles les invités doivent accéder.

Si vous ne pouvez déchiffrer le trafic des invités pour des raisons juridiques, isolez alors le trafic des invités et empêcher-le de se déplacer latéralement au sein de votre réseau :

- Créez une zone distincte pour les invités et restreignez l'accès des invités à cette zone. Pour empêcher les mouvements latéraux, n'autorisez pas l'accès des invités aux autres zones.
- N'autorisez que les applications autorisées, utilisez le filtrage des URL pour empêcher l'accès à des catégories d'URL risquées et appliquez les profils de sécurité exemplaires.
- Appliquez un profil d'absence de déchiffrement à la politique pour empêcher les invités d'accéder aux sites Web possédant des CA inconnus ou expirés.

Tous les employés, agents contractuels, partenaires et autres utilisateurs doivent utiliser votre infrastructure d'entreprise ordinaire, et vous devriez déchiffrer et inspecter leur trafic.

## Dimensionnez le déploiement du pare-feu de décryptage

Le déchiffrement du trafic chiffré consomme les ressources du processeur du pare-feu et peut affecter le débit. En général, plus la sécurité est serrée (plus le trafic SSL que vous déchiffrez et plus les paramètres de votre protocole seront stricts), plus le déchiffrement consomme des ressources du pare-feu. Travaillez avec votre SE/CE Palo Alto Networks SE/CE pour dimensionner le déploiement de votre pare-feu et éviter les erreurs de dimensionnement. Les facteurs qui affectent la consommation des ressources de déchiffrement et, par conséquent, le volume de trafic que le pare-feu peut déchiffrer sont les suivants :

- La quantité de trafic SSL que vous souhaitez déchiffrer. Celui-ci varie d'un réseau à l'autre. Par exemple, certaines applications doivent être déchiffrées pour empêcher l'injection de programmes malveillants ou d'exploitations dans le réseau ou les transferts de données non autorisés, certaines applications ne peuvent pas être déchiffrées en raison des lois et des règlements locaux ou pour des raisons commerciales, et d'autres applications sont en texte clair (non chiffré) et n'ont pas besoin d'être déchiffrées. Plus le trafic que vous souhaitez décrypter est important, plus vous aurez besoin de ressources.

- La version du protocole TLS. Les versions supérieures sont plus sécuritaires mais consomment plus de ressources. Utilisez la version de protocole TLS la plus élevée possible pour optimiser la sécurité.
- La taille de la clé. Plus la taille de la clé est grande, meilleure est la sécurité, et plus le traitement de la clé consomme de ressources.
- L'algorithme d'échange de clés Les algorithmes d'échange de clés éphémères Perfect Forward Secrecy (Confidentialité de transmission parfaite ; PFS) tels que Diffie-Hellman Ephemeral (DHE) Elliptic-Curve Diffie-Hellman Exchange (Diffie-Hellman basé sur les courbes elliptiques éphémères ; ECDHE) utilisent davantage de ressources de traitement que les algorithmes RSA. Les algorithmes d'échange de clés PFS offrent une sécurité accrue par rapport aux algorithmes d'échange de clés RSA, car le pare-feu doit générer une nouvelle clé de chiffrement pour chaque session. Toutefois, sa génération consomme plus de ressources du pare-feu. Par contre, si un attaquant compromet une clé de session, PFS l'empêche de l'utiliser pour déchiffrer toute autre session entre le même client et le même serveur, contrairement à RSA.
- L'algorithme de chiffrement. L'algorithme d'échange de clés détermine si l'algorithme de chiffrement est PFS ou RSA.
- La méthode d'authentification par certificat. RSA (et non pas l'algorithme d'échange de clés RSA) consomme moins de ressources que le Elliptic Curve Digital Signature Algorithm (Algorithme de signature numérique à courbe elliptique ; ECDSA), mais ECDSA est plus sécurisé.

  ***La combinaison de l'algorithme d'échange de clés et de la méthode d'authentification par certificat affecte le débit de traitement, comme indiqué dans les*** tests de référence ***de RSA et ECDSA. Le coût de traitement de PFS est compensé par la sécurité plus élevée que celle que procure PFS, mais PFS pourrait ne pas être nécessaire pour tous les types de trafic. Vous pouvez enregistrer les cycles du processeur du pare-feu en utilisant RSA pour le trafic que vous souhaitez déchiffrer et inspecter afin d'y détecter les menaces, mais qui n'est pas sensible.***

- Taille moyenne des transactions. Par exemple, les types de transactions moyennes faibles ont besoin d'une plus grande puissance de traitement pour le déchiffrement. Mesurez la taille des transactions moyennes de tout le trafic, puis mesurez la taille des transactions moyennes du trafic sur le port 443 (le port par défaut pour le trafic HTTPS chiffré) pour comprendre la portion du trafic chiffré qui passe par le pare-feu par rapport au trafic total ainsi que les tailles moyennes des transactions. Éliminez les valeurs aberrantes comme les opérations inhabituellement importantes pour obtenir une mesure plus juste de la taille moyenne des transactions.
- Le modèle et les ressources du pare-feu. Les nouveaux modèles de pare-feu offrent plus de puissance de traitement que les anciens modèles.

La combinaison de ces facteurs détermine la consommation des ressources de traitement du pare-feu par le déchiffrement. Pour exploiter les ressources du pare-feu au mieux, comprenez les risques que comportent les données que vous protégez. Si les ressources du pare-feu sont un enjeu, utilisez un déchiffrement plus fort pour le trafic de priorité absolue et utilisez un déchiffrement moins exigeant pour le processeur pour déchiffrer et inspecter le trafic de moindre priorité jusqu'à ce que vous puissiez accroître les ressources disponibles. Par exemple, vous pouvez utiliser RSA au lieu de ECDHE et ECDSA pour le trafic non sensible ou hautement prioritaire, afin de préserver les ressources de pare-feu lors de l'utilisation du déchiffrement basé sur PFS pour un trafic sensible de priorité supérieure. (Vous continuez à déchiffrer et à inspecter le trafic de priorité inférieure, mais vous utilisez des algorithmes moins sécurisés que PFS.) La clé consiste à comprendre les risques que présentent différents types de trafic et de les traiter en conséquence.

Mesurez la capacité de traitement du pare-feu afin de comprendre les ressources qui sont actuellement disponibles, ce qui vous aidera à déterminer si vous avez besoin d'accroître les ressources du pare-feu pour déchiffrer le trafic que vous souhaitez déchiffrer. La mesure de la capacité de traitement du pare-feu définit également une base de comparaison de la capacité de traitement après le déploiement du déchiffrement.

Lorsque vous dimensionnez le déploiement du pare-feu, fiez-vous non seulement à vos besoins actuels, mais également à vos besoins futurs. Prévoyez une marge de manœuvre pour la croissance du trafic de déchiffrement, car Gartner prédit que jusqu'en 2019, plus de 80 % du trafic Web des entreprises sera chiffré et que plus de 50 % des nouvelles campagnes malveillantes utiliseront diverses formes de chiffrement. Travaillez de concert avec vos représentants de Palo Alto Networks et profitez de leur expérience en dimensionnement de pare-feu pour vous aider à dimensionner le déploiement de déchiffrement de votre pare-feu.

## Prévoir un déploiement hiérarchisé et organisé

Planifiez le déploiement du déchiffrement d'une manière contrôlée, morceau par morceau. Ne déployez pas votre déploiement de déchiffrement complètement d'une seule fois. Testez le déchiffrement et assurez-vous qu'il fonctionne comme prévu et que les utilisateurs comprennent ce que vous faites et pourquoi. Le déploiement du déchiffrement de cette manière facilite le dépannage si le déploiement ne fonctionne pas comme prévu et aide les utilisateurs à s'adapter aux changements.

Il est essentiel d'informer les parties prenantes, les employés et les autres utilisateurs, comme les entrepreneurs et les partenaires, car les paramètres de déchiffrement peuvent changer leur capacité à accéder à certains sites Web. Les utilisateurs devraient comprendre comment répondre à des situations dans lesquelles des sites Web accessibles deviennent inaccessibles et les informations à donner au soutien technique. Le soutien doit comprendre le déploiement et comment aider les utilisateurs qui son confrontés à des problèmes. Avant de déployer le déchiffrement à la population générale :

- Identifiez les adopteurs précoces pour favoriser la promotion du déchiffrement et les personnes qui seront en mesure d'aider d'autres employés qui ont des questions tout au long du déploiement complet. Mobilisez les directeurs des services et aidez-les à comprendre les avantages du déchiffrement du trafic.
- Établissez les tests de Proof-Of-Concept (preuve de concept ; POC) dans chaque service avec les adopteurs précoces et les autres employés qui comprennent l'importance du déchiffrement du trafic. Informez les participants à la POC et de la manière de communiquer avec le soutien technique s'ils sont confrontés à des problèmes. Ainsi, les POC du déchiffrement deviennent une occasion de travailler avec le soutien technique pour tester la manière de soutenir le déchiffrement et de développer la méthode la moins souffrante de soutenir le déploiement général. L'interaction entre les utilisateurs de la POC et le soutien technique vous autorise également à peaufiner les politiques et la manière de communiquer avec les utilisateurs.

  Les POC vous autorisent à expérimenter la hiérarchisation et de déterminer ce que vous devez déchiffrer en premier. Ainsi, lorsque vous mettez en œuvre le déchiffrement auprès de la population générale, votre expérience POC vous aide à comprendre la manière de mettre en œuvre le déchiffrement de différentes catégories d'URL. Mesurez la manière dont le déchiffrement affecte l'utilisateur du processeur et de la mémoire du pare-feu pour vous aider à comprendre si le dimensionnement du pare-feu est bon ou si vous devez procéder à une mise à niveau. Les POC peuvent également révéler les applications qui interrompent le déchiffrement

techniquement (leur déchiffrement bloque leur trafic) et qui doivent être ajoutées à la liste d'exclusion de déchiffrement.

Lorsque vous définissez des POC, vous devez également définir un groupe d'utilisateurs qui peut attester de l'état de préparation opérationnelle et des procédures avant le déploiement général.

- Informez la population d'utilisateurs avant le déploiement général, et planifiez d'informer les nouveaux utilisateurs lorsqu'ils joignent l'entreprise. Il s'agit d'une phase critique du déploiement du déchiffrement, car le déploiement peut affecter des sites Web que les utilisateurs visitaient anciennement, mais qui ne sont pas sécuritaires. Ces sites ne sont donc plus accessibles. L'expérience POC permet de déterminer les points les plus importants à communiquer.
- Déployez le déchiffrement. Vous pouvez procéder de plusieurs façons. Vous pouvez déchiffrer le trafic de priorité absolue dans un premier temps (par exemple, les catégories d'URL les plus susceptibles de contenir du trafic malveillant, comme les jeux), puis d'en déchiffrer davantage lorsque vous acquérez de l'expérience. Vous pouvez éventuellement adopter une approche plus prudente et déchiffrer les catégories d'URL qui n'affectent pas votre entreprise dans un premier temps (ainsi, si quelque chose ne se passe pas comme prévu, aucun problème affectant l'entreprise ne se produit), par exemple, de nouveaux fils d'attente. Dans tous les cas, la meilleure façon de déployer le déchiffrement consiste à déchiffrer quelques catégories d'URL, de tenir compte des commentaires des utilisateurs, d'exécuter les rapports pour s'assurer que le déchiffrement fonctionne comme prévu, puis de graduellement déchiffrer quelques catégories d'URL supplémentaires, de les vérifier, etc. Planifiez de faire des exclusions de déchiffrement pour exclure les sites du déchiffrement, si vous ne pouvez les déchiffrer pour des raisons techniques ou parce que vous choisissez de ne pas les déchiffrer.

  Si vous procédez à l'Activation de l'exclusion de décryptage SSL par les utilisateurs (les utilisateurs voient une page de réponse qui les autorise à exclure le déchiffrement et à mettre fin à la session sans se rendre au site ou à accéder au site et à accepter le déchiffrement du trafic), expliquer aux utilisateurs de quoi il s'agit, pourquoi ils voient cette information et les options qui s'offrent à eux.
- Créez des calendriers de déploiement réalistes qui donnent le temps d'évaluer chaque étape du déploiement.

***Positionnez les pare-feu de manière à ce qu'ils puissent voir tout le trafic du réseau et ainsi veiller à ce qu'aucun trafic non chiffré ne puisse obtenir accès à votre réseau en contournant le pare-feu.***

# Définition du trafic à décrypter

Une règle de politique déchiffrement vous permet de définir le trafic que vous souhaitez que le pare-feu déchiffre et de définir le trafic que vous choisissez d'exclure du déchiffrement, car il est personnel ou en raison des règlements locaux, par exemple.

Associez un profil de déchiffrement à chaque règle de politiques de déchiffrement pour permettre les vérifications des certificats, les vérifications des modes de session, les vérification des échecs et les vérifications des protocoles et des algorithmes, selon le profil. Ces vérifications empêchent les connexions risquées, telles que des session comportant des émetteurs de certificats non approuvés, des protocoles, des suites de chiffrement et des algorithmes faibles ainsi que les serveurs qui présentent des problèmes de certificat.

***Passez en revue la** liste de contrôle des meilleures pratiques de déploiement du décryptage **pour vous assurer que vous comprenez les meilleures pratiques recommandées.***

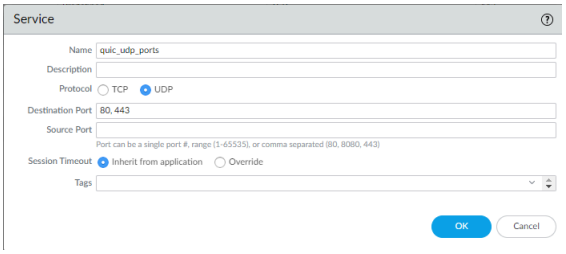
Bloquez les catégories de filtrage des URL dangereuses qui sont connues, notamment les logiciels malveillants, le hameçonnage, les DNS dynamiques, les inconnus, les commandes et contrôles, les contournements de proxy et anonymiseurs, la violation des droits d'auteur, l'extrémisme, les domaines récemment enregistrés, les logiciels indésirables et les domaines en parkings. Si vous devez autoriser l'une de ces catégories pour des raisons professionnelles, décryptez-la et appliquez des profils de sécurité stricts au trafic.

Voici certaines catégories d'URL que vous devez toujours déchiffrer si vous les autorisez : stockage en ligne et de secours, messagerie Web, hébergement Web, sites personnels et blogues et réseaux de diffusion de contenu.

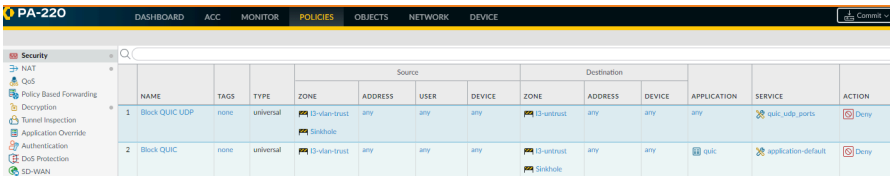
 

*Dans la politique de sécurité, bloquez le protocole Quick UDP Internet Connections (QUIC), sauf pour des raisons d'affaires, si vous voulez autoriser le trafic du navigateur chiffré. Chrome et certains autres navigateurs établissent des sessions au moyen du protocole QUIC au lieu du protocole TLS, mais QUIC utilise un chiffrement propriétaire que le pare-feu ne peut déchiffrer ; le trafic potentiellement dangereux peut alors entrer sur le réseau en tant que trafic chiffré. En bloquant le protocole QUIC, vous forcez le navigateur à utiliser le protocole TLS, ce qui permet au pare-feu de déchiffrer le trafic.*

*Créez une règle de politique de sécurité pour bloquer le protocole QUIC sur ses ports de service UDP (80 et 443) et créez une règle distincte pour bloquer l'application QUIC. Pour la règle qui bloque les ports UDP 80 et 443, créez un service (**Objects [Objets]** > **Services**) qui inclut les ports UDP 80 et 443:*




*Utilisez le service pour spécifier les ports UDP à bloquer pour QUIC. Dans la deuxième règle, bloquez l'application QUIC :*




- Création d'un profil de décryptage
- Création d'une règle de politique de décryptage

# Création d'un profil de décryptage

Un profil de déchiffrement vous permet d'effectuer des vérifications du trafic déchiffré et du trafic SSL que vous avez ***décidé*** d'exclure du déchiffrement. (Si un serveur interrompt le déchiffrement SSL techniquement en raison de l'épinglage du certificat ou d'une autre raison, ajoutez le serveur à la liste d'exclusion du déchiffrement.) Selon vos besoins, créez des profils de déchiffrement pour :

- Bloquer des sessions en fonction de l'état du certificat, y compris bloquer des sessions comportant des certificats expirés, des émetteurs non approuvés, un certificat dont l'état est inconnu et des extensions de certificat de même qu'à l'expiration de la vérification de l'état du certificat.
- Bloquer les sessions comportant des versions et des suites de chiffrement non prises en charge qui exigent l'utilisation de l'authentification du client.
- Bloquer des sessions si les ressources nécessaires pour effectuer le déchiffrement ne sont pas disponibles ou si un module de sécurité matériel n'est pas disponible pour signer les certificats.
- Définir les versions de protocoles et les algorithmes d'authentification, de chiffrement et d'échange de clés permis pour le proxy de transfert SSL et le trafic d'inspection SSL entrante dans les paramètres du protocole SSL.

N'affaiblissez pas le profil de déchiffrement principal qui vous appliquez à la plupart des sites pour répondre aux besoins des sites plus faibles. Créez plutôt un ou plusieurs profils de déchiffrement distincts pour les sites que vous devez prendre en charge, mais qui ne prennent pas en charge les suites de chiffrement et les algorithmes forts. Vous pouvez également créer différents profils de déchiffrement pour différentes catégories d'URL afin d'affiner la sécurité par rapport à la performance pour le trafic qui ne contient aucune donnée sensible ; cependant, vous devriez toujours déchiffrer et inspecter tout le trafic que vous pouvez déchiffrer.

Lorsque vous avez créé le profil de déchiffrement, associez-le à une politique de déchiffrement ; le pare-feu applique les paramètres du profil de déchiffrement au trafic mis en correspondance avec la règle de politique de déchiffrement.

Les pare-feu Palo Alto Networks comprennent un profil de déchiffrement par défaut que vous pouvez utiliser pour appliquer les versions de base des protocoles recommandés et les suites de déchiffrement. Cependant, il est recommandé d'activer des contrôles de déchiffrement plus rigoureux, comme décrit dans les rubriques Profil de décryptage du proxy de transfert SSL, Profil de décryptage d'inspection entrante SSL et Paramètre des profil de décryptage SSL.

***Évitez d'appuyer des protocoles ou algorithmes faibles parce qu'ils contiennent des vulnérabilités connues que les pirates peuvent exploiter. Si vous devez autoriser un protocole ou un algorithme plus faible pour soutenir un partenaire ou un entrepreneur clé qui utilise les anciens systèmes présentant des protocoles faibles, créez un profil de déchiffrement distinct pour l'exception et associez-le à une politique de déchiffrement qui applique le profil uniquement au trafic pertinent (par exemple, l'adresse IP source du partenaire). N'autorisez pas le protocole faible pour l'ensemble du trafic.***

**STEP 1 |** Créez un nouveau profil de déchiffrement.

Sélectionnez **Objects (Objets)** > **Decryption Profile (Profil de déchiffrement)**, **Add (Ajoutez)** ou modifiez une règle de profil de déchiffrement, et donnez à la règle un **Name (Nom)** descriptif.

**STEP 2 |** (Facultatif) Autorisez le **Shared (Partage)** de la règle de profil sur tous les systèmes virtuels d'un pare-feu ou tous les groupes de périphériques de Panorama.

**STEP 3 |** (Mise en miroir du déchiffrement uniquement) Activez une interface ethernet que le pare-feu doit utiliser pour copier et transférer le trafic déchiffré.

En plus de cette tâche, suivez les étapes pour effectuer la configuration de la mise en miroir du port de décryptage. Soyez au fait des règlements sur la protection des renseignements personnels qui peuvent interdire la mise en miroir ou contrôler le type de trafic que vous pouvez

mettre en miroir. La mise en miroir du port de déchiffrement nécessite une licence de mise en miroir du port de déchiffrement.

**STEP 4 |** (Facultatif) Bloquez et contrôlez le trafic par tunnel SSL et/ou le trafic entrant :

*Bien qu'il soit facultatif d'appliquer un profil de déchiffrement au trafic déchiffré, il est recommandé de toujours appliquer un profil de déchiffrement aux règles de politique afin de protéger votre réseau contre les menaces chiffrées. Vous ne pouvez vous protéger des menaces que vous ne voyez pas.*

Sélectionnez **SSL Decryption (Déchiffrement SSL)** :

- Sélectionnez **SSL Forward Proxy (Proxy de transfert SSL)** pour configurer les paramètres pour vérifier les certificats, appliquer les versions du protocole et les suites de cryptage et effectuer la vérification des défaillances du trafic SSL déchiffré. Ces paramètres ne sont actifs que lorsque ce profil est associé à une règle de politique de déchiffrement qui est configurée pour effectuer le déchiffrement du proxy de transfert SSL.
- Sélectionnez **SSL Inbound Inspection (Inspection SSL entrante)** pour configurer les paramètres pour appliquer les versions du protocole et les suites de cryptage et effectuer la vérification des défaillances du trafic SSL entrant. Ces paramètres ne sont actifs que lorsque ce profil est associé à une règle de politique de déchiffrement qui effectue l'inspection SSL entrante.
- Sélectionnez **SSL Protocol Settings (Paramètres du protocole SSL)** pour configurer les paramètres qui contrôlent les versions minimales et maximales du protocole ainsi que l'échange de clé, le chiffrement et les algorithmes d'authentification à appliquer au trafic SSL déchiffré. Ces paramètres sont actifs lorsque ce profil est associé à des règles de politique de déchiffrement qui sont configurées pour effectuer le déchiffrement du proxy de transfert SSL ou l'inspection SSL entrante.

*Si le pare-feu est en mode FIPS-CC et géré par un serveur d'administration Panorama™ en mode standard, un profil de déchiffrement doit être créé localement sur le pare-feu. Les profils de déchiffrement créés sur Panorama en mode standard contiennent des références aux algorithmes de chiffrement **3DES** et **RC4** et à l'algorithme d'authentification **MD5** qui ne sont pas pris en charge et provoquent l'échec des poussées vers le pare-feu géré.*

**STEP 5 |** (Facultatif) Bloquez et contrôlez le trafic (par exemple, une catégorie d'URL) pour lequel vous avez choisi de créer une exclusion de déchiffrement basée sur une politique.

*Bien qu'il soit facultatif d'appliquer un profil de déchiffrement au trafic que vous décidez de déchiffrer, il est recommandé de toujours appliquer un profil de déchiffrement aux règles de politique afin de protéger votre réseau contre les sessions comportant des certificats expirés ou des émetteurs non approuvés.*

Sélectionnez **No Decryption (Absence de déchiffrement)** pour configurer le Profil pour l'absence de déchiffrement, puis cochez les cases **Block sessions with expired certificates (Bloquer les sessions avec des certificats expirés)** et **Block sessions with untrusted issuers (Bloquer les sessions avec des émetteurs non approuvés)** pour valider les certificats applicables au trafic qui est exclu du déchiffrement. Créez des exclusions basées sur les politiques uniquement pour le trafic que vous choisissez de ne pas déchiffrer. Si un serveur interrompt le déchiffrement pour

des raisons techniques, ajoutez le serveur à la liste d'exclusion du déchiffrement SSL (**Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **SSL Decryption Exclusion (Exclusions de déchiffrement SSL)**).

Ces paramètres ne sont actifs que lorsque le profil de déchiffrement est associé à une règle de politique de déchiffrement qui désactive le déchiffrement de certain types de trafic.

**STEP 6 |** (Facultatif) Bloquez et contrôlez le trafic SSH déchiffré.

Sélectionnez **SSH Proxy (Proxy SSH)** et configurez le Profil de décryptage SSL et configurez les paramètres pour appliquer les versions du protocole prises en charge et pour bloquer les sessions si les ressources du système ne sont pas disponibles pour effectuer le déchiffrement.

Ces paramètres ne sont actifs que lorsque le profil de déchiffrement est associé à une règle de politique de déchiffrement qui déchiffre le trafic SSH.

**STEP 7 |** Ajoutez le profil de déchiffrement lorsque vous créez une règle de politique de déchiffrement.

Le pare-feu applique le profil de déchiffrement aux paramètres du profil et les appliquer au trafic mis en correspondance avec la règle de politique de déchiffrement.

**STEP 8 |** **Commit (Validez)** la configuration.

## Création d'une règle de politique de décryptage

Créez une règle de politique de décryptage pour définir le trafic que le pare-feu doit déchiffrer et le type de déchiffrement que vous souhaitez que le pare-feu effectue : Décryptage du proxy de transfert SSL, de l'inspection SSL entrante ou du proxy SSH. Vous pouvez également utiliser une politique de décryptage pour définir la mise en miroir du décryptage.

**STEP 1 |** Ajoutez une nouvelle règle de politique de déchiffrement.

Sélectionnez **Policies (Politiques)** > **Decryption (Déchiffrement)**, **Add (Ajoutez)** une nouvelle règle de politique de déchiffrement et donnez à la règle de la politique un **Name (Nom)** descriptif.

**STEP 2 |** Configurez la règle de déchiffrement à faire correspondre au trafic selon le réseau et les objets de la politique :

- **Zones de sécurité du pare-feu** : Sélectionnez **Source (Source)** et/ou **Destination (Destination)** et faites correspondre au trafic selon la **Source Zone (Zone source)** et/ou la **Destination Zone (Zone de destination)**.
- **Adresse IP, objets d'adresse et/ou groupes d'adresses** : Sélectionnez **Source (Source)** et/ou **Destination (Destination)** à faire correspondre au trafic selon la **Source Address (Adresse source)** et/ou la **Destination Address (Adresse de destination)**. Éventuellement, sélectionnez **Negate (Refuser)** pour exclure la liste des adresses source du décryptage.
- **Utilisateurs** : Sélectionnez **Source (Source)** et définissez le **Source User (Utilisateur source)** pour qui déchiffrer le trafic. Vous pouvez déchiffrer un utilisateur ou un groupe de trafic donné ou déchiffrer le trafic de certains types d'utilisateurs, comme les utilisateurs connus ou les utilisateurs en pré-ouverture de session (utilisateurs qui sont connectés à GlobalProtect, mais qui n'ont pas encore ouvert de session).
- **Ports et protocoles** : Sélectionnez **Service/URL Category (Catégorie de service/d'URL)** pour définir la règle à faire correspondre au trafic selon le service. Par défaut, la règle de la politique est configurée pour déchiffrer **Any (Tout)** trafic sur les ports TCP et UDP. Vous

pouvez **Add (Ajouter)** un service ou un groupe de services et, éventuellement, définir la règle sur **application-default (par défaut de l'application)** pour faire correspondre aux applications uniquement sur les ports par défaut des applications.

*Le paramètre par défaut de l'application peut être utile lorsque vous procédez à la* création d'une exclusion de déchiffrement basée sur une politique*. Vous pouvez exclure du déchiffrement les applications transitant par leurs ports par défaut, tout en continuant de déchiffrer les mêmes applications lorsqu'elles sont détectées sur des ports non standard.*

- **URL et catégories d'URL** : sélectionnez Service/URL Category (Catégorie de service/d'URL) et déchiffrez le trafic en fonction de :
  - Une liste d'URL hébergée à l'externe que le pare-feu récupère pour la mise en œuvre des politiques (référez-vous à **Objects (Objets)** > **External Dynamic Lists (Listes dynamiques externes)**).
  - Les catégories d'URL prédéfinies de Palo Alto Networks, qui facilitent le déchiffrement de catégories complètes de trafic autorisé. Cette option s'avère également utile lorsque vous créer des exclusions de déchiffrement basées sur les politiques, car vous pouvez exclure des sites sensibles en fonction de la catégorie plutôt qu'individuellement. Par exemple, bien que vous puissiez créer une catégorie d'URL personnalisée pour regrouper les sites que vous ne voulez pas déchiffrer, vous pouvez exclure les sites relatifs à la finance ou à la santé du déchiffrement selon les catégories d'URL prédéfinies de Palo Alto Networks. De plus, vous pouvez bloquer des catégories d'URL risquées et créer des pages Confort pour communiquer la raison pour laquelle les sites sont bloqués ou pour procéder à l'activation de l'exclusion de décryptage SSL par les utilisateurs.

    Vous pouvez utiliser les catégories d'URL à risque élevé et à risque modéré prédéfinies pour créer une règle de politique de décryptage qui déchiffre tout le trafic URL à risque élevé ou à risque modéré. Placez la règle au bas de la base de règle (toutes les exceptions de déchiffrement doivent se trouver au-dessus de cette règle pour éviter que vous ne déchiffriez de l'information de nature délicate) comme filet de sécurité pour veiller à déchiffrer et à inspecter tout le trafic risqué. Cependant, si des sites à risque modéré ou élevé auxquels vous autorisez l'accès contiennent des informations personnelles identifiables ou d'autres informations de nature délicate que vous ne voulez pas déchiffrer, vous devez soit bloquer ces sites pour éviter d'autoriser du trafic chiffré présentant des risques tout en évitant les problèmes de confidentialité, soit créer une règle d'absence de déchiffrement pour gérer le trafic de nature délicate.
  - Des catégories d'URL personnalisées (voir **Objects (Objets)** > **Custom Objects (Objets personnalisés)** > **URL Category (Catégorie d'URL)**). Par exemple, vous pouvez créer une catégories d'URL personnalisée pour spécifier un groupe de sites auquel vous devez accéder à des fins professionnels, mais qui ne prend pas en charge les protocoles et les algorithmes les plus sûrs, puis appliquer un profil de déchiffrement personnalisée pour permettre les protocoles et algorithmes moins stricts de ces sites (de cette manière, vous ne diminuez pas la sécurité en rétrogradant le profil de déchiffrement que vous utilisez pour accéder à la plupart des sites).

**STEP 3 |** Définissez la règle pour déchiffrer le trafic correspondant ou pour exclure le trafic correspondant du déchiffrement.

Sélectionnez **Options (Options)** et définissez l'**Action (Action)** de la règle de la politique :

Pour déchiffrer le trafic correspondant :

1. Définissez l'**Action (Action)** sur **Decrypt (Déchiffrer)**.
2. Définissez le **Type (Type)** de déchiffrement que le pare-feu doit effectuer sur le trafic correspondant :
   - Proxy de transfert SSL
   - Inspection SSL entrante. Si vous souhaitez activer l'inspection SSL, vous devez également sélectionnez le **Certificate (Certificat)** pour le serveur interne qui est la destination du trafic SSL entrant.
   - Proxy SSH

Pour exclure le trafic correspondant du décryptage :

Définissez l'**Action (Action)** sur **No Decrypt (Aucun déchiffrement)**.

**STEP 4 |** (Facultatif) Sélectionnez un **Decryption Profile (Profil de déchiffrement)** pour effectuer des vérifications supplémentaires sur le trafic qui correspond à la règle de politique.

***Bien qu'il soit facultatif d'appliquer un profil de déchiffrement au trafic déchiffré, il est recommandé de toujours appliquer un profil de déchiffrement aux règles de politique afin de protéger votre réseau contre les menaces chiffrées. Vous ne pouvez vous protéger des menaces que vous ne voyez pas.***

Par exemple, associez un profil de déchiffrement à une règle de politique pour garantir que les certificats de serveur sont valides et pour bloquer les sessions qui utilisent des protocoles non pris en charge et des suites de déchiffrement. Pour créer un profil de déchiffrement, sélectionnez **Objects (Objets)** > **Decryption Profile (Profil de déchiffrement)**.

1. Créez une règle de politique de décryptage ou ouvrez une règle existante pour la modifier.
2. Sélectionnez **Options (Options)**, puis sélectionnez un **Decryption Profile (Profil de déchiffrement)** pour bloquer et contrôler divers aspects du trafic correspondant à la règle.

   Les paramètres de la règle de profil que le pare-feu applique au trafic correspondant dépend de la règle **Action (Action)** de la politique (Déchiffrement ou Aucun déchiffrement) et du **Type (Type)** de règle de politique (Proxy de transfert SSL, Inspection entrante SSL ou proxy SSH). Ainsi, vous pouvez utiliser des profils de déchiffrement différents avec différents types de règles de stratégie de décryptage qui s'appliquent à différents types de trafic et d'utilisateurs.
3. Cliquez sur **OK**.

**STEP 5 |** Configuration de la journalisation de décryptage (configurer l'enregistrement des communications TLS réussies et avortées et configurez le transfert du journal de décryptage).

**STEP 6 |** Cliquez sur **OK (OK)** pour enregistrer la politique.

**STEP 7 |** Choisissez la prochaine étape pour autoriser pleinement le pare-feu à déchiffrer le trafic...

- Configurer le proxy de transfert SSL
- Configurer l'inspection SSL entrante
- Configurer le proxy SSH
- Créez des exclusions de déchiffrement basées sur les politiques pour le trafic que vous ***choisissez*** de ne pas déchiffrer et ajoutez les sites qui interrompent le déchiffrement pour des raisons techniques, comme des certificats épinglés ou l'authentification mutuelle à la liste d'exclusion de déchiffrement SSL.

# Configuration du proxy de transfert SSL

Pour permettre au pare-feu d'effectuer le déchiffrement du proxy de transfert SSL, vous devez configurer les certificats nécessaires pour établir le pare-feu comme un tiers de confiance (proxy) pendant la session entre le client et le serveur. Le pare-feu peut utiliser des certificats signés par une autorité de certification d'entreprise ou des certificats auto-signés générés sur le pare-feu avant que les *certificats d'approbation de transfert* puisse authentifier la session SSL auprès du client.

- (Best Practice (Bonnes pratiques)) **Enterprise CA-signed Certificates (Certificats signés par une CA d'entreprise)** : Une CA d'entreprise peut générer un certificat de signature que le pare-feu peut utiliser pour signer les certificats pour les sites nécessitant un décryptage SSL. Lorsque le pare-feu approuve la CA ayant signé le certificat du serveur de destination, le pare-feu peut envoyer au client une copie du certificat du serveur de destination signé par la CA de l'entreprise. Il s'agit d'une pratique exemplaire, car, en général, tous les périphériques réseau approuvent déjà la CA d'entreprise (elle est généralement déjà installée dans le stockage approuvé de la CA du périphérique). Vous n'avez donc pas besoin de déployer le certificat sur les points de terminaison, ce qui facilite le processus de déploiement.
- **Certificats auto-signés** : Le pare-feu peut agir en tant CA et générer des certificats auto-signés que le pare-feu peut utiliser pour signer les certificats pour les sites qui nécessitent le déchiffrement SSL. Le pare-feu peut signer une copie du certificat de serveur à présenter au client et établir la session SSL. Cette méthode exige que vous installiez les certificats auto-signés sur tous vos périphériques réseau afin que ces périphériques reconnaissent les certificats auto-signés du pare-feu. Puisque les certificats doivent être déployés sur tous les périphériques, cette méthode convient mieux aux petits déploiements et aux tests de preuve de concept (POC) qu'aux grands déploiements.

De plus, établissez un *certificat de refus de transfert* que le pare-feu pourra présenter aux clients lorsque le certificat du serveur est signé par une CA qui n'est pas approuvée par le pare-feu. Cette approche garantit que les clients sont informés par un avertissement de certificat lors des tentatives d'accès aux sites avec des certificats non approuvés.

*Que vous génériez des certificats d'approbation de transfert depuis votre CA racine d'entreprise ou que vous utilisiez un certificat auto-signé généré sur le pare-feu, générez un certificat d'autorité de confiance d'approbation de transfert subalterne distinct pour chaque pare-feu. La souplesse d'utiliser des CA subordonnées distincts vous permet de* révoquer *un certificat lorsque vous mettez un périphérique (ou une paire de périphériques) hors service sans affecter le reste du déploiement et réduit l'impact dans toutes les situations où vous avez besoin de révoquer un certificat. Les CA d'approbation de transfert distincts sur chaque pare-feu aident également à résoudre les problèmes, parce que le message d'erreur de la CA que l'utilisateur voit comprend des informations sur le trafic qui traverse le pare-feu. Si vous utilisez la même CA d'approbation de transfert sur chaque pare-feu, vous perdez la granularité de l'information.*

Après avoir défini les certificats d'approbation de transfert et de non-approbation de transfert nécessaires au déchiffrement du proxy de transfert SSL, créez une règle de politique de déchiffrement pour définir le trafic que le pare-feu doit déchiffrer et créez un profil de déchiffrement pour appliquer les vérifications et les contrôles SSL au trafic. La politique de déchiffrement déchiffre le trafic par tunnel SSL qui correspond à la règle en trafic en texte clair. Le pare-feu bloque et

restreint le trafic selon le profil de déchiffrement associé à la politique de déchiffrement et de la politique de sécurité du pare-feu. Le trafic crypte de nouveau le trafic dès qu'il sort du pare-feu.

*Lorsque vous configurez le proxy de transfert SSL, le trafic proxy ne prend pas en charge les points de code DSCP ou QoS.*

**STEP 1 |** Vérifiez que les interfaces appropriées sont configurées en des interfaces soit de câble virtuel, soit de Couche 2, soit de Couche 3.

Affichez les interfaces configurées dans l'onglet **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)**. La colonne **Interface Type (Type d'interface)** s'affiche si une interface est configurée en une interface de **Virtual Cable (Câble virtuel)** ou de **Layer 2 (Couche 2)** ou de **Layer 3 (Couche 3)**. Vous pouvez sélectionner une interface pour modifier sa configuration, y compris son type d'interface.

**STEP 2 |** Configurez le certificat d'approbation de transfert que le pare-feu pourra présenter aux clients lorsqu'une CA de confiance aura signé le certificat du serveur. Il peut s'agir d'un certificat signé par la CA de l'entreprise ou d'un certificat auto-signé.

(Pratique exemplaire recommandée) Utilisez un certificat signé par la CA de l'entreprise en tant que certificat d'approbation de transfert : Créez un certificat d'approbation de transfert ayant un nom unique sur chaque pare-feu :

1. Générez une Certificate Signing Request (demande de signature de certificat ; CSR) que l'AC d'entreprise signera et validera :
   1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**, puis cliquez sur **Generate (Générer)**.
   2. Saisissez un **Certificate Name (Nom de certificat)**. Utilisez un nom unique pour chaque pare-feu.
   3. Dans la liste déroulante **Signed By (Signé par)**, sélectionnez **External Authority (CSR) (Autorité externe (demande de signature de certificat))**.
   4. (Facultatif) Si votre CA d'entreprise l'exige, ajoutez des **Certificate Attributes (Attributs du certificat)** pour identifier plus précisément les informations relatives au pare-feu, telles que le Pays ou le Département.
   5. Cliquez sur **Generate (Générer)** pour enregistrer la CSR. Le certificat en attente est désormais affiché sur l'onglet **Device Certificates (Certificats du périphérique)**.
2. Exportez la demande de signature de certificat :
   1. Sélectionnez le certificat en attente affiché sur l'onglet **Device Certificates (Certificats du périphérique)**.
   2. Cliquez sur **Export (Exporter)** pour télécharger et enregistrer le fichier du certificat.

      *Laissez la case **Export private key (Exporter la clé privée)** décochée afin de garantir que la clé privée demeure en toute sécurité sur le pare-feu.*
   3. Cliquez sur **OK**.
3. Fournissez le fichier du certificat à votre CA d'entreprise. Lorsque vous recevez le certificat CA d'entreprise signé de la part de votre CA d'entreprise, enregistrez le certificat CA d'entreprise signé pour l'importation sur le pare-feu.
4. Importez le certificat signé par la CA d'entreprise sur le pare-feu :
   1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**, puis cliquez sur **Import (Importer)**.
   2. Saisissez exactement le **Certificate Name (Nom du certificat)** en attente Le **Certificate Name (Nom du certificat)** que vous entrez doit correspondre exactement au nom du certificat en attente pour que le certificat en attente soit validé.
   3. Sélectionnez le **Certificate File (Fichier du certificat)** signé que vous avez reçu de la part de votre CA d'entreprise.
   4. Cliquez sur **OK**. Le certificat est affiché comme étant valide avec les cases Key (Clé) et CA (CA) cochées.
5. Sélectionnez le certificat validé, pour l'activer en tant que **Forward Trust Certificate (Certificat d'approbation de transfert)** à utiliser pour le décryptage du proxy de transfert SSL.

6. Cliquez sur **OK (OK)** pour enregistrer le certificat d'approbation du transfert signé par la CA de l'entreprise.

Utilisation d'un certificat auto-signé en tant que certificat d'approbation de transfert :

1. Créer un certificat racine CA auto-signé.
2. Cliquez sur le certificat CA racine auto-signé (**Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**) pour ouvrir les **Certificate information (Informations sur le certificat)**, puis cliquez sur la case **Trusted Root CA (CA racine approuvée)**.
3. Cliquez sur **OK**.
4. Générez de nouveaux certificats CA subordonnés pour chaque pare-feu :
    1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**.
    2. Cliquez sur **Generate (Générer)** au bas de la fenêtre.
    3. Saisissez un **Certificate Name (Nom de certificat)**.
    4. Saisissez un **Common Name (Nom commun)**, par exemple 192.168.2.1. Il s'agit de l'adresse IP ou du nom de domaine complet (FQDN) qui devrait apparaître sur le certificat. Dans ce cas, l'adresse IP de l'interface d'approbation est utilisée. Évitez d'utiliser des espaces dans ce champ.
    5. Dans le champ **Signed By (Signé par)**, sélectionnez le certificat CA racine auto-signé que vous avez créé.
    6. Cochez la case **Certificate Authority (Autorité de certification)** pour activer le pare-feu et générer le certificat. Vous créez ainsi une Certificate Authority (autorité de certification ; CA) sur le pare-feu, qui sera importée vers les navigateurs des clients, de manière à ce que les clients approuvent le pare-feu comme autorité de certification.
    7. **Generate (Générez)** le certificat.
5. Cliquez sur le nouveau certificat pour le modifier et cochez la case **Forward Trust Certificate (Certificat d'approbation de transfert)** pour configurer le certificat en tant que certificat d'approbation de transfert.
6. Cliquez sur **OK (OK)** pour enregistrer le certificat d'approbation du transfert auto-signé.
7. Répétez cette procédure pour générer un certificat CA subordonné unique sur chaque pare-feu.

**STEP 3 |** Distribuez le certificat d'approbation de transfert aux magasins de certificats des systèmes clients.

Si vous utilisez un certificat signé par une CA d'entreprise en tant que certificat d'approbation de transfert pour le déchiffrement du proxy de transfert et que la CA d'entreprise figure déjà dans la liste locale des autorités de certification racines de confiance des systèmes clients, vous pouvez

ignorer cette étape. (Les systèmes clients approuvent les certificats CA subordonnés que vous avez générés sur le pare-feu, parce que la CA de racine de confiance de l'entreprise les a signés.)

*Si vous n'installez pas le certificat d'approbation de transfert sur les systèmes clients, les utilisateurs voient des avertissements de certificat affichés pour chaque site SSL qu'ils visitent.*

Sur un pare-feu configuré en tant que portail GlobalProtect :

*Cette option est prise en charge sur les versions de système d'exploitation client Windows et Mac ; la version 3.0.0 de l'agent GlobalProtect (ou toute version ultérieure) doit être installée sur les systèmes clients.*

1. Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)**, puis sélectionnez une configuration de portail existante ou **Add (Ajoutez)**-en une nouvelle.
2. Sélectionnez **Agent (Agent)**, puis sélectionnez une configuration d'agent existante ou **Add (Ajoutez)**-en une nouvelle.
3. **Add (Ajoutez)** le certificat de l'autorité de certification racine de confiance auto-signé à la section Trusted Root CA (Ca racine approuvée). Une fois que GlobalProtect distribue le certificat CA racine de confiance du pare-feu aux systèmes clients, les systèmes clients approuvent les certificats CA subordonnés du pare-feu, car les clients approuvent le certificat CA racine du pare-feu.
4. **Install in Local Root Certificate Store (Installez-les dans la boutique des certificats racines locaux)** pour que le portail GlobalProtect puisse distribuer automatiquement les certificats et les installer dans la boutique des certificats des systèmes clients GlobalProtect.
5. Cliquez deux fois sur **OK**.

Sans GlobalProtect :

Exportez le certificat CA racine de confiance pour pouvoir l'importer dans les systèmes clients. Surlignez le certificat et cliquez sur **Export (Exporter)** au bas de la fenêtre. Choisissez le format PEM.

*Ne sélectionnez pas la case **Export private key (Exporter la clé privée)**! La clé privée doit rester sur le pare-feu et ne doit pas être exportée vers les systèmes clients.*

Importez le certificat CA racine approuvée du pare-feu dans la liste des autorités de certification racines de confiance du navigateur sur les systèmes clients pour que les clients l'approuvent. Lors de l'importation sur le navigateur du client, vérifiez que vous ajoutez le certificat à la boutique des certificats des CA racines de confiance. Sur les systèmes Windows, l'emplacement d'importation par défaut est la boutique des certificats personnels. Vous pouvez aussi simplifier ce processus en utilisant une option de déploiement centralisée comme un Group Policy Object (objet de politique de groupe ; GPO) d'Active Directory.

**STEP 4 |** Configurez le certificat de non-approbation de transfert (utilisez le même certificat de non-approbation de transfert pour tous les pare-feu).

1. Cliquez sur **Generate (Générer)** au bas de la page Certificats.
2. Saisissez un **Certificate Name (Nom de certificat)**, tel que ssl-fwd-untrust.
3. Définissez le **Common Name (Nom commun)**, par exemple 192.168.2.1. Laissez le champ **Signed By (Signé par)** vide.
4. Cochez la case **Certificate Authority (Autorité de certification)** pour activer le pare-feu et générer le certificat.
5. Cliquez sur **Generate (Générer)** pour générer le certificat.
6. Cliquez sur **OK (OK)** pour enregistrer les paramètres.
7. Cliquez sur le nouveau certificat my-ssl-fwd-untrust pour le modifier, puis activez l'option **Forward Untrust Certificate (Certificat de non-approbation de transfert)**.

   *N'exportez pas le certificat de non-approbation de transfert dans les listes d'approbation de certificats des périphériques de votre réseau! N'installez pas le certificat de non-approbation de transfert sur les systèmes clients. C'est essentiel, car lorsque vous installez le certificat de non-approbation dans la liste de confiance, les périphériques approuvent des sites Web qui ne le pare-feu n'approuve pas. De plus, les utilisateurs ne voient pas les avertissements de certificat pour les sites non approuvés, ils ne sauront donc pas que les sites ne sont pas approuvés et pourront y accéder, ce qui pourrait exposer votre réseau aux menaces.*
8. Cliquez sur **OK (OK)** pour enregistrer les paramètres.

**STEP 5 |** (Facultatif) Effectuez la configuration de la taille de clé des certificats du serveur proxy de transfert SSL présentés par le pare-feu aux clients. Par défaut, le pare-feu détermine la taille de clé à utiliser en fonction de la taille de clé du certificat du serveur de destination.

**STEP 6 |** Vous devez créer une règle de politique de déchiffrement pour définir le trafic que le pare-feu doit déchiffrer et créer un profil de déchiffrement pour appliquer les contrôles SSL au trafic.

*Bien que les profils de déchiffrement soient facultatifs, il est recommandé d'inclure un profil de déchiffrement avec chaque règle de politique de déchiffrement pour empêcher les protocoles et algorithmes vulnérables et faibles d'autoriser le trafic douteux sur votre réseau.*

1. Sélectionnez **Policies (Politiques)** > **Decryption (Déchiffrement)**, Add (Ajoutez) ou modifiez une règle existante et définissez le trafic qui doit être déchiffré.
2. Sélectionnez **Options (Options)** et :
   - Définissez l'**Action (Action)** sur **Decrypt (Déchiffrer)** pour déchiffrer le trafic correspondant.
   - Définissez le **Type (Type)** de règle sur **SSL Forward Proxy (Proxy de transfert SSL)**.
   - (Facultatif, mais pratique exemplaire) Configurez ou sélectionnez un **Decryption Profile (Profil de déchiffrement)** existant pour bloquer et contrôler divers aspects du trafic qui est déchiffré (par exemple, procédez à la création d'un profil de déchiffrement pour

effectuer des vérifications de certificats et mettre en œuvre des versions de protocole et des suites de déchiffrement).

3. Cliquez sur **OK (OK)** pour enregistrer les paramètres.

**STEP 7 |** Activez, sur le pare-feu, le transfert du trafic décrypté pour analyse par WildFire.

*Cette option nécessite une licence WildFire active ; il s'agit d'une* recommandation WildFire.

**STEP 8 |** **Commit (Validez)** la configuration.

**STEP 9 |** Choisissez votre étape suivante :

- Activation de l'exclusion de décryptage SSL par les utilisateurs.
- Configurez les exclusions du déchiffrement pour désactiver le déchiffrement de certains types de trafic.

# Configuration de l'inspection SSL entrante

Servez-vous de l'inspection SSL entrante pour déchiffrer et inspecter le trafic SSL entrant destiné au serveur réseau (vous pouvez effectuer l'inspection SSL entrante de n'importe quel serveur si vous chargez le certificat du serveur sur le pare-feu). Avec une politique de décryptage Inspection SSL entrante activée, le pare-feu déchiffre tout le trafic SSL identifié par la politique en un trafic de texte clair et l'inspecte. Le pare-feu bloque, restreint, ou autorise le trafic selon le profil de déchiffrement qui est associé à la politique et la politique de sécurité qui s'applique au trafic, y compris tous les profils antivirus, de protection contre les vulnérabilités, antispyware, de filtrage des URL, de blocage des fichiers. Il est recommandé d'activer, sur le pare-feu, le transfert du trafic SSL déchiffré pour analyse WildFire et la génération de signatures.

La configuration de l'inspection SSL entrante inclut l'installation du certificat du serveur ciblé sur le pare-feu, la création d'une politique de déchiffrement de l'inspection SSL entrante et l'application d'un profil de déchiffrement à la politique.

*Lorsque vous configurez l'inspection entrante SSL, le trafic proxy ne prend pas en charge les points de code DSCP ou QoS.*

*Inspection SSL entrante ne prend pas en charge la* redirection du portail d'authentification*. Pour utiliser la redirection et le décryptage du portail d'authentification, vous devez utiliser le* proxy de transfert SSL*.*

**STEP 1 |** Vérifiez que les interfaces appropriées sont configurées en des interfaces tap, de câble virtuel, de Couche 2 ou de Couche 3.

*Vous ne pouvez utiliser une interface en mode TAP pour l'inspection SSL entrante si les chiffrements négociés incluent des algorithmes d'échange de clés PFS (DHE et ECDHE).*

Affichez les interfaces configurées dans l'onglet **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)**. La colonne **Interface Type (Type d'interface)** s'affiche si une interface est configurée en une interface de **Virtual Cable (Câble virtuel)** ou de **Layer 2 (Couche 2)** ou de **Layer 3 (Couche 3)**. Vous pouvez sélectionner une interface pour modifier sa configuration, y compris le type d'interface.

**STEP 2 |** Vérifiez que le certificat du serveur ciblé est bien installé sur le pare-feu.

*Si vous avez activé l'inspection entrante SSL à l'aide d'algorithmes d'échange de clés PFS, vous devez* upload a certificate bundle (télécharger un ensemble de certificats) *(un seul fichier) dans le pare-feu avec vos certificats organisés comme suit :*

1. *Certificat d'entité finale (feuille)*
2. *Certificats intermédiaires (dans l'ordre d'émission)*
3. *(Optional (Facultatif)) Certificat racine*

*Le téléchargement du fichier garantit que les clients reçoivent la chaîne de certificats complète pendant les négociations SSL, évitant ainsi les problèmes d'authentification des certificats de serveur côté client.*

Sur l'interface Web, sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)** pour afficher les certificats installés sur le pare-feu.

Pour importer le certificat du serveur ciblé sur le pare-feu :

1. Dans l'onglet **Device Certificates (Certificats de périphérique)**, sélectionnez **Import (Importer)**.
2. Saisissez un **Certificate Name (Nom de certificat)** descriptif.
3. Naviguez jusqu'au **Certificate File (Fichier du certificat)** du serveur ciblé et sélectionnez-le.
4. Cliquez sur **OK**.

**STEP 3 |** Vous devez créer une règle de politique de déchiffrement pour définir le trafic que le pare-feu doit déchiffrer et créer un profil de déchiffrement pour appliquer les contrôles SSL au trafic.

*Bien que les profils de déchiffrement soient facultatifs, il est recommandé d'inclure un profil de déchiffrement avec chaque règle de politique de déchiffrement pour empêcher les protocoles et algorithmes vulnérables et faibles d'autoriser le trafic douteux sur votre réseau.*

1. Sélectionnez **Policies (Politiques)** > **Decryption (Déchiffrement)**, **Add (Ajoutez)** ou modifiez une règle existante et définissez le trafic qui doit être déchiffré.
2. Sélectionnez **Options (Options)** et :
   - Définissez l'**Action (Action)** sur **Decrypt (Déchiffrer)** pour déchiffrer le trafic correspondant.
   - Définissez le **Type (Type)** de règle sur **SSL Inbound Inspection (Inspection SSL entrante)**.
   - Sélectionnez le **Certificate (Certificat)** pour le serveur interne qui est la destination du trafic SSL entrant.
   - (Facultatif, mais recommandé) Configurez ou sélectionnez un **Decryption Profile (Profil de déchiffrement)** pour bloquer et contrôler divers aspects du trafic déchiffré (par exemple, créez un profil de déchiffrement pour mettre fin à des sessions comportant des algorithmes non pris en charge et des suites de chiffrement non prises en charge).

     *Lorsque vous configurez les Paramètre des profil de décryptage SSL pour le trafic d'inspection SSL entrante, créez des profils distincts pour les serveurs ayant des capacités de sécurité différentes. Par exemple, si un ensemble de serveurs ne prend en charge que RSA, les paramètres de protocole SSL doivent uniquement prendre en charge RSA. Toutefois, les paramètres de protocole SSL pour les serveurs prenant en charge PFS doivent prendre en charge PFS. Configurez les paramètres de protocole SSL pour obtenir le niveau de sécurité maximal pris en charge par le serveur, mais vérifiez les performances pour vous assurer que les ressources de pare-feu peuvent gérer la charge de traitement supérieure requise par les protocoles et algorithmes de sécurité élevés.*
3. Cliquez sur **OK (OK)** pour enregistrer les paramètres.

**STEP 4 |** Activez, sur le pare-feu, le transfert du trafic décrypté pour analyse par WildFire.

*Cette option nécessite une licence WildFire active ; il s'agit d'une recommandation WildFire.*

**STEP 5 |** **Commit (Validez)** la configuration.

**STEP 6 |** Choisissez votre étape suivante…

- Activation de l'exclusion de décryptage SSL par les utilisateurs.
- Configurez les exclusions du déchiffrement pour désactiver le déchiffrement de certains types de trafic.

# Configuration du proxy SSH

La configuration du proxy SSH ne nécessite pas de certificats et la clé utilisée pour décrypter les sessions SSH est automatiquement générée sur le pare-feu pendant le démarrage. Lorsque le déchiffrement SSH est activé, le pare-feu déchiffre le trafic SSH et bloque ou restreint le trafic SSH en fonction des paramètres de votre politique de déchiffrement et de votre profil de déchiffrement. Le trafic est de nouveau crypté dès qu'il quitte le pare-feu.

*Lorsque vous configurez le proxy SSH, le trafic proxy ne prend pas en charge les points de code DSCP ou la qualité de service.*

**STEP 1 |** Vérifiez que les interfaces appropriées sont configurées en des interfaces soit de câble virtuel, soit de Couche 2, soit de Couche 3. Le décryptage peut uniquement être effectué sur des interfaces de câble virtuel, de Couche 2, ou de Couche 3.

Affichez les interfaces configurées dans l'onglet **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)**. La colonne **Interface Type (Type d'interface)** s'affiche si une interface est configurée en une interface de **Virtual Cable (Câble virtuel)** ou de **Layer 2 (Couche 2)** ou de **Layer 3 (Couche 3)**. Vous pouvez sélectionner une interface pour modifier sa configuration, y compris son type d'interface.

**STEP 2 |** Vous devez créer une règle de politique de déchiffrement pour définir le trafic que le pare-feu doit déchiffrer et créer un profil de déchiffrement pour appliquer les vérifications au trafic SSH.

*Bien que les profils de déchiffrement soient facultatifs, il est recommandé d'inclure un profil de déchiffrement avec chaque règle de politique de déchiffrement pour empêcher les protocoles et algorithmes vulnérables et faibles d'autoriser le trafic douteux sur votre réseau.*

1. Sélectionnez **Policies (Politiques)** > **Decryption (Déchiffrement)**, Add (Ajoutez) ou modifiez une règle existante et définissez le trafic qui doit être déchiffré.
2. Sélectionnez **Options (Options)** et :
   - Définissez l'**Action (Action)** sur **Decrypt (Déchiffrer)** pour déchiffrer le trafic correspondant.
   - Définissez le **Type (Type)** de règle sur **SSH Proxy (proxy SSH)**.
   - (Facultatif, mais recommandé) Configurez ou sélectionnez un **Decryption Profile (Profil de déchiffrement)** pour bloquer et contrôler divers aspects du trafic déchiffré (par exemple, créez un profil de déchiffrement pour mettre fin à des sessions comportant des versions non prises en charge et des algorithmes non pris en charge).
3. Cliquez sur **OK (OK)** pour enregistrer les paramètres.

**STEP 3 |** **Commit (Validez)** la configuration.

**STEP 4 |** (Facultatif) Passez aux exclusions du déchiffrement pour désactiver le déchiffrement de certains types de trafic.

# Configuration de la vérification des certificats du serveur pour le trafic déchiffré

Vous créez des politiques de non déchiffrement pour le trafic que vous ***choisissez*** de ne pas déchiffrer parce que le trafic est personnel, sensible ou assujetti aux lois et aux règlements locaux. Par exemple, vous pourriez décider de ne pas déchiffrer le trafic de certains dirigeants ou le trafic entre les utilisateurs de services financiers et les serveurs de services financiers qui contiennent des informations personnelles. (N'excluez pas le trafic que vous ne pouvez pas déchiffrer parce qu'un site force le déchiffrement pour des raisons techniques, comme un certificat épinglé ou une authentification mutuelle, selon la politique. Ajoutez plutôt le nom d'hôte à la liste d'exclusion du de déchiffrement.)

Cependant, ce n'est pas parce que vous ne déchiffrez pas le trafic que vous devriez laisser passer tout le trafic non chiffré sur votre réseau. Il est recommandé d'appliquer un profil d'absence de déchiffrement au trafic non déchiffré pour bloquer les sessions avec des certificats expirés et des émetteurs non approuvés.

**STEP 1 |** Créez une règle de stratégie de déchiffrement pour identifier le trafic non déchiffré et créez un profil de déchiffrement pour bloquer les mauvaises sessions.

1. Sélectionnez **Policies (Politiques)** > **Decryption (Déchiffrement)**, puis ajoutez une règle ou modifiez-en une existante pour identifier le trafic non chiffré.
2. Sélectionnez **Options (Options)** et :
   - Définissez l'**Action** de la règle sur **No Decrypt (Aucun déchiffrement)**, pour que le pare-feu ne déchiffre pas le trafic qui correspond à la règle.
   - Ignorez le **Type** de règle, parce que le trafic n'est pas déchiffré.
   - (Facultatif, mais recommandé) Configurez ou sélectionnez un profil de déchiffrement pour le trafic non déchiffré afin de bloquer les sessions avec des certificats sont expirés et des émetteurs de certificats non approuvés.

   ***Ne joignez pas de profil Pas de décryptage aux politiques de décryptage pour le trafic TLSv1.3 que vous ne décryptez pas parce que le pare-feu ne peut pas lire les informations cryptées du certificat, il ne peut donc pas effectuer de vérification du certificat. Cependant, vous devez toujours créer une politique de décryptage pour le trafic TLSv1.3 que vous ne décryptez pas car le trafic non décrypté n'est pas enregistré à moins qu'une politique de décryptage ne contrôle ce trafic.***

**STEP 2 |** **Commit (Validez)** la configuration.

**STEP 3 |** Choisissez votre étape suivante :

- Activation de l'exclusion de décryptage SSL par les utilisateurs.
- Configurez les exclusions du déchiffrement pour désactiver le déchiffrement de certains types de trafic.

# Exclusions de déchiffrement

Vous pouvez exclure deux types de trafic du déchiffrement :

- Le trafic qui interrompt le décryptage pour des ***raisons techniques***, comme un certificat épinglé, une chaîne de certificat incomplète, des chiffrements non pris en charge ou une authentification mutuelle (la tentative de décryptage du trafic entraîne le blocage du trafic). Palo Alto Networks fournit une liste d'exclusion de décryptage SSL prédéfinie (**Device (Périphérique)** > **Certificate management (Gestion des certificats)** > **SSL Decryption Exclusion (Exclusion du décryptage SSL)**) qui exclut les hôtes ayant des applications et des services qui sont connus pour interrompre par défaut le décryptage SSL techniquement. Si vous rencontrez des sites qui interrompent le déchiffrement techniquement et qui ne figurent pas sur la liste d'exclusion du déchiffrement SSL, vous pouvez les ajouter à la liste manuellement selon le nom d'hôte du serveur. Le pare-feu bloque les sites dont les applications et les services interrompent le déchiffrement techniquement, sauf si vous les ajoutez à la liste d'exclusion du déchiffrement SSL.

  Si le profil de décryptage autorise les **Unsupported Modes (Modes non pris en charge)** (sessions avec authentification du client, versions non prises en charge ou suites de chiffrement non prises en charge), le pare-feu ajoute automatiquement les serveurs et les applications qui utilisent les modes non pris en charge autorisés à son Local SSL Decryption Exclusion Cache (Cache d'exclusion de décryptage SSL local) (**Device (Périphérique)** > **Certificate Management (Gestion de certificat)** > **SSL Decryption Exclusion (Exclusion de décryptage SSL)** > **Show Local Exclusion Cache (Afficher le cache d'exclusion local)**). Lorsque vous bloquez les modes non pris en charge, vous augmentez la sécurité mais vous bloquez également la communication avec les applications qui utilisent ces modes.
- Le trafic que vous ***choisissez*** de ne pas décrypter en raison de questions commerciales, réglementaires, personnelles ou autres, comme le trafic relatif aux services financiers, à la santé et à la médecine ou au gouvernement. Vous pouvez choisir d'exclure le trafic en fonction de la source, de la destination, de la catégorie d'URL et du service.

Vous pouvez utiliser des astérisques (*) en tant que caractères génériques pour créer des exclusions de déchiffrement pour plusieurs noms d'hôte associés avec un domaine. Les astérisques se comportent de la même façon que les carets (^) se comportent avec les exceptions de catégories URL : chaque astérisque indique un sous-domaine variable (étiquette) dans le nom d'hôte. Ceci vous permet de créer des exclusions aussi bien très spécifiques que très générales. Par exemple :

- mail.*.com correspond à mail.company.com, mais ne correspond pas à mail.company.sso.com.
- *.company.com correspond à tools.company.com, mais ne correspond pas à eng.tools.company.com.
- *.*.company.com correspond à eng.tools.company.com, mais ne correspond pas à eng.company.com.
- *.*.*.company.com correspond à corp.exec.mail.company.com, mais ne correspond pas à corp.mail.company.com.
- mail.google.* correspond à mail.google.com, mais ne correspond pas à mail.google.uk.com.
- mail.google.*.* correspond à mail.google.co.uk, mais ne correspond pas à mail.google.com.

Par exemple, pour utiliser des caractères génériques pour exclure video-stats.video.google.com du décryptage, mais sans exclure video.google.com du décryptage, excluez *.*.google.com

*Peu importe le nombre d'astérisques qui précèdent le nom d'hôte (sans une étiquette de caractère non générique qui précède le nom d'hôte), le nom d'hôte correspond à l'entrée. Par exemple, *.google.com, *.*.google.com et *.*.*.google.com correspondent tous à google.com. Cependant, *.dev.*.google.com ne correspond pas à google.com, car une étiquette (dev) n'est pas un caractère générique.*

Pour accroître la visibilité du trafic et réduire la surface d'attaque autant que possible, ne faites aucune exception de déchiffrement sauf si vous êtes obligé de le faire.

- Exclusions de décryptage prédéfinies de Palo Alto Networks
- Exclure un serveur du déchiffrement pour des raisons techniques
- Cache d'exclusion du décryptage local
- Création d'une exclusion de déchiffrement basée sur une politique

## Exclusions de décryptage prédéfinies de Palo Alto Networks

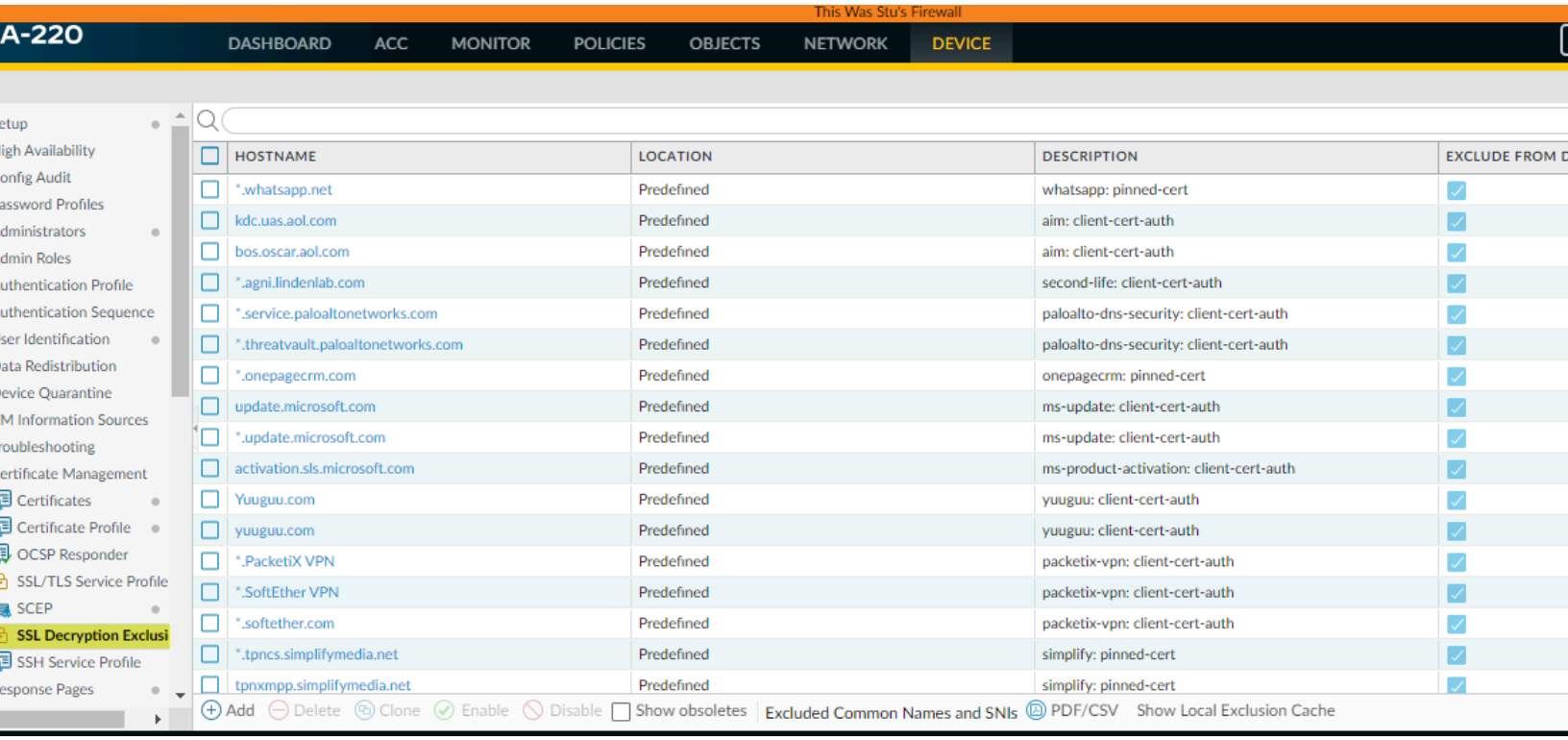
Le pare-feu fournit une liste d'exclusion du déchiffrement SSL prédéfinie pour exclure du déchiffrement les sites utilisés couramment qui interrompent le déchiffrement pour des raisons techniques, comme des certificats épinglés et l'authentification mutuelle. Les exclusions de déchiffrement prédéfinies sont activées par défaut et Palo Alto Networks fournit au pare-feu des exclusions de déchiffrement prédéfinies nouvelles et mises à jour dans le cadre des mises à jour du contenu des menaces et des applications (ou dans le cadre de la mise à jour du contenu des applications, si vous ne disposez pas d'une licence de prévention contre les menaces). Le pare-feu ne déchiffre pas le trafic qui correspond aux exclusions prédéfinies et autorise le trafic chiffré selon la politique de sécurité qui régit ce trafic. Cependant, le pare-feu ne peut inspecter le trafic chiffré ou lui appliquer la politique de sécurité.

*La liste d'exclusion du déchiffrement SSL **ne doit pas** contenir les sites que vous choisissez de ne pas déchiffrer pour juridiques, réglementaires, d'affaires, de la protection des renseignements personnels ou autres. Elle ne doit contenir que les sites qui interrompent le déchiffrement techniquement (le déchiffrement de ces sites en bloque le trafic). Pour le trafic, comme les adresses IP, les utilisateurs, les catégories d'URL, les services et même des zones entières, que vous choisissez de ne pas déchiffrer,* créez une exclusion de déchiffrement basée sur une politique**.**

Comme le trafic des sites qui figurent sur la liste d'exclusion du déchiffrement SSL demeuré chiffré, le pare-feu n'inspecte pas le trafic ou ne fournit aucune application de la sécurité supplémentaire. Vous pouvez désactiver une exclusion prédéfinie. Par exemple, vous pouvez choisir de désactiver les exclusions prédéfinies pour appliquer une politique de sécurité stricte qui autorise uniquement des applications et des services que le pare-feu peut inspecter et sur lesquels le pare-feu peut appliquer la politique de sécurité. Cependant, le pare-feu bloque les sites dont les applications et les services interrompent le déchiffrement techniquement, s'ils ne sont pas activés sur la liste d'exclusion du déchiffrement SSL.

Vous pouvez afficher et gérer toutes les exclusions prédéfinies de décryptage SSL de Palo Alto Networks directement sur le pare-feu (**Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **SSL Decryption Exclusions (Exclusions de décryptage SSL)**).




Le **Hostname (Nom d'hôte)** affiche le nom de l'hôte qui héberge l'application ou le service qui interrompt le déchiffrement techniquement. Vous pouvez également **Add (Ajouter)** les hôtes pour exclure un serveur du déchiffrement pour des raisons techniques s'il ne figure pas sur la liste prédéfinie.

La **Description** affiche la raison pour laquelle le pare-feu ne peut déchiffrer le trafic du site, par exemple, **pinned-cert** (un certificat épinglé) ou **client-cert-auth** (autorisation client).

Le pare-feu supprime automatiquement de la liste les exclusions de déchiffrement SSL prédéfinies qui sont activées lorsqu'elles deviennent désuètes (le pare-feu supprime une application dont le déchiffrement causait anciennement le dysfonctionnement lorsqu'elle devient prise en charge par le déchiffrement). **Show Obsoletes (Afficher les exclusions désuètes)** vérifie si des exclusions prédéfinies désactivées demeurent sur la liste et qu'elles ne sont plus nécessaires. Le pare-feu ne supprime automatiquement aucune exclusion de déchiffrement prédéfinie qui est désactivée de la liste, mais vous pouvez sélectionner des entrées désuètes et les **Delete (Supprimer)**.

Vous pouvez cochez la case d'un nom d'hôte, puis cliquer sur **Disable (Désactiver)** pour supprimer les sites prédéfinies de la liste. Utilisez la liste d'exclusion du décryptage SSL uniquement pour les sites qui interrompent le déchiffrement pour des raisons techniques, ne l'utilisez pas pour les sites que vous choisissez de ne pas déchiffrer.

## Exclure un serveur du déchiffrement pour des raisons techniques

Si le déchiffrement interrompt une application ou un service important techniquement (le déchiffrement du trafic le bloque), vous pouvez ajouter le nom d'hôte du site qui héberge l'application ou le service à la liste d'exclusion du déchiffrement SSL prédéfinie de Palo Alto Networks pour une exception de déchiffrement personnalisée. Le pare-feu ne déchiffre pas et n'inspecte pas les règles de sécurité et ne les applique pas au trafic que la liste d'exclusion du déchiffrement SSL autorise. Vous devez donc vous assurer que les sites que vous ajoutez à la liste sont vraiment des

sites offrant des applications ou services dont vous avez besoin pour des raisons professionnelles. Par exemple, certaines applications internes critiques de l'entreprise qui sont personnalisées pourraient interrompre le déchiffrement, et vous pouvez les ajouter à la liste pour que le pare-feu autorise le trafic de l'application personnalisé chiffré.

*La liste d'exclusion du déchiffrement SSL **ne doit pas** contenir les sites que vous choisissez de ne pas déchiffrer pour juridiques, réglementaires, d'affaires, de la protection des renseignements personnels ou autres. Elle ne doit contenir que les sites qui interrompent le déchiffrement techniquement. Pour le trafic (adresses IP, utilisateurs, catégories d'URL, services et même des zones entières) que vous choisissez de ne pas déchiffrer,* créez une exclusion de déchiffrement basée sur une politique*.*

Les raisons pour lesquelles les sites interrompent le décryptage techniquement comprennent les certificats épinglés, l'authentification des clients, les chaînes de certificats incomplètes et les chiffrements non pris en charge. Pour le HTTP public key pinning (épinglage des clés publiques HTTP ; HPKP), la plupart des navigateurs qui utilisent HPKP autorisent le déchiffrement du proxy de transfert si vous installez le certificat CA d'entreprise (ou la chaîne de certificat) sur le client.

*Si la raison technique qui justifie l'exclusion d'un site du déchiffrement est une chaîne de certificats incomplète, le pare-feu de nouvelle génération ne réparera pas automatiquement la chaîne comme un navigateur le ferait. Si vous devez ajouter un site à la liste d'Exclusions de Décryptage, passez le site en revue manuellement pour vous assurer que c'est un site commercial légitime, puis téléchargez les autorités de certification subordonnées manquantes et procédez à leur* chargement et déploiement *sur le pare-feu.*

Après avoir ajouté un serveur à la liste d'exclusion de déchiffrement SSL, le pare-feu compare le nom d'hôte du serveur que vous utilisez pour définir l'exclusion de déchiffrement à la fois à l'indication de nom de serveur (SNI) dans le message de bienvenue du client et au nom commun (CN) dans le serveur certificat. Si le SNI ou le CN correspondent à l'entrée dans la liste d'exclusion du déchiffrement SSL, le pare-feu exclut le trafic du déchiffrement.

**STEP 1 |** Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **SSL Decryption Exclusions (Exclusion du déchiffrement SSL)**.

**STEP 2 |** **Add (Ajoutez)** une exclusion du déchiffrement ou sélectionnez une entrée personnalisée existante pour la modifier.

**STEP 3 |** Entrez le **hostname (nom d'hôte)** du site Web ou de l'application que vous souhaitez exclure du déchiffrement.

*Le nom d'hôte est sensible à la casse.*

Vous pouvez utiliser les caractères spéciaux pour exclure plusieurs noms d'hôte associés à un domaine. Le pare-feu exclut toutes les sessions où le serveur présente un CN qui correspond au domaine du déchiffrement.

Assurez-vous que le champ du nom d'hôte est unique pour chaque entrée personnalisée. Si une exclusion prédéfinie est mise en correspondance avec une entrée personnalisée, l'entrée personnalisée a la priorité.

**STEP 4 |** (Facultatif) Sélectionnez **Shared (Partagé)** pour partager l'exclusion sur tous les systèmes virtuels dans un pare-feu à plusieurs systèmes virtuels.

**STEP 5 |** **Exclude (Excluez)** l'application du déchiffrement. Si vous modifiez une exclusion du déchiffrement existante, vous pouvez éventuellement décocher cette case pour commencer à déchiffrer une entrée qui a été précédemment exclue du déchiffrement.

**STEP 6 |** Cliquez sur **OK (OK)** pour enregistrer la nouvelle exclusion.

## Cache d'exclusion du décryptage local

Le pare-feu peut ajouter des serveurs au cache d'exclusion de décryptage local (**Device (Périphérique)** > **Certificate Management (Gestion de certificat)** > **SSL Decryption Exclusion (Exclusion de décryptage SSL)** > **Show Local Exclusion Cache (Afficher le cache d'exclusion local)**) et exclure automatiquement leur trafic du décryptage pendant 12 heures si ce trafic interrompt le décryptage pour des raisons techniques telles qu'un certificat épinglé ou un certificat non pris en charge. Lorsque le profil de décryptage autorise des modes non pris en charge - sessions avec authentification du client, versions non prises en charge ou suites de chiffrement non prises en charge - et que le trafic autorisé utilise un mode non pris en charge, alors le dispositif ajoute automatiquement le serveur au cache d'exclusion local et contourne le décryptage. Le pare-feu ne décrypte pas, n'inspecte pas et n'applique pas la politique de sécurité sur le trafic que le cache d'exclusion de décryptage local autorise parce que le trafic reste crypté. Assurez-vous que les sites que vous excluez du décryptage (en appliquant un profil de décryptage qui permet des modes non pris en charge) sont des sites avec des applications ou des services dont vous avez besoin professionnellement.

Le blocage des modes non pris en charge bloque la communication avec les applications qui utilisent ces modes pour accroître la sécurité. L'authentification du client est une raison courante pour exclure les applications du décryptage. C'est pourquoi la meilleure pratique consiste à bloquer les versions et les chiffres non pris en charge et à permettre l'authentification du client dans le profil de décryptage. Si le profil de décryptage permet l'authentification du client, alors lorsqu'un client démarre une session avec un serveur qui lui demande de s'authentifier, au lieu de bloquer le trafic parce que le pare-feu ne peut pas le décrypter, le pare-feu ajoute l'application et le serveur au cache d'exclusion local et autorise le trafic.

***Si vous autorisez le trafic provenant de sites qui utilisent l'authentification du client et qui ne figurent pas dans les sites prédéfinis de la** liste d'exclusion de décryptage SSL**, créez un profil de décryptage qui autorise les sessions avec authentification du client. Ajoutez le profil à une règle de politique de décryptage qui s'applique uniquement aux serveurs qui hébergent l'application. Pour renforcer encore plus la sécurité, vous pouvez exiger une Authentification Multifactorielle pour compléter le processus de connexion de l'utilisateur. Vous pouvez également ajouter le site à la liste d'exclusion de décryptage SSL pour sauter le décryptage sans utiliser une politique de décryptage explicite.*

Le pare-feu ajoute des entrées de cache d'exclusion de décryptage SSL local basées sur la politique de décryptage et le profil qui contrôle le trafic de l'application. Si vous ne bloquez pas les **Unsupported Mode Checks (Contrôles de mode non pris en charge)** dans le profil de décryptage, le pare-feu ajoute des entrées dans le cache local d'exclusion de décryptage SSL lorsque :

- Le client ne prend en charge que TLSv1.2 et le serveur ne prend en charge que TLSv1.3. Dans le cache local, la raison indiquée pour cette exclusion est SSL_UNSUPPORTED.

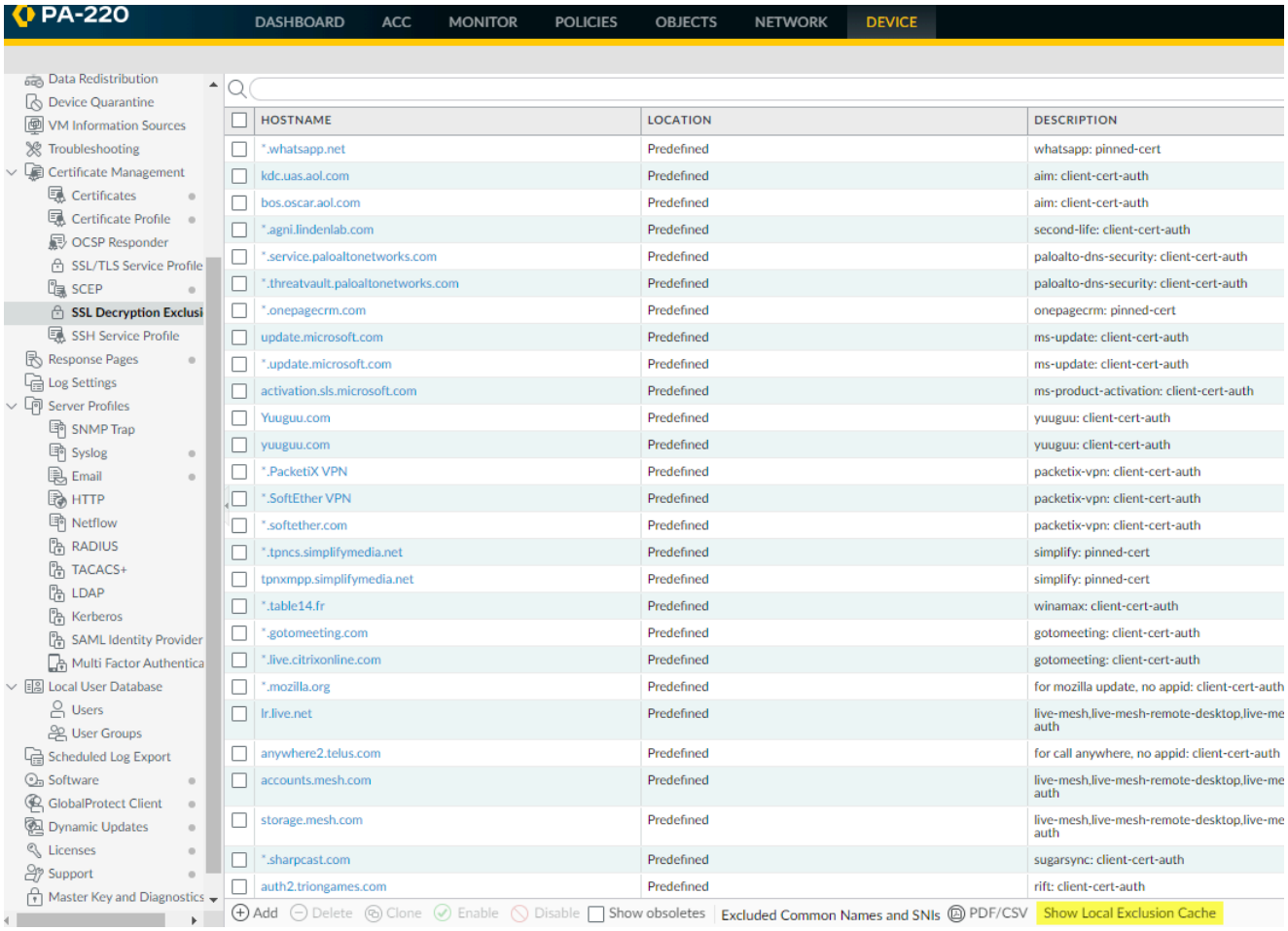
- Le client prend en charge TLSv1.3 et TLSv1.2, et le serveur ne prend en charge que TLSv1.2. Dans ce cas, la colonne **Reason (Raison)** indique TLS13_UNSUPPORTED.

  *Lorsque la **Reason (Raison)** de l'ajout d'un serveur au cache local d'exclusion de décryptage SSL est TLS13_UNSUPPORTED, le pare-feu déclasse le protocole en TLSv1.2 et le pare-feu décrypte et inspecte le trafic.*

- Le client annonce un chiffrement spécifique que le serveur ne prend pas en charge.
- Le client annonce une courbe spécifique que le serveur ne prend pas en charge.

Le cache local contient un maximum de 1 024 entrées. Vous ne pouvez pas ajouter manuellement des exclusions locales au cache d'exclusion de décryptage SSL local (mais vous pouvez ajouter manuellement des exclusions de décryptage à la liste d'exclusion de décryptage SSL).

Vous devez disposer d'un accès administratif de super utilisateur ou de gestion des certificats pour visualiser le cache d'exclusion de décryptage SSL local. Pour le consulter, accédez à **Device (Périphérique)** > **Certificate Management (Gestion de certificat)** > **SSL Decryption Exclusion (Exclusion de décryptage SSL)** puis cliquez sur **Show Local Exclusion Cache (Afficher le cache d'exclusion local)** proche du bas de l'écran. Le cache d'exclusion local affiche l'application, le serveur, la raison de l'inclusion dans le cache, le profil de décryptage qui contrôle le trafic, et plus encore pour chaque entrée. Vous pouvez sélectionner et supprimer manuellement des entrées dans le cache local.




Vous pouvez également supprimer les entrées en cache en utilisant la CLI :

```
clear ssl-decrypt exclude-cache [server <value>] [application
 <value>]
```

Si quelqu'un tente d'accéder au même serveur avant que l'entrée de la mémoire cache locale ne soit épuisée (12 heures), le pare-feu fait correspondre la session à l'entrée de la mémoire cache, contourne le décryptage et autorise le trafic. Le pare-feu vide le cache d'exclusion local si vous modifiez la politique ou le profil de décryptage, car ces modifications peuvent affecter la classification de la session. Si le cache devient plein, le pare-feu purge les entrées les plus anciennes au fur et à mesure que de nouvelles entrées arrivent.

## Création d'une exclusion de déchiffrement basée sur une politique

Les exclusions de déchiffrement basées sur les politiques visent l'exclusion du trafic que vous ***choisissez*** de ne pas déchiffrer. Vous pouvez créez une exclusion de déchiffrement basée sur une politique en fonction de toute combinaison de la source, de la destination, du service ou de la catégorie d'URL du trafic. Voici des exemples de trafic que vous pourriez choisir de ne pas déchiffrer :

- Le trafic que vous ne devriez jamais déchiffrer parce qu'il contient des personally identifiable information (informations d'identification personnelle ; PII) ou d'autres informations de nature délicate, comme les catégories de filtrage des URL services financiers, santé et médecine, et gouvernement.
- Le trafic qui provient de cadres supérieurs ou d'autres utilisateurs dont le trafic ne devrait pas être déchiffré, ou est destiné à de tels utilisateurs.
- Il se peut que certains périphériques comme les serveurs des finances doivent être exclus du déchiffrement.
- Selon l'activité, certaines entreprises peuvent accorder une plus grande valeur à la vie privée et à l'expérience utilisateur qu'à la sécurité de certaines applications.
- Les lois ou règlements locaux qui interdisent le déchiffrement d'un certain trafic.

  Le Règlement général sur la protection des données (RGPD) de l'Union européenne (UE) est un exemple de l'absence de déchiffrement du trafic à des fins de conformité réglementaire et juridique. Le RGPD de l'UE exigera une protection solide de toutes les données personnelles de toutes les personnes. Le RGPD affecte toutes les entreprises, y compris les entreprises situées à l'étranger, qui recueillent ou traitent les données personnelles de ressortissants de l'UE.

  Des règlementations et règles de conformité différentes peuvent signifier que les mêmes données seront traitées différemment selon les pays ou les régions du monde. Habituellement, les entreprises peuvent décrypter les informations personnelles présentes dans leur centre de données d'entreprise car elles sont propriétaires de ces informations. La meilleure pratique consiste à décrypter le plus de trafic possible, afin d'avoir le plus de visibilité et de pouvoir lui appliquer une protection de sécurité.

Vous pouvez utiliser les catégories d'URL prédéfinies pour exclure des catégories entières de sites Web du déchiffrement. Vous pouvez créer des catégories d'URL personnalisée pour définir une liste personnalisée d'URL que vous ne voulez pas déchiffrer ou vous pouvez créer une liste dynamique externe (EDL) pour définir une liste personnalisée d'URL que vous ne voulez pas déchiffrer.

Dans des environnements comme Office 365 qui ont des adresses IP qui changent de façon dynamique ou dans des environnements où vous apportez fréquemment des changements à la liste des URL que vous souhaitez exclure du déchiffrement, il est souvent préférable d'utiliser une

EDL au lieu d'une catégorie d'URL pour spécifier les URL exclus. L'utilisation d'une EDL est moins perturbatrice dans les environnements dynamiques, car la modification d'une EDL change les catégories d'URL de manière dynamique, sans **Commit (Validation)**, tandis que la modification d'une catégories d'URL personnalisées doit faire l'objet d'une **Commit (Validation)** pour prendre effet.

*Créez une EDL ou une catégories d'URL personnalisée qui contient toutes les catégories que vous décidez de ne pas déchiffrer. Ainsi, une seule règle de politique de déchiffrement régit le trafic chiffré que vous décidez d'autoriser. Appliquez un profil d'absence de déchiffrement à la règle. La capacité d'ajouter des catégories à une EDL ou à une catégorie d'URL personnalisée facilite l'exclusion du trafic du déchiffrement et permet de disposer d'une base de règles propre.*

*Tout comme c'est le cas pour les règles de politique de sécurité, le pare-feu compare le trafic entrant aux règles de politique de déchiffrement de la séquence de la base de règles de la politique. Placez les règles d'exclusion du déchiffrement au haut de la base de règles pour éviter de déchiffrer par mégarde du trafic de nature délicate ou du trafic que les lois ou les règlements vous empêchent de déchiffrer.*

Si vous créez des exclusions de déchiffrement basées sur la politique, il est recommandé de placer les règles d'exclusion suivantes au haut de la base de règles du déchiffrement, dans l'ordre suivant :

1. les exceptions basées sur l'adresse IP pour des serveurs de destination sensibles ;
2. les exceptions basées sur l'utilisateur source pour les cadres supérieurs et les autres utilisateurs ou groupes ;
3. les exceptions basées sur des EDL ou URL personnalisées pour les URL de destination ;
4. les exceptions basées sur les catégories d'URL prédéfinies qui son sensibles pour les URL de destination de catégories complètes, comme les services financiers, la santé et la médecine, le gouvernement.

Placez les règles qui déchiffrent le trafic après ces règles dans la base de règles de déchiffrement.

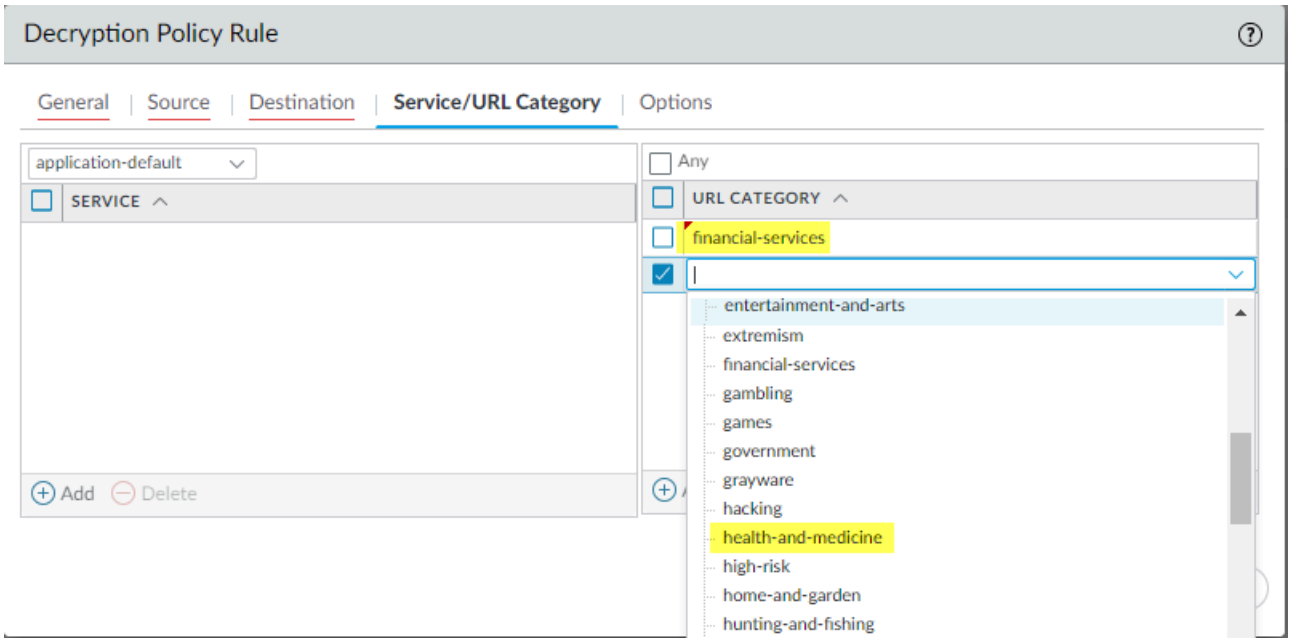
**STEP 1 |** Excluez le trafic du déchiffrement en fonction des critères de correspondance.

Cet exemple explique comment exclure le trafic classé dans la catégorie des sites relatifs à la finance ou à la santé du décryptage du proxy de transfert SSL.

1. Sélectionnez **Policies (Politiques)** > **Decryption (Déchiffrement)**, puis **Add (Ajoutez)** ou modifiez une règle de politique de déchiffrement.
2. Définissez le trafic que vous souhaitez exclure du déchiffrement.

   Dans cet exemple :

   1. Donnez à la règle un **Name (Nom)** descriptif, tel que No-Decrypt-Finance-Health.
   2. Définissez la **Source (Source)** et la **Destination (Destination)** sur **Any (Indifférent)** pour appliquer la règle No-Decrypt-Finance-Health à tout le trafic SSL destiné à un serveur externe.
   3. Sélectionnez la **URL Category (Catégorie d'URL)** et **Add (Ajoutez)** les catégories d'URL de sites relatifs à des services de finance ou à la santé et aux médicaments.




3. Sélectionnez **Options (Options)** et définissez la règle sur **No Decrypt (Aucun déchiffrement)**.
4. (Facultatif, mais recommandé) Créez et joignez un profil de non décryptage à la règle pour valider des certificats pour les sessions que le pare-feu ne décrypte pas. Configurez le profil pour **Block sessions with expired certificates (Bloquer les sessions avec un**

**certificat expiré)** et **Block sessions with untrusted issuers (Bloquer les sessions avec des émetteurs non approuvés)**.

*Exception : Ne joignez pas de profil Pas de décryptage aux politiques de décryptage pour le trafic TLSv1.3 que vous ne décryptez pas parce que le pare-feu ne peut pas lire les informations cryptées du certificat, il ne peut donc pas effectuer de vérification du certificat. Cependant, vous devez toujours créer une politique de décryptage pour le trafic TLSv1.3 que vous ne décryptez pas car le trafic non décrypté n'est pas enregistré à moins qu'une politique de décryptage ne contrôle ce trafic.*

5. Cliquez sur **OK** pour enregistrer la règle de décryptage No-Decrypt-Finance-Health.

**STEP 2 |** Placez la règle d'exclusion du déchiffrement en tête de la règle de bases de la politique de déchiffrement.

Le pare-feu applique les règles de déchiffrement au trafic entrant dans la séquence de la base de règles et applique la première règle qui correspond au trafic.

Sélectionnez la politique **No-Decrypt-Finance-Health (Aucun déchiffrement des sites liés à la finance et à la santé)** (**Decryption (Décryptage)** > **Policies (Politiques)**), puis cliquez sur **Move Up (Remonter)** jusqu'à ce qu'elle figure en tête de liste ou faites glisser-déposer la règle.

**STEP 3 |** Enregistrer la configuration.

Cliquez sur **Commit (Valider)**.

# Blocage d'exportation de clé privée

Vous pouvez bloquer en permanence l'exportation de clés privées pour les certificats lorsque vous les générez ou les importez dans PAN-OS ou Panorama. Le blocage de l'exportation de clés privées depuis vos périphériques PAN-OS durcit votre posture de sécurité car il empêche les administrateurs malhonnêtes ou autres mauvais acteurs d'utiliser les clés à mauvais escient. Les administrateurs dont le rôle inclut la gestion des certificats peuvent bloquer l'exportation de clés privées. Vous ne pouvez pas bloquer les clés qui existent déjà sur un périphérique ; vous ne pouvez bloquer les clés qu'au moment où vous les générez ou les importez dans PAN-OS.

Lorsqu'un administrateur bloque l'exportation d'une clé privée, aucun administrateur ne peut exporter cette clé, pas même les administrateurs super utilisateurs. Si vous avez besoin d'exporter une clé privée depuis un appareil PAN-OS, régénérez le certificat et la clé sans sélectionner l'option de blocage de l'exportation de la clé privée.

Pour passer à une version antérieure de PAN-OS, vous devez d'abord supprimer les certificats dont les clés privées sont bloquées. Si vous ne supprimez pas les certificats dont les clés privées sont bloquées avant de tenter de déclasser, un message d'erreur vous demande de supprimer ces certificats. Vous ne pouvez pas déclasser tant que vous ne les avez pas supprimés. Après avoir déclassé, réimporter ou régénérer les certificats supprimés si vous en avez besoin.

*Si vous utilisez une infrastructure à clé publique (PKI) d'entreprise pour générer des certificats et des clés privées, bloquez l'exportation des clés privées car vous pouvez les installer sur les nouveaux pare-feu et Panoramas de votre autorité de certification (CA) d'entreprise, il n'y a donc aucune raison de les exporter depuis PAN-OS.*

*Si vous générez des certificats auto-signés sur le pare-feu ou Panorama et que vous appliquez l'option d'exportation de clé privée en bloc, vous ne pouvez pas exporter le certificat et la clé vers d'autres appareils PAN-OS.*

Vous pouvez exporter et importer l'état de l'appareil (**Device** > **Setup** > **Operations**) même si vous bloquez l'exportation de clés privées. Nous incluons les clés privées dans les importations et exportations d'état de périphérique, mais les administrateurs ne peuvent pas les lire ou les décoder.

*Vous pouvez importer ou charger la configuration d'un pare-feu sur un autre pare-feu si la clé principale est la même sur les deux pare-feu. Si la clé principale est différente sur les pare-feux, alors l'importation ou le chargement de la configuration ne fonctionne pas et la validation échoue lors de la lecture des certificats.*

- Génération et blocage d'une clé privée
- Importation et blocage d'une clé privée
- Importation et blocage d'une clé privée pour passerelle IKE
- Vérification du blocage de clé privée

## Génération et blocage d'une clé privée

Bloquez l'exportation d'une clé privée pour empêcher son utilisation abusive après avoir généré un certificat.

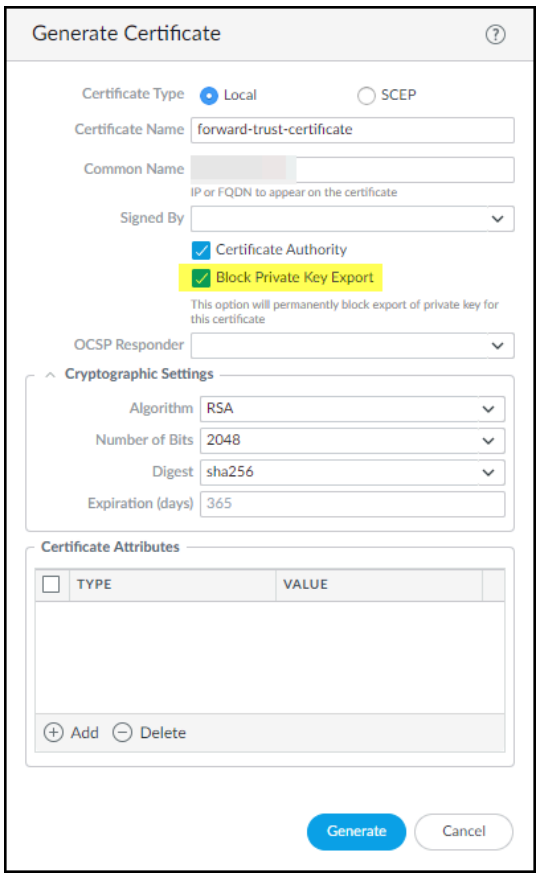
**STEP 1 |** Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**.

S'il existe plus d'un système virtuel, sélectionnez **Location (Emplacement)** ou **Shared (Partagé)** pour le certificat.

**STEP 2 |** **Generate (Générez)** le certificat.

**STEP 3 |** Sélectionnez **Block Private Key Export (Bloquer l'exportation de clés privés)** pour empêcher quiconque d'exporter le certificat.

Consultez la section Génération d'un certificat pour plus d'informations sur les autres champs du certificat.




**STEP 4 |** Cliquez sur **Generate (Générer)** pour générer le nouveau certificat.

*Vous pouvez également générer un certificat et bloquer sa clé privée à l'exportation en utilisant la commande CLI opérationnelle :*

```
admin@pa-220> request certificate generate block-private-keys yes
```

*La commande CLI précédente peut également inclure le certificat et d'autres paramètres qui ne sont pas affichés.*

# Importation et blocage d'une clé privée

Bloquez l'exportation d'une clé privée pour empêcher son utilisation abusive après avoir importé un certificat.

**STEP 1 |** Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**.

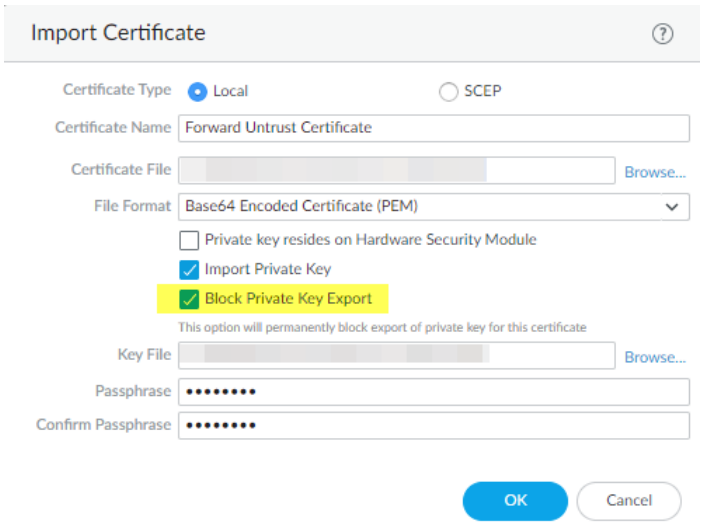
S'il existe plus d'un système virtuel, sélectionnez **Location (Emplacement)** ou **Shared (Partagé)** pour le certificat.

**STEP 2 |** **Import (Importez)** le certificat.

**STEP 3 |** Sélectionnez **Import Private Key (Importer une clé privée)** pour activer l'option permettant de bloquer l'exportation de clés privées.

**STEP 4 |** Sélectionnez **Block Private Key Export (Bloquer l'exportation de clés privés)** pour empêcher quiconque d'exporter le certificat.

Consultez Importation d'un certificat et d'une clé privée pour plus d'informations sur les autres champs d'importation du certificat.



**STEP 5 |** Cliquez sur **OK** pour importer le certificat.

*Si vous utilisez la commande CLI opérationnelle SCP pour importer un certificat ou pour importer une clé privée pour un certificat, vous pouvez toujours bloquer l'exportation de la clé privée :*

- ***admin@pa-220> scp import private-key block-private-key ...***

*Chacune des commandes CLI précédentes peut également inclure des mots clés pour spécifier la source, le nom du certificat et d'autres paramètres qui ne sont pas affichés.*

*Si vous utilisez la commande CLI opérationnelle SCP pour exporter un certificat et inclure sa clé privée (**scp export certificate passphrase <phrase> remote-port <1-65536> to <destination> certificate-name <name> include-key <yes | no> format <der | pem | pkcs10 | pkcs12>**), et si la clé privée du certificat est bloquée, la commande échoue et renvoie un message d'erreur car vous ne pouvez pas exporter une clé privée bloquée.*

## Importation et blocage d'une clé privée pour passerelle IKE

Bloquez l'exportation d'une clé privée pour empêcher son utilisation abusive après avoir généré un certificat pour l'authentification de passerelle IKE.

**STEP 1 |** Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Gateways (Passerelles IKE)**.

**STEP 2 |** **Add (Ajoutez)** une nouvelle passerelle IKE.

**STEP 3 |** Sur l'onglet **General (Général)**, pour **Authentication (Authentification)**, sélectionnez **Certificate (Certificat)**.

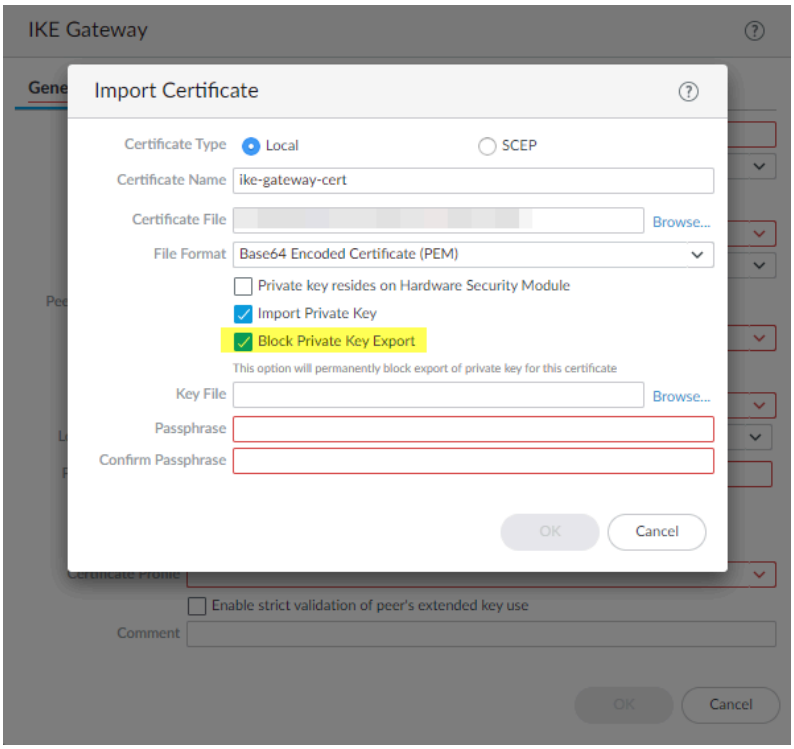
**STEP 4 |** Pour **Local Certificate (Certificat local)** sélectionnez **Import (Importer)** ou **Generate (Générer)** selon que vous souhaitez importer un certificat existant ou créer un certificat.

**STEP 5 |** Saisissez les informations du certificat. Si vous importez le certificat, sélectionnez **Import Private Key (Importer une clé privée)** pour activer la case à cocher **Block Private Key Export (Bloquer l'exportation de clés privées)**.

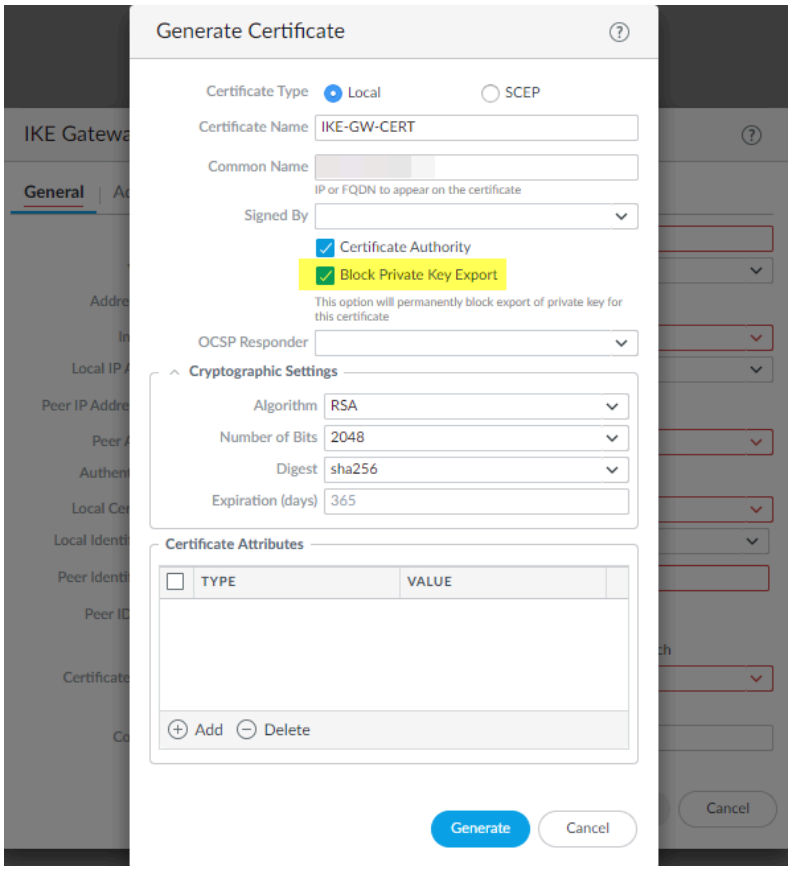
**STEP 6 |** Sélectionnez **Block Private Key Export (Bloquer l'exportation de clés privées)** pour empêcher quiconque d'exporter la clé.

Pour importer d'un certificat, saisissez et confirmez la **Passphrase (Phrase secrète)** puis cliquez sur **OK**




Pour générer un certificat, cliquez sur **Generate (Générer)**.



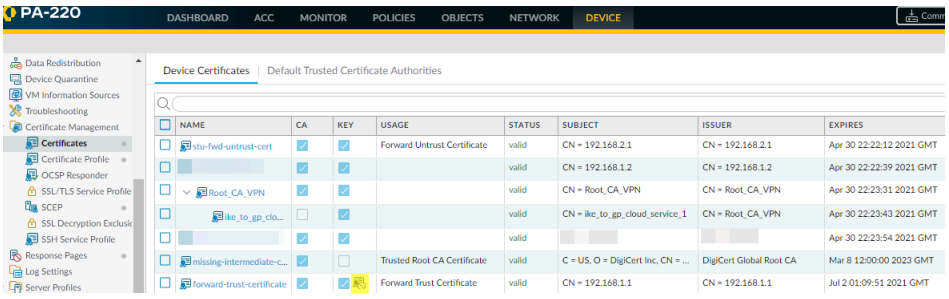

**STEP 7 |** Saisissez la **Passphrase (Phrase secrète)**, confirmez-la, puis cliquez sur **OK**.

## Vérification du blocage de clé privée

Vous pouvez vérifier si une clé privée est bloquée à l'exportation de plusieurs façons.

- Vérifiez la colonne **Key (Clé)** dans **Device (Périphérique)** > **Certificate Management (Gestion de certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**.

  Dans cet exemple, le certificat de confiance de transfert est bloqué :




- Lorsque vous tentez d'exporter un certificat dont la clé privée est bloquée à l'exportation, la case à cocher **Export Private Key (Exporter la clé privée)** n'est pas disponible et vous ne pouvez pas exporter la clé, vous pouvez seulement exporter le certificat.

- Utilisez la commande CLI opérationnelle suivante pour lister tous les certificats sur le périphérique ou dans un Vsys particulier qui ont des clés privées bloquées à l'exportation :

```
admin@pa-220> request certificate show-blocked <shared | vsys>
```

- Utilisez la commande CLI opérationnelle suivante pour vérifier si la clé privée d'un certificat particulier est bloquée à l'exportation :

```
admin@pa-220> request certificate is-blocked certificate-name
 <name>
```

Si le certificat est bloqué à l'exportation, la commande renvoie **yes (oui)** et si le certificat n'est pas bloqué, la commande renvoie **no (non)**.

# Activation de l'exclusion de décryptage SSL par les utilisateurs

Dans les situations sensibles à caractère privé, vous pourriez vouloir alerter vos utilisateurs que le pare-feu déchiffre certains trafics Web et leur permettre d'accéder au site tout en étant conscient du déchiffrement de leur trafic ou mettre fin à la session et leur interdire l'accès au site. (Il n'existe aucune option permettant de se rendre au site et d'éviter également le déchiffrement.)

La première fois qu'un utilisateur tente d'accéder à une application ou à un site HTTPS qui correspond à la politique de déchiffrement, le pare-feu affiche une page de réponse qui informe les utilisateurs que la session sera déchiffrée. Les utilisateurs peuvent soit cliquer sur **Yes (Oui)** pour autoriser le déchiffrement et continuer vers le site ou cliquez sur **No (Non)** pour exclure le déchiffrement et mettre fin à la session. Le choix d'autoriser le déchiffrement s'applique à tous les sites HTTPS auxquels les utilisateurs tentent d'accéder pendant les prochaines 24 heures, après quoi le pare-feu réaffiche la page de réponse. Les utilisateurs qui excluent le décryptage SSL ne peuvent accéder à la page Web demandée ou tout autre site HTTPS pendant la prochaine minute. Une fois la minute écoulée, le pare-feu réaffiche la page de réponse la prochaine fois que les utilisateurs tentent d'accéder au site HTTPS.

Le pare-feu inclut une page d'exclusion de décryptage SSL prédéfinie que vous pouvez activer. Vous pouvez éventuellement personnaliser cette page avec votre propre texte et/ou vos propres images. Cependant, la meilleure pratique consiste à autoriser les utilisateurs à se retirer du déchiffrement.

*Les pages de réponse personnalisées qui dépassent la taille maximale prise en charge ne sont pas déchiffrées ou affichées aux utilisateurs. Dans la version 8.1.2 de PAN-OS et les versions de PAN-OS 8.1 antérieures, les pages de réponse personnalisées sur un site déchiffré ne peuvent dépasser 8 191 octets ; la taille maximale est passée à 17 999 octets dans PAN-OS 8.1.3 et les versions ultérieures.*

**STEP 1 |** (Facultatif) Personnalisez la page d'exclusion de décryptage SSL.

1. Sélectionnez **Device (Périphérique)** > **Response Pages (Pages de réponse)**.
2. Sélectionnez le lien **SSL Decryption Opt-out Page (Page d'exclusion de décryptage SSL)**.
3. Sélectionnez la page **Predefined (Prédéfinie)** et cliquez sur **Export (Exporter)**.
4. À l'aide de l'éditeur de texte HTML de votre choix, modifiez la page.
5. Si vous souhaitez ajouter une image, hébergez-la sur le serveur Web qui est accessible par les systèmes de vos utilisateurs finaux.
6. Ajoutez une ligne dans l'éditeur HTML pour pointer l'image. Par exemple :

   ```
   <img src="http://cdn.slidesharecdn.com/ Acme-logo-96x96.jpg?
   1382722588"/>
   ```

7. Enregistrez la page modifiée avec un nouveau nom de fichier. Veillez à ce que la page conserve son codage UTF-8.
8. De retour sur le pare-feu, sélectionnez **Device (Périphérique)** > **Response Pages (Pages de réponse)**.
9. Sélectionnez le lien **SSL Decryption Opt-out Page (Page d'exclusion de décryptage SSL)**.
10. Cliquez sur **Import (Importer)** puis saisissez le chemin et le nom de fichier dans le champ **Import File (Importer le fichier)** ou **Browse (Naviguez)** pour trouver le fichier.
11. (Facultatif) Sélectionnez le système virtuel sur lequel cette page d'ouverture de session sera utilisée dans la liste déroulante **Destination (Destination)** ou sélectionnez Shared (Partagée) pour la rendre disponible pour tous les systèmes virtuels.
12. Cliquez sur **OK** pour importer le fichier.
13. Sélectionnez la page de réponse que vous venez d'importer et cliquez sur **Close (Fermer)**.

**STEP 2 |** Activez l'exclusion de décryptage SSL.

1. Sous **Device (Périphérique)** > **Response Pages (Pages de réponse)**, cliquez sur le lien **Disabled (Désactivées)**.
2. Sélectionnez l'option **Enable SSL Opt-out Page (Activer la page d'exclusion SSL)** et cliquez sur **OK (OK)**.
3. **Commit (Validez)** les modifications.

**STEP 3 |** Vérifiez que la page d'exclusion SSL s'affiche lorsque vous tentez d'accéder à un site.

Dans un navigateur, accédez à un site crypté qui correspond à votre politique de décryptage. Vérifiez alors que la page d'exclusion de décryptage SSL s'affiche.

# Désactivation temporaire du décryptage SSL

Dans certains cas, il se peut que vous souhaitiez désactiver temporairement le décryptage SSL. Par exemple, si vous avez déployé le déchiffrement SSL trop rapidement et que quelque chose ne fonctionne pas correctement, mais que vous ne savez pas exactement de quoi il s'agit et que vous devez examiner de nombreuses règles, vous pouvez utiliser la CLI pour désactiver temporairement le déchiffrement et prendre le temps d'analyser et de résoudre le problème. Après avoir réglé le problème, vous pouvez utiliser la CLI pour réactiver le déchiffrement SSL. Comme la désactivation temporaire et la réactivation du déchiffrement au moyen de la CLI n'a pas à faire l'objet d'une opération de validation, vous pouvez le faire sans perturber le trafic réseau.

Les commandes CLI suivantes désactivent temporairement le déchiffrement SSL sans validation et réactivent le déchiffrement sans validation.

***La commande de désactiver le déchiffrement SSL ne persiste pas dans la configuration après un redémarrage. Si vous désactivez temporairement le déchiffrement, puis redémarrez le pare-feu, le déchiffrement sera réactivé, que le problème soit résolu ou non.***

- Désactiver le décryptage SSL

```
set system setting
ssl-decrypt skip-ssl-decrypt yes
```

- Réactiver le décryptage SSL

```
set system setting
ssl-decrypt skip-ssl-decrypt no
```

# Configuration de la mise en miroir du port de décryptage

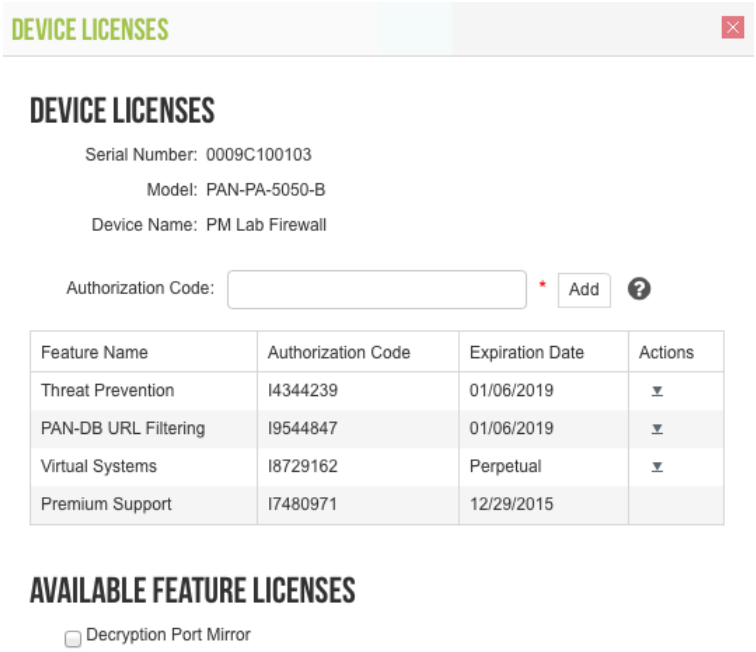
Avant que vous puissiez activer la mise en miroir du déchiffrement, vous devez obtenir et installer une licence de miroir du port de décryptage. La licence est gratuite et peut être activée via le portail de support comme cela est décrit dans la procédure qui suit. Une fois que vous avez installé la licence de miroir du port de décryptage et redémarré le pare-feu, vous pouvez activer le miroir du port de décryptage.

N'oubliez pas que le décryptage, le stockage, l'inspection et/ou l'utilisation du trafic SSL sont régis par la législation dans certains pays et que le consentement des utilisateurs peut être exigé afin d'utiliser la fonction Miroir du décryptage. En outre, l'utilisation de cette fonction pourrait accorder à des utilisateurs malveillants un accès administrateur au pare-feu leur permettant de récolter des noms d'utilisateur, des mots de passe, des numéros de sécurité sociale, des numéros de carte de crédit, ou d'autres informations sensibles envoyées via un canal crypté. Palo Alto Networks vous recommande de consulter la direction de votre entreprise avant d'activer et d'utiliser cette fonction dans un environnement de production.

**STEP 1 |** Demandez une licence pour chaque pare-feu sur lequel vous souhaitez activer le miroir du port de déchiffrement.

1. Connectez-vous au site de site Web de support client de Palo Alto Networks et accédez à l'onglet **Assets (Ressources)**.
2. Sélectionnez l'entrée du pare-feu correspondant au pare-feu pour lequel vous souhaitez activer la licence et sélectionnez **Actions (Actions)**.
3. Sélectionnez **Decryption Port Mirror (Miroir du port de décryptage)**. Un avis juridique s'affiche.
4. Si vous avez bien compris les implications légales potentielles et les conditions requises et que vous souhaitez toujours configurer la mise en miroir du port de décryptage, cliquez sur **I understand and wish to proceed (J'ai compris et je souhaite poursuivre)**.
5. Cliquez sur **Activate (Activer)**.




**STEP 2 |** Installez la licence de miroir du port de déchiffrement sur le pare-feu.

1. Dans l'interface Web du pare-feu, sélectionnez **Device (Périphérique)** > **Licenses (Licences)**.
2. Cliquez sur **Retrieve license keys from license server (Récupérer les clés de licence auprès du serveur de licences)**.
3. Vérifiez que la licence a été activée sur le pare-feu.


4. Redémarrez le pare-feu (**Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)**). Cette fonction n'est pas disponible pour la configuration tant que PAN-OS n'a pas redémarré.

**STEP 3 |** Autorisez le pare-feu à transmettre le trafic déchiffré. L'autorisation Super-utilisateur est obligatoire pour effectuer cette étape.

**Sur un pare-feu prenant en charge la fonction d'un seul système virtuel :**

1. Sélectionnez **Device (Périphérique)** > **Setup( Configuration)** > **Content ID**.
2. Cochez la case **Allow forwarding of decrypted content (Autoriser le transfert de contenu crypté)**.
3. Cliquez sur **OK (OK)** pour enregistrer les paramètres.

**Sur un pare-feu prenant en charge la fonction de systèmes virtuels multiples :**

1. Sélectionnez **Device (Périphérique)** > **Virtual System (Système virtuel).**
2. Sélectionnez un système virtuel à modifier ou créez un nouveau système virtuel en sélectionnant **Add (Ajouter)**.
3. Cochez la case **Allow forwarding of decrypted content (Autoriser le transfert de contenu crypté)**.
4. Cliquez sur **OK (OK)** pour enregistrer les paramètres.

**STEP 4 |** Activez une interface Ethernet à utiliser pour la mise en miroir du déchiffrement.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**.
2. Sélectionnez l'interface Ethernet que vous souhaitez configurer pour le miroir du port de décryptage.
3. Sélectionnez **Decrypt Mirror (Miroir de décryptage)** pour le **Interface Type (Type d'interface)**.

   Ce type d'interface n'apparaît que si la licence de miroir du port de décryptage est installée.
4. Cliquez sur **OK (OK)** pour enregistrer les paramètres.

**STEP 5 |** Activez la mise en miroir du trafic déchiffré.

1. Sélectionnez **Objects (Objets)** > **Decryption Profile (Profil de décryptage)**.
2. Sélectionnez une **Interface (Interface)** à utiliser pour la **Decryption Mirroring (Mise en miroir du déchiffrement)**.

   La liste déroulante **Interface (Interface)** contient toutes les interfaces Ethernet qui ont été définies pour le type : **Decrypt Mirror (Miroir de décryptage)**.
3. Précisez si le trafic décrypté doit être mis en miroir avant ou après l'application de politiques.

   Par défaut, le pare-feu mettra en miroir tout le trafic décrypté sur l'interface avant la recherche des politiques de sécurité, ce qui vous permet de rejouer les événements et d'analyser le trafic qui génère une menace ou déclenche une action d'abandon. Si vous souhaitez uniquement mettre en miroir le trafic décrypté après l'application de politiques de sécurité, cochez la case **Forwarded Only (Trafic transféré uniquement)**. Avec cette option, seul le trafic qui est transféré vers le pare-feu est mis en miroir. Cette option est utile si vous transférez le trafic décrypté vers d'autres périphériques de détection des menaces, tels qu'un périphérique DLP (prévention des fuites de données) ou un autre système de prévention des intrusions (IPS).
4. Cliquez sur **OK (OK)** pour enregistrer le profil de décryptage.

**STEP 6 |** Associez la règle de profil de déchiffrement (avec mise en miroir du port de décryptage) à une règle de politique de déchiffrement. Tout le trafic déchiffré en fonction de la règle de politique est mis en miroir.

1. Sélectionnez **Policies (Politiques)** > **Decryption (Déchiffrement)**.
2. Cliquez sur **Add (Ajouter)** pour configurer une politique de décryptage ou sélectionnez une politique de décryptage existante à modifier.
3. Dans l'onglet **Options (Options)**, sélectionnez **Decrypt (Décrypter)** et le **Decryption Profile (Profil de décryptage)** créé à l'étape 4.
4. Cliquez sur **OK (OK)** pour enregistrer la politique.

**STEP 7 |** Enregistrer la configuration.

Cliquez sur **Commit (Valider)**.

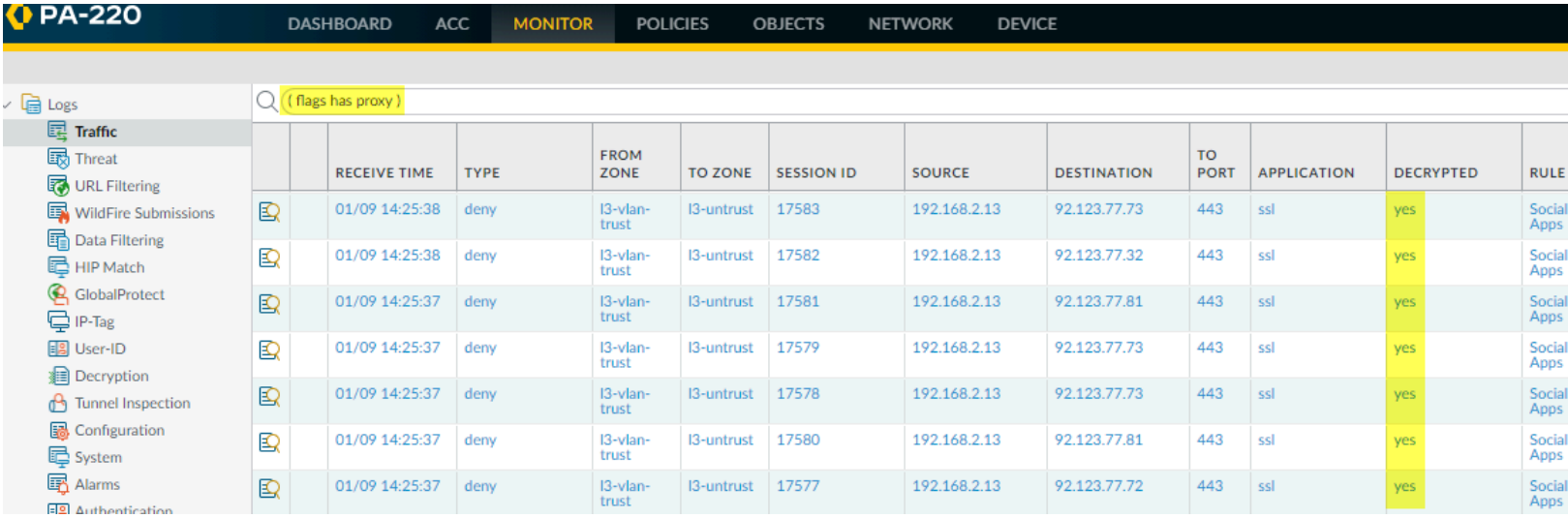
 

# Vérification du déchiffrement

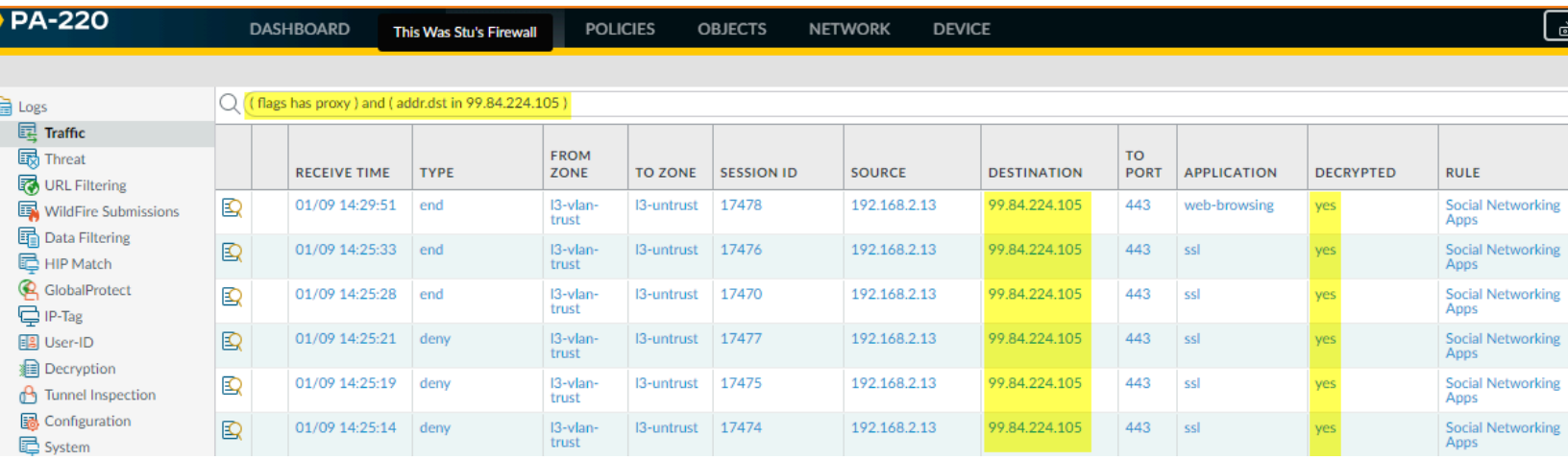
Après avoir configuré un profil de décryptage des meilleures pratiques et l'avoir appliqué au trafic, vous pouvez vérifier à la fois les journaux de décryptage (introduits dans PAN-OS 10.0) et les journaux du trafic pour vérifier que le pare-feu décrypte le trafic que vous avez l'intention de décrypter et que le pare-feu ne décrypte pas le trafic que vous ne voulez pas décrypter. Cette rubrique vous montre comment vérifier le décryptage à l'aide des journaux du trafic. De plus, veuillez suivre les pratiques exemplaires en matière de déchiffrement post-déploiement pour maintenir le déploiement.

- **Afficher les sessions de trafic déchiffrées** : Filtrez les journaux de trafic (**Monitor (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)**) en utilisant le filtre **`( flags has proxy )`**.

  Ce filtre n'affiche que les journaux pour lesquels l'indicateur de proxy SSL est activé, c'est-à-dire le trafic déchiffré (la valeur yes (oui) est indiquée dans la colonne **Decrypted (Déchiffré)** de chaque entrée du journal).



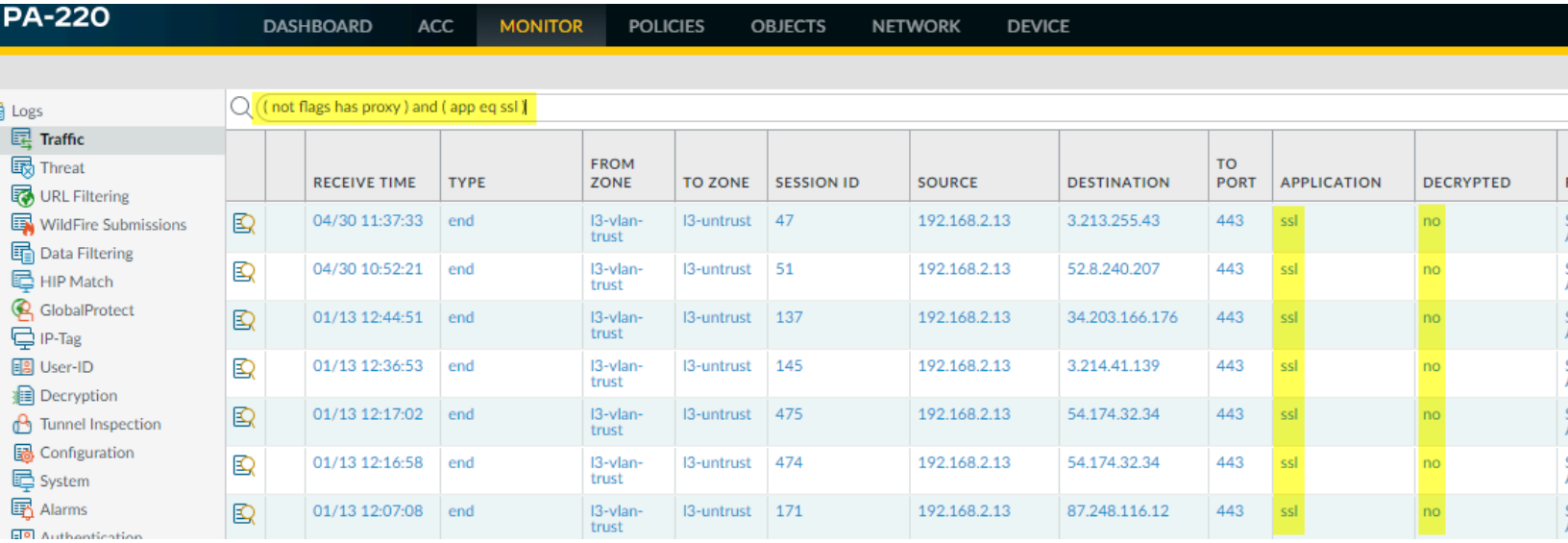

Vous pouvez filtrer le trafic de manière plus granulaire en ajoutant plus de termes au filtre. Par exemple, vous pouvez filtrer le trafic déchiffré qui est transmis uniquement à l'adresse IP de destination 99.84.224.105 en ajoutant le filtre **`(addr.dst in 99.84.224.105)`** :



- **Affichez les sessions de trafic SSL qui ne sont pas décryptées** : filtrez les journaux du trafic (**Monitor (Moniteur)** > **Logs (Journaux)** > **Traffic (Trafic)**) au moyen du filtre **`(not flags has proxy) and (app eq ssl)`**.

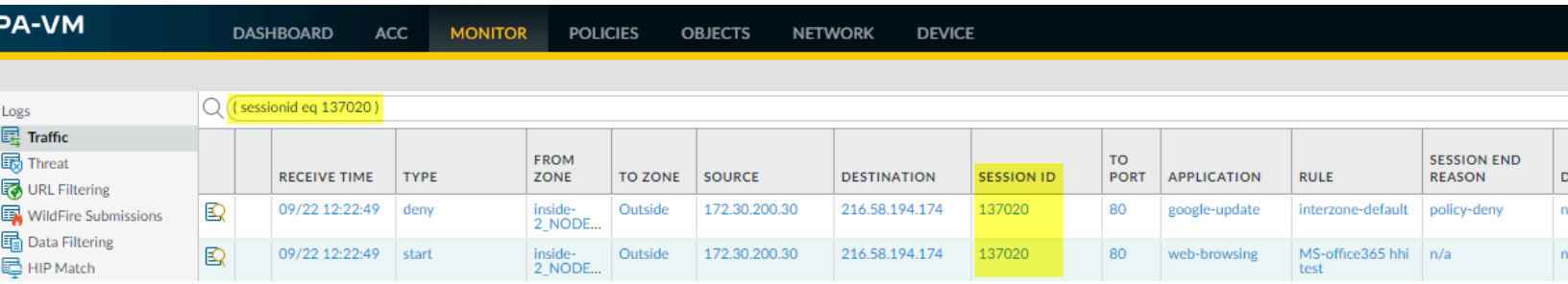
  Ce filtre n'affiche que les journaux pour lesquels l'indicateur de proxy SSL est désactivé (c'est-à-dire le trafic chiffré uniquement). La valeur **no (non)** est indiquée dans la colonne **Decrypted (Déchiffré)** et la valeur **ssl** est indiquée dans la colonne **Application** de chaque entrée du journal.




Tout comme c'était le cas pour l'affichage des journaux de trafic déchiffrés, vous pouvez ajouter des termes pour filtrer le trafic que vous ne déchiffrez pas d'une manière plus granulaire.

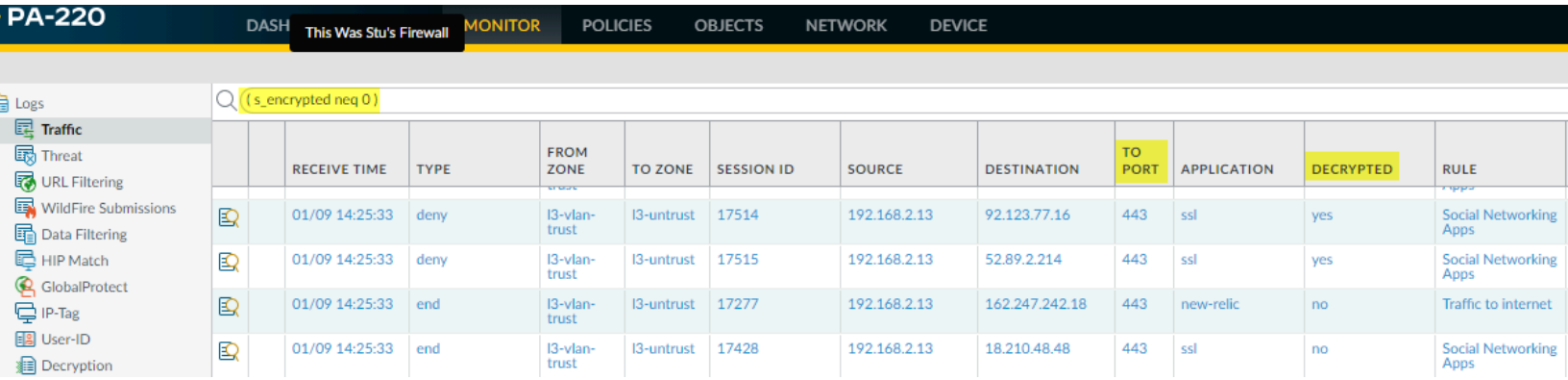
- **Affichez le journal d'une session particulière** : pour afficher le journal de décryptage d'une session donnée, filtrez l'ID de session.

  Par exemple, pour voir le journal d'une session dont l'ID est 137020, filtrez en utilisant le terme **`(sessionid eq 137020)`**. Vous pouvez trouver le numéro de l'ID dans la colonne Session ID (ID de session) de la sortie du journal, comme présenté sur les écrans précédents. Si la colonne Session ID (ID de session) ne s'affiche pas, ajoutez la colonne à la sortie.



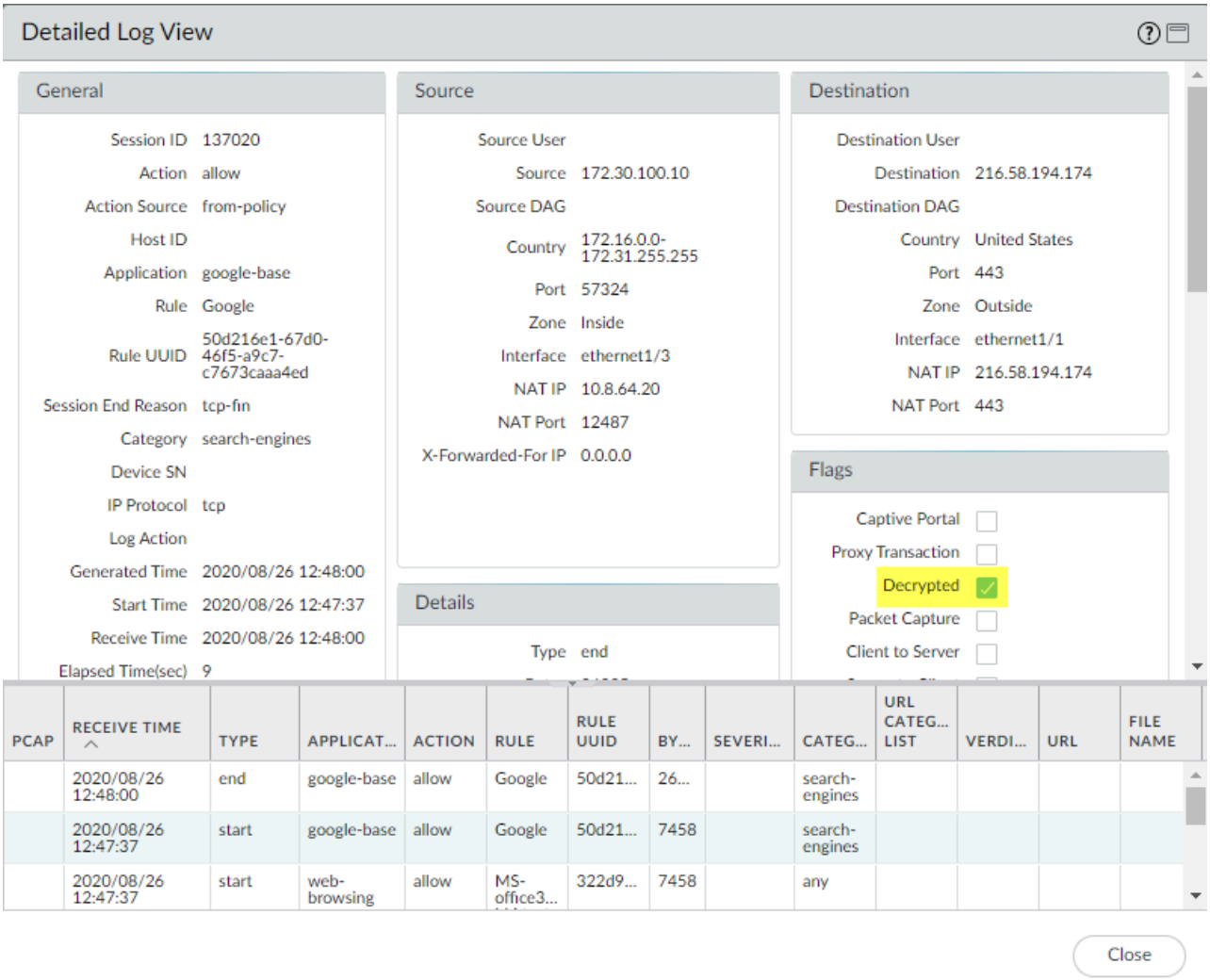

 

- **Affichez tout le trafic TLS et SSH** : filtres les journaux du trafic (**Monitor (Moniteur)** > **Logs (Journaux)** > **Traffic (Trafic)**) pour afficher à la fois le trafic TLS et SSH décrypté et non décrypté à l'aide du filtre **`(s_encrypted neq 0)`** :



- **Accédez aux détails** : Pour voir plus d'informations sur une entrée donnée du journal, cliquez sur la loupe pour afficher un aperçu détaillé du journal. Par exemple, pour l'ID de session 137020 (présenté à la puce précédente), voici un aperçu du journal détaillé :




La case de l'indicateur **Decrypted (Déchiffré)** offre une deuxième façon de vérifier si le trafic est déchiffré.

Vous pouvez également prendre des captures de paquets en amont ou en aval du trafic déchiffré pour voir comment le pare-feu traite le trafic SSL et quelle action il prend à l'égard des paquets, ou vous pouvez procéder à une inspection approfondie des paquets.

# Dépannage et surveillance du décryptage

Les outils de dépannage offrent une meilleure visibilité sur le trafic TLS afin que vous puissiez surveiller votre déploiement de décryptage. Ces outils vous permettent de diagnostiquer et de résoudre rapidement et facilement les problèmes de décryptage, de remédier aux faiblesses de votre déploiement de décryptage et de corriger les problèmes de décryptage pour améliorer votre posture de sécurité. Par exemple, vous pouvez :

- Identifiez le trafic qui provoque des défaillances de décryptage par l'identification du nom de service (SNI) et l'application.
- Identifiez le trafic qui utilise des protocoles et des algorithmes faibles.
- Examinez les activités de décryptage réussies et non réussies dans le réseau.
- Affichez les informations détaillées sur les sessions individuelles.
- Utilisation et modèles de décryptage des profils.
- Surveillez les statistiques de décryptage détaillées et les informations sur l'adoption, les échecs, les versions, les algorithmes, etc.

Les outils suivants fournissent une visibilité complète de la communication TLS et vous aident à dépanner et à surveiller votre déploiement de décryptage :

- **ACC** > **SSL Activity (Activité SSL)** : les cinq widgets ACC de cet onglet (introduits dans PAN-OS 10.0) fournissent des détails sur les activités de décryptage réussies ou non dans votre réseau, y compris les échecs de décryptage, les versions TLS, les échanges de clés, ainsi que la quantité et le type de trafic décrypté et non décrypté.
- **Monitor (Moniteur)** > **Logs (Journaux)** > **Decryption (Décryptage)** : le journal de décryptage (introduit dans PAN-OS 10.0) fournit des informations complètes sur les sessions individuelles qui correspondent à une politique de décryptage (utilisez une politique de non décryptage pour le trafic que vous ne décryptez pas) et sur les sessions GlobalProtect lorsque vous activez la journalisation du décryptage dans la configuration du portail GlobalProtect ou des passerelles GlobalProtect. Sélectionnez les colonnes à afficher pour voir les informations telles que l'application, le SNI, le nom de la politique de décryptage, l'index d'erreur, la version TLS, la version d'échange de clés, l'algorithme de cryptage, les types de clés de certificat et de nombreuses autres caractéristiques. Filtrez les informations dans les colonnes pour identifier le trafic qui utilise des versions et des algorithmes TLS particuliers, des erreurs particulières ou toute autre caractéristique que vous souhaitez étudier. Par défaut, les politiques de décryptage n'enregistrent que les communications TLS avortées. En fonction de la capacité de stockage du journal, vous pouvez configurer les politiques de décryptage pour enregistrer également les communications TLS réussies.
- **Cache d'exclusion de décryptage local** : il existe deux constructions pour les sites qui interrompent le décryptage pour des raisons techniques telles que l'authentification des clients ou les certificats épinglés et qui doivent donc être exclus du décryptage : la liste d'exclusion de décryptage SSL et le cache d'exclusion de décryptage local. La liste d'exclusion de décryptage SSL contient les sites que Palo Alto Networks a identifiés et qui interrompent techniquement le décryptage. Les mises à jour du contenu permettent de maintenir la liste à jour et vous pouvez ajouter des sites à la liste manuellement. Le cache d'exclusion de décryptage local ajoute automatiquement les sites que les utilisateurs locaux rencontrent et qui interrompent le décryptage pour des raisons techniques et les exclut du décryptage, à condition que le profil de

décryptage appliqué au trafic autorise les modes non pris en charge (si les modes non pris en charge sont bloqués, alors le trafic est bloqué au lieu d'être ajouté au cache local).

- **Modèles de rapport personnalisé pour le décryptage** : vous pouvez créer des rapports personnalisés (**Monitor (Moniteur)** > **Manage Custom Reports (Gérer les rapports personnalisés)**) en utilisant quatre modèles prédéfinis qui résument l'activité de décryptage (introduits dans PAN-OS 10.0).

La méthodologie générale de dépannage consiste à utiliser les nouveaux widgets de l'ACC pour identifier le trafic qui provoque des problèmes de décryptage, puis à utiliser le nouveau journal de décryptage et les modèles de rapports personnalisés pour approfondir les détails et mettre en contexte ce trafic, ce qui vous permet de diagnostiquer les problèmes avec précision et beaucoup plus facilement que par le passé. La compréhension des problèmes de décryptage et de leurs causes vous permet de choisir le moyen approprié pour résoudre chaque problème, par exemple :

- Modifier les règles de politique de décryptage (une règle de politique définit le trafic que la règle affecte, les mesures prises sur ce trafic, les paramètres du journal et le profil de décryptage appliqué au trafic)
- Modifier les profils de décryptage (protocoles et algorithmes acceptables pour le trafic qu'une règle de politique de décryptage définit, plus les contrôles d'échec, les contrôles de mode non pris en charge pour des éléments tels que les chiffres et versions non pris en charge, les contrôles de certificat, etc.)
- Ajouter les sites qui interrompent le décryptage pour des raisons techniques à la liste d'exclusion du décryptage SSL
- Évaluer les décisions de sécurité concernant les sites auxquels vos employés, clients et partenaires doivent réellement accéder et les sites que vous pouvez bloquer lorsque les sites utilisent des protocoles ou des algorithmes de décryptage faibles

Les objectifs devraient être de décrypter tout le trafic que vous pouvez décrypter (une meilleure pratique de décryptage) afin que vous puissiez l'inspecter et de traiter correctement le trafic que vous ne décryptez pas.

Lorsque vous passez à PAN-OS 10.0, l'appareil prend 1 % de l'espace de journalisation et l'alloue aux journaux de décryptage. L'étape 3 dans Configuration de la journalisation de décryptage vous montre comment modifier l'allocation d'espace pour les journaux afin de fournir plus d'espace pour les journaux de décryptage.

Si vous passez de PAN-OS 10.1 ou plus à PAN-OS 9.1 ou une version antérieure, les fonctionnalités introduites dans PAN-OS 10.1 (journal de décryptage, widgets d'activité SSL dans l'ACC, modèles de décryptage de rapports personnalisés) sont supprimées de l'interface utilisateur. Les références aux journaux de décryptage sont également supprimées des profils de transfert de journaux. En outre, le cache d'exclusion de décryptage local n'est visible qu'en utilisant la CLI dans PAN-OS 9.1 et les versions antérieures (PAN-OS 10.1 a ajouté le cache local à l'interface utilisateur).

Si vous poussez les configurations de Panorama sur PAN-OS 10.1 ou des versions ultérieures vers des appareils qui fonctionnent sous PAN-OS 9.1 ou des versions antérieures, Panorama supprime les fonctionnalités introduites dans PAN-OS 10.0.

- Widgets du centre de commande des applications de décryptage
- Journal de décryptage
- Modèles de rapport personnalisé pour le décryptage
- Exemples de flux de production de dépannage de décryptage

# Widgets du centre de commande des applications de décryptage

Les widgets de l'Application Command Center (Centre de commande des applications - ACC) pour le décryptage (**ACC** > **SSL Activity**) introduits dans PAN-OS 10.1 fonctionnent avec Journal de décryptage pour vous aider à diagnostiquer et à résoudre rapidement et facilement les problèmes de décryptage. Utilisez le widget **SSL Activity** pour visualiser et analyser l'activité de décryptage du réseau, comme le nombre de sessions décryptées et non décryptées, la quantité de trafic utilisant différentes versions du protocole TLS, les raisons d'échec de décryptage les plus courantes, et les applications et identifications de nom de serveur (SNI) qui utilisent des chiffrements et des algorithmes faibles. Ensuite, utilisez les journaux de décryptage pour approfondir les sessions et diagnostiquer le problème exact afin de pouvoir prendre les mesures appropriées.

PAN-OS 10.1 a introduit cinq nouveaux widgets de décryptage. Utilisez les informations fournies par les widgets pour identifier les politiques et les profils de décryptage mal configurés et pour prendre des décisions éclairées sur le trafic à autoriser et celui à bloquer :

- **Traffic Activity (Activité de trafic)** : montre l'activité SSL/TLS comparée à l'activité non-SSL/TLS par le nombre total de sessions ou par le volume de trafic en octets.
- **SSL/TLS Traffic (Trafic SSL/TLS)** : montre la quantité de trafic décrypté et non décrypté par nombre de sessions ou quantité de trafic en octets. Les raisons pour lesquelles le trafic n'est pas décrypté sont notamment les suivantes :
  - Aucune politique de décryptage n'est appliquée au trafic.
  - La politique de décryptage a intentionnellement exempté le trafic du décryptage (par exemple, une politique de non décryptage).
  - La politique de décryptage a été mal configurée et le trafic était censé être décrypté mais ne l'est pas.
  - Le site se trouve dans la SSL Decryption Exclusion List (Liste d'exclusion de décryptage SSL) (**Device (Périphérique)** > **Certificate Management (Gestion de certificat)** > **SSL Decryption Exclusion (Exclusion de décryptage SSL)**), qui contient des sites que Palo Alto Networks a identifiés comme cassant le décryptage pour des raisons techniques telles que les certificats épinglés ou l'authentification des clients. Pour ces sites, le pare-feu contourne le décryptage.
  - Le site se trouve dans le Local Decryption Exclusion Cache (Cache d'exclusion de décryptage local), qui contient des sites que les utilisateurs locaux rencontrent et qui empêchent le décryptage pour des raisons techniques.

L'ACC ne remplit les trois widgets suivants qu'avec des données provenant du trafic contrôlé par une politique de décryptage. Si vous n'appliquez pas une politique de décryptage au trafic, ce trafic n'alimente pas ces widgets.

- **Decryption Failure Reasons (Raison de l'échec du décryptage)** : indique les raisons des échecs de décryptage : protocole, certificat, version, chiffrement, HSM, ressources, reprise, ou problèmes de fonctionnalités, par SNI. Utilisez ces informations pour détecter les problèmes causés par une politique de décryptage ou une mauvaise configuration du profil ou par un trafic qui utilise des protocoles ou des algorithmes faibles non pris en charge. Cliquez sur une raison d'échec pour approfondir et isoler le nombre de sessions par SNI ayant subi l'échec ou cliquez sur un SNI pour voir tous les échecs de décryptage pour ce SNI.
- **Successful TLS Version Activity (Activité de version TLS réussie)** : affiche les connexions TLS réussies par version TLS pour les applications ou les SNI (les SNI ne sont disponibles que pour le proxy de transfert) afin que vous puissiez évaluer le risque que vous prenez en autorisant des

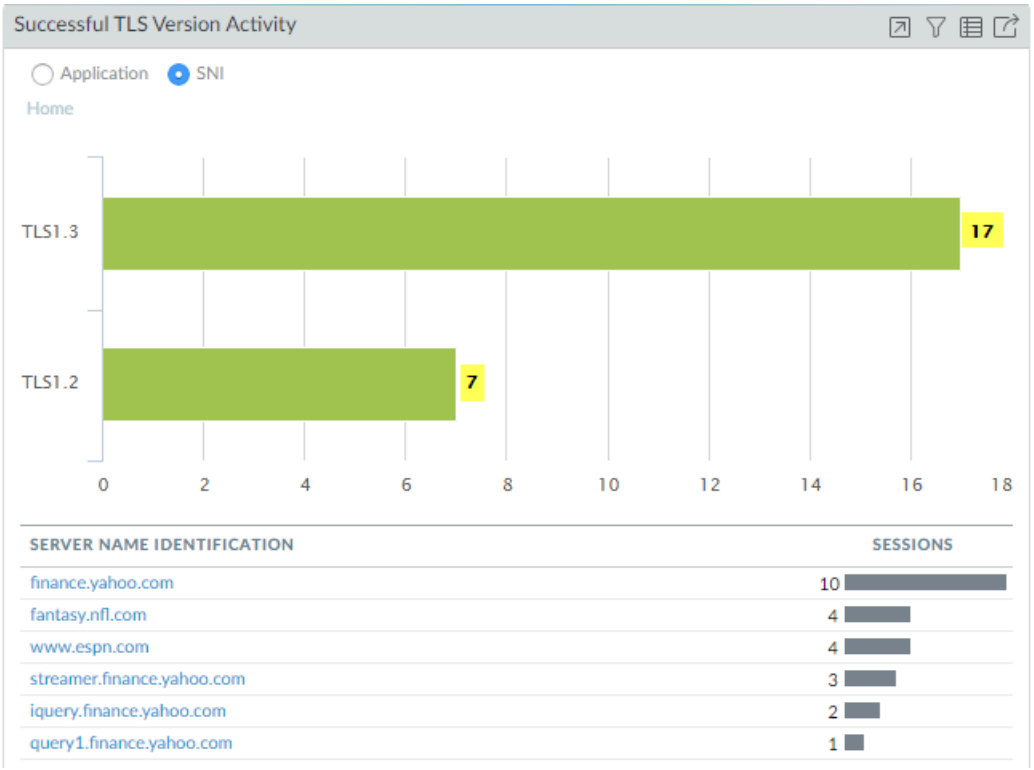
 

versions plus faibles du protocole TLS. L'identification des applications et des SNI qui utilisent des protocoles faibles vous permet d'évaluer chacune d'entre elles et de décider si vous devez en autoriser l'accès pour des raisons professionnelles. Si vous n'avez pas besoin de l'application à des fins professionnelles, vous pouvez bloquer le trafic au lieu de le laisser réduire le risque. Cliquez sur une version de TLS pour accéder aux SNI ou aux applications qui ont utilisé cette version de TLS. Cliquez sur une application ou une SNI pour voir combien de sessions de cette application ou de cette SNI ont utilisé chaque version de TLS.

- **Successful Key Exchange Activity (Activité d'échange de clés réussie)** : montre l'activité d'échange de clés réussie par algorithme pour les applications ou les SNI (les SNI ne sont disponibles que pour le proxy de transfert). Cliquez sur un algorithme d'échange de clés pour voir l'activité de cet algorithme ou cliquez sur une application ou un SNI pour voir l'activité de l'algorithme d'échange de clés pour cette application ou ce SNI.

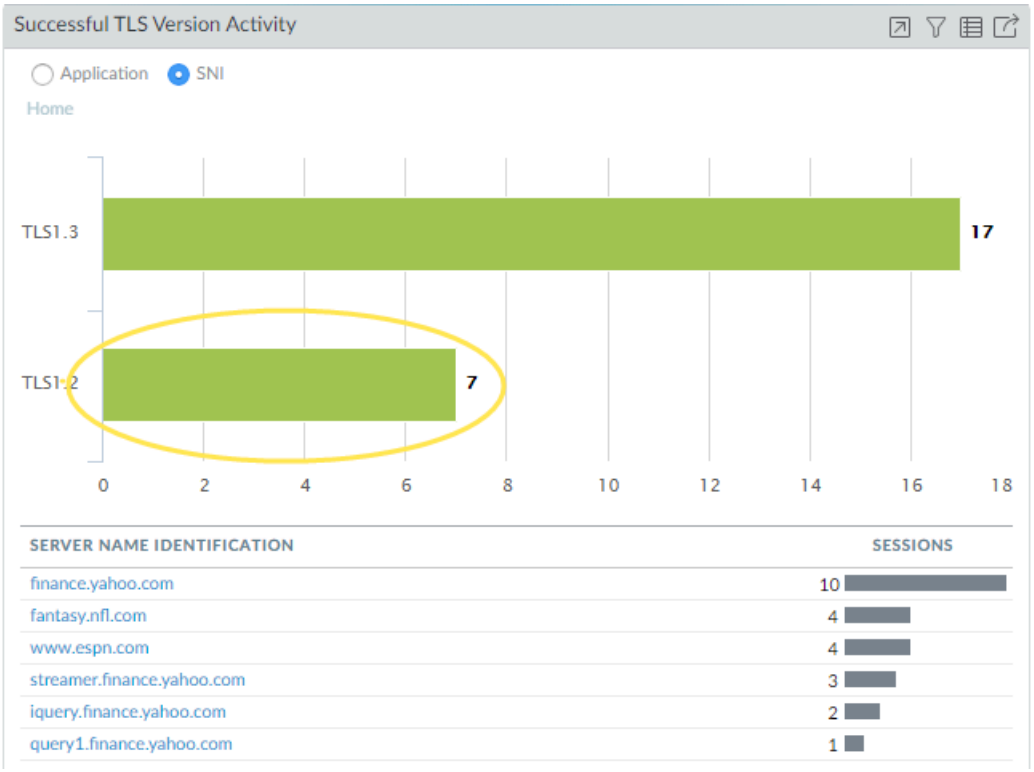
L'exemple suivant d'exploration des données ACC vous montre comment examiner l'activité d'une version TLS réussie :

1. Le widget **Successful TLS Version Activity** montre que dix-sept sessions ont utilisé TLSv1.3 et sept sessions ont utilisé TLSv1.2. La liste des SNI indique les SNI de destination et le nombre de sessions par SNI.

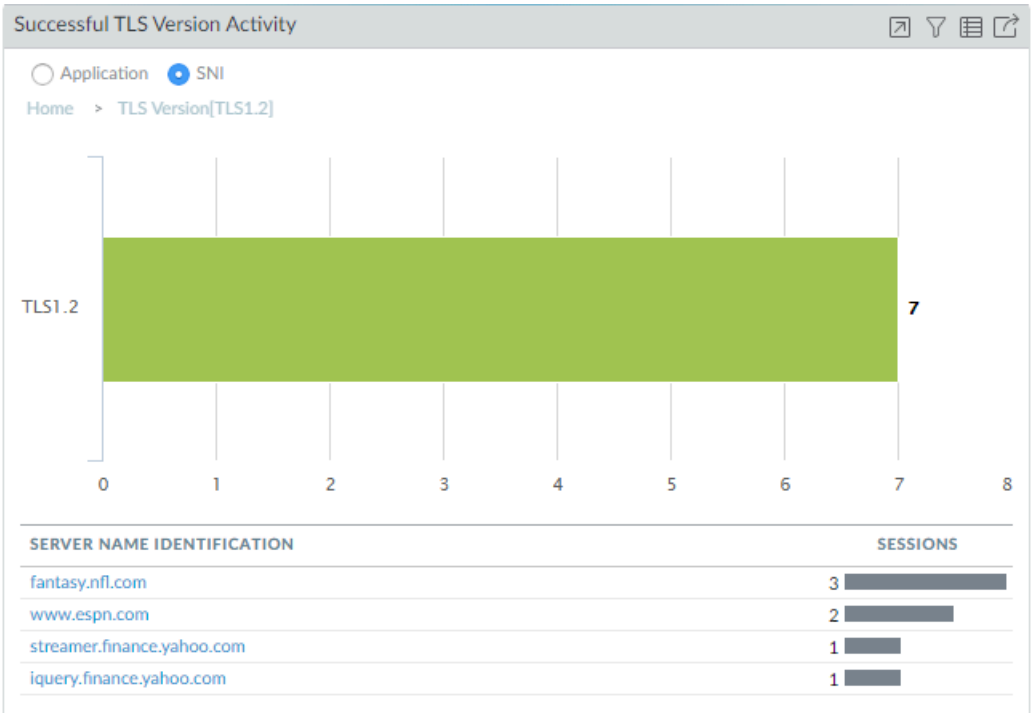


2. Pour voir quels SNI ont utilisé TLSv1.2, cliquez sur la barre verte intitulée TLS1.2.

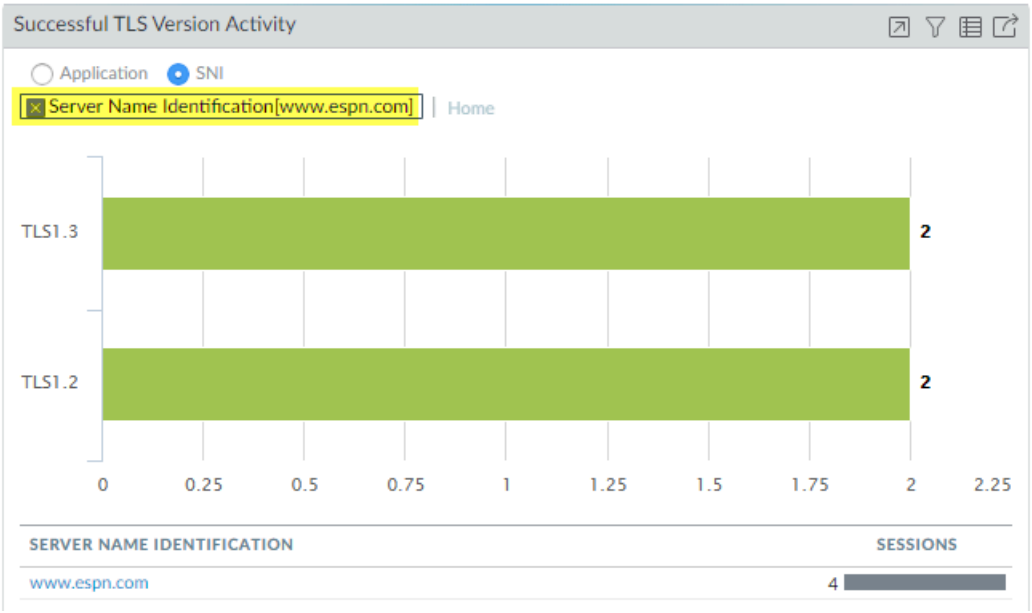



3. Vous pouvez maintenant voir que les sept sessions TLSv1.2 ont été réparties sur quatre serveurs.



4. Cliquez sur **Home (Accueil)** pour revenir à l'écran d'accueil. Maintenant, cliquer sur www.espn.com SNI nous montre les versions TLS qu'il a utilisées. Nous pouvons voir que deux des quatre sessions ont utilisé TLSv1.3 et deux ont utilisé TLSv1.2.




Pour tout widget de décryptage, cliquez sur l'icône Jump to Logs (Accéder aux journaux) pour accéder directement aux journaux de décryptage qui correspondent aux données de l'ACC :


Dans l'exemple précédent, à tout moment de l'enquête, vous pouvez passer aux journaux de décryptage pour que les données soient approfondies. Par exemple, vous pourriez examiner les journaux des sessions individuelles qui ont utilisé TLSv1.2 pour savoir pourquoi elles n'ont pas utilisé TLSv1.3.

Les widgets ACC de décryptage montrent le nom de l'application décryptée basée sur l'App-ID de Palo Alto Networks. Pour remplir l'ACC, le pare-feu ne peut identifier que les applications qui ont un App-ID de Palo Alto Networks ; le pare-feu ne peut pas remplir l'ACC avec des applications personnalisées ou des applications qui n'ont pas d'App-ID. Content updates (Mises à jour du contenu) met à jour régulièrement les App-ID. Il existe d'autres raisons pour lesquelles l'application peut être indiquée comme incomplète ou inconnue :

- Le pare-feu a abandonné la session avant de pouvoir identifier l'application.
- Les journaux de décryptage dépendent des journaux de trafic pour remplir le champ d'application du journal de décryptage. Cependant, si le journal de trafic n'est pas complété en 60 secondes ou moins, le journal de trafic ne remplit pas l'application dans le journal de décryptage et l'application s'affiche comme incomplète ou inconnue.

## Journal de décryptage

Le journal de décryptage (**Monitor (Moniteur)** > **Logs (Journaux)** > **Decryption (Décryptage)**) fournit des informations complètes sur les sessions qui correspondent à une politique de décryptage pour vous aider à mettre en contexte ce trafic afin que vous puissiez diagnostiquer et résoudre précisément et facilement les problèmes de décryptage. Le pare-feu n'enregistre pas le trafic si celui-

ci ne correspond pas à une politique de décryptage. Si vous voulez enregistrer le trafic que vous ne décryptez pas, créez une exclusion de décryptage basée sur les politiques et, pour les politiques qui régissent le trafic TLSv1.2 et antérieur, appliquez un profil de non décryptage au trafic.

PAN-OS prend en charge les journaux de décryptage pour les types de trafic suivants :

- Proxy de transfert : plusieurs champs n'affichent que les informations relatives au trafic du proxy de transfert, notamment le CA racine (pour les certificats fiables uniquement) et l'identification du nom du serveur (SNI).
- Inspection entrante.
- Pas de décryptage (trafic exclu du décryptage par la politique de décryptage).

  ***Comme la session reste cryptée, le pare-feu affiche moins d'informations. Pour le trafic TLSv1.3 non décrypté, il n'y a pas d'informations de certificat car TLSv1.3 crypte les informations de certificat.***

- GlobalProtect : couvre la passerelle GlobalProtect, le portail GlobalProtect et le VPN sans client GlobalProtect (client vers pare-feu uniquement).

  ***GlobalProtect ne prend pas en charge TLSv1.3.***

- Mise en miroir du décryptage

***Tous les types de trafic ne prennent pas en charge tous les paramètres.*** Paramètres non pris en charge par type de proxy et version TLS ***fournit une liste complète des paramètres non pris en charge pour chaque type de trafic de décryptage.***

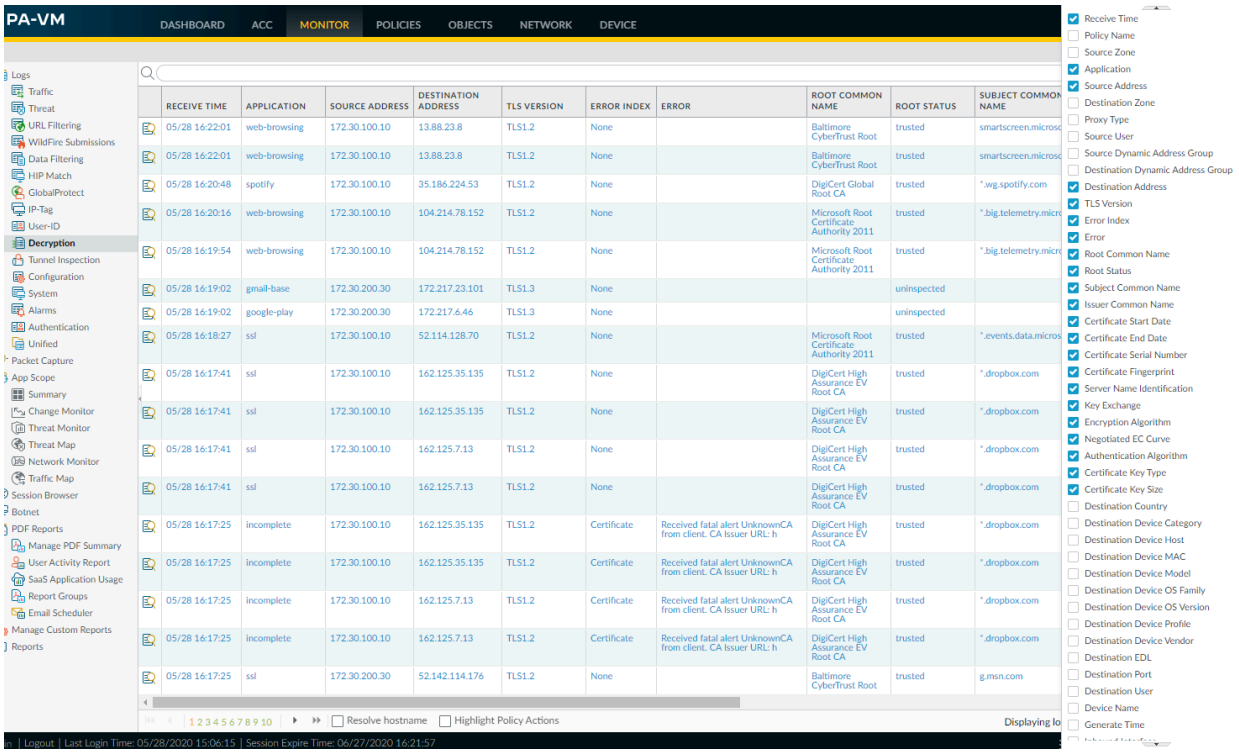
Les données pour le trafic du proxy de transfert sont basées sur la réussite ou l'échec de la communication TLS. En cas de communications TLS avortées, le pare-feu envoie des données d'erreur pour la partie de la transaction qui a provoqué l'erreur, soit de client à pare-feu, soit de pare-feu à serveur. Pour les communications TLS réussies, les données proviennent de la première étape qui s'achève avec succès, qui est généralement de client à pare-feu.

***Le pare-feu ne génère pas d'entrées de journal de déchiffrement pour le trafic Web bloqué lors de***SSL/TLS handshake inspection (inspection de la négociation SSL/TLS)***. Ces sessions n'apparaissent pas dans les journaux de déchiffrement car le pare-feu empêche le déchiffrement lorsqu'il réinitialise la connexion SSL/TLS, mettant fin à la négociation. Vous pouvez afficher les détails des sessions bloquées dans les journaux de filtrage d'URL.***

***Les journaux de décryptage ne sont pas pris en charge pour le trafic du proxy SSH. En outre, les informations relatives aux certificats ne sont pas disponibles pour les journaux de reprise de session.***

Par défaut, le pare-feu enregistre tout trafic de communication TLS avortée. Vous pouvez également enregistrer le trafic de communication TLS réussie si vous le souhaitez. Vous pouvez consulter jusqu'à 62 colonnes d'informations de journal telles que l'application, le SNI, le nom de la politique de décryptage, l'index d'erreur, la version TLS, la version d'échange de clés, l'algorithme de cryptage, les types de clés de certificat et de nombreuses autres caractéristiques :




Cliquez sur l'icône de la loupe ( ) pour voir la vue détaillée du journal d'une session.

*Le journal de décryptage apprend l'App-ID de chaque session à partir du journal de trafic, donc les journaux de trafic doivent être activés pour voir l'App-ID dans le journal de décryptage. Si les journaux de trafic sont désactivés, l'App-ID apparaît comme* ***incomplete (incomplet)****. Par exemple, une grande partie du trafic GlobalProtect est du trafic intra-zone (zone non approuvée vers zone non approuvée), mais la politique intra-zone par défaut n'active pas les journaux de trafic. Pour voir l'App-ID pour le trafic intra-zone de GlobalProtect, vous devez activer le journal du trafic pour le trafic intra-zone.*

*Une autre raison pour laquelle l'App-ID peut s'afficher comme* ***incomplete (incomplet)*** *est que pour les longues sessions, le pare-feu peut générer le journal de décryptage avant que le journal de trafic ne soit complet (le journal de trafic est généralement généré à la fin de la session). Dans ces cas, l'App-ID n'est pas disponible pour le journal de décryptage. En outre, lorsque la communication TLS échoue et génère un journal d'erreurs, l'App-ID n'est pas disponible car l'échec met fin à la session avant que le pare-feu ne puisse déterminer l'App-ID. Dans ces cas, l'application peut s'afficher comme* ***ssl*** *ou* ***incomplete (incomplète)****.*

Pour résoudre les problèmes, utilisez les widgets ACC de décryptage (**ACC** > **SSL Activity**) pour identifier le trafic à l'origine des problèmes de décryptage, puis utilisez le journal de décryptage et Modèles de rapport personnalisé pour le décryptage pour approfondir les détails.

Lorsque vous transmettez les journaux de décryptage pour stockage, assurez-vous que vous sécurisez correctement le transport et le stockage des journaux car les journaux de décryptage contiennent des informations sensibles.

*Lorsque les journaux de décryptage sont activés, le pare-feu envoie des journaux HTTP/2 en tant que journaux d'inspection des tunnels (lorsque les journaux de décryptage sont désactivés, les journaux HTTP/2 sont envoyés en tant que journaux de trafic), vous devez donc vérifier les journaux d'inspection des tunnels plutôt que les journaux de trafic pour les événements HTTP/2. En outre, vous devez activer l'*inspection du contenu du tunnel *pour obtenir l'App-ID pour le trafic HTTP/2.*

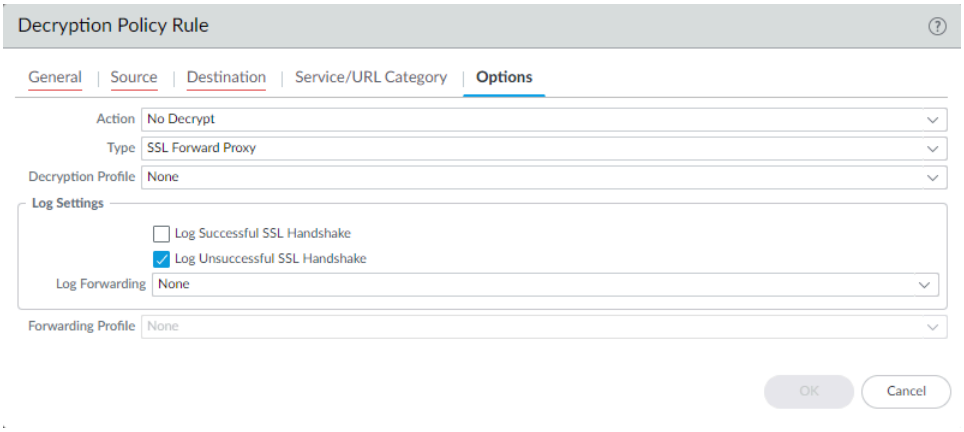
- Configuration de la journalisation de décryptage
- Réparation des chaînes de certificats incomplètes
- Erreurs du journal de décryptage, index d'erreurs et masques

## Configuration de la journalisation de décryptage

Le pare-feu génère des journaux de décryptage pour les sessions régies par une politique de décryptage, y compris les sessions avec une politique de non décryptage. Configurez l'enregistrement du décryptage dans la politique de décryptage qui contrôle le trafic que vous voulez enregistrer.

**STEP 1 |** Configurez le trafic de décryptage que vous souhaitez journaliser dans la politique de décryptage (**Policies** > **Decryption (Décryptage des politiques)**).

Par défaut, le pare-feu ne journalise que les communications TLS avortées.



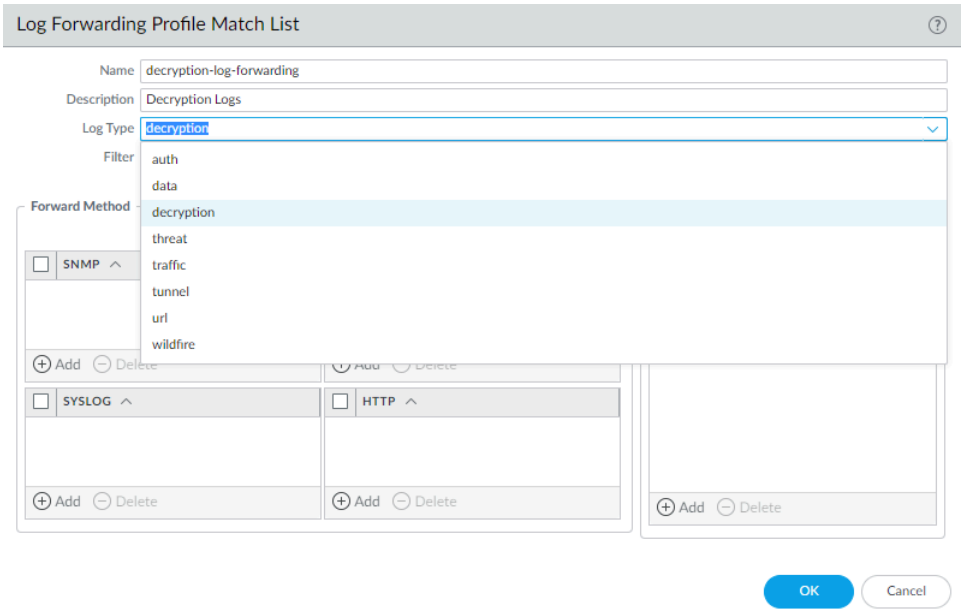

*Journalisez les communications réussies ainsi que les communications avortées afin d'avoir une visibilité sur autant de trafic décrypté que les* resources (ressources) *disponibles de votre périphérique l'autorisent (ne décryptez pas le trafic privé ou sensible ; respectez les* decryption best practices (bonnes pratiques du décryptage) *et décryptez autant de trafic que possible).*

**STEP 2 |** Créez un Log Forwarding profile (Profil de transfert de journal) pour transférer les journaux de décryptage aux collecteurs de journaux, à d'autres périphériques de stockage ou à des

administrateurs spécifiques, puis spécifiez le profil dans le champ **Log Forwarding (Transfert de journal)** de l'onglet **Options** de politique de décryptage.

Pour transmettre les journaux de décryptage, vous devez configurer un profil de transmission de journaux (**Objects** > **Log Forwarding**) afin de spécifier le **Log Type (type de journal)** de décryptage et la méthode de transmission des journaux.



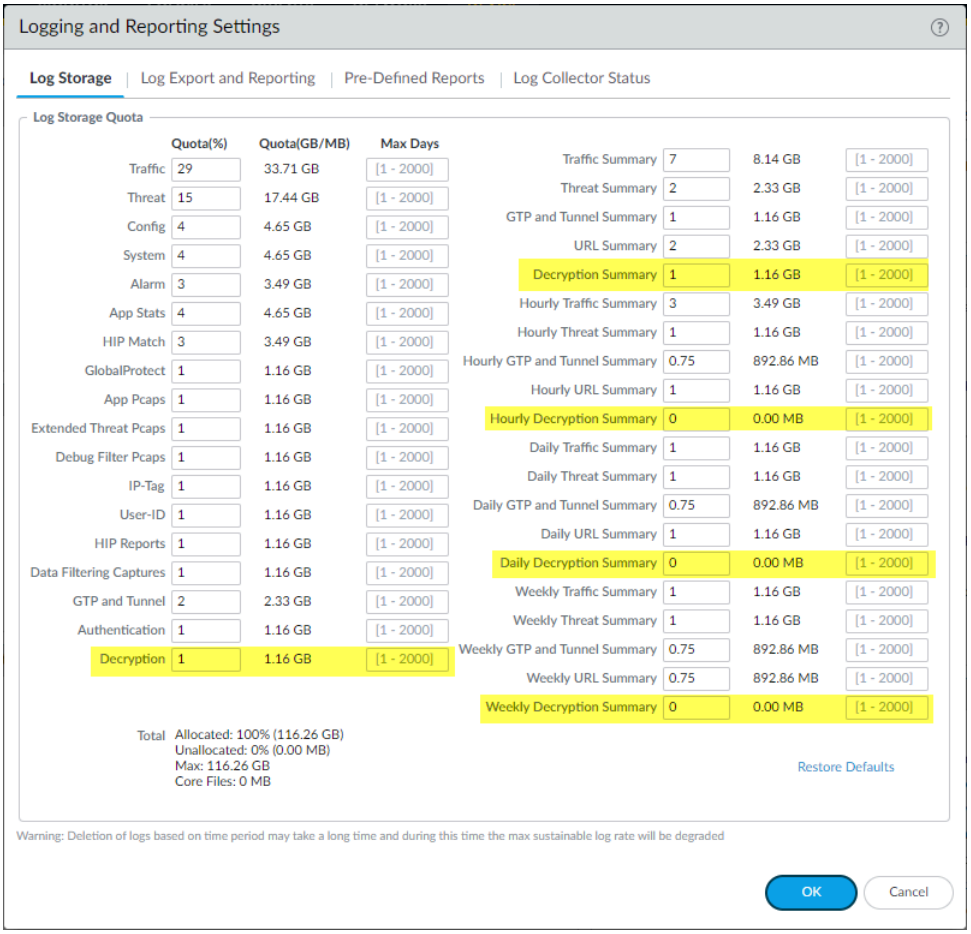

Si vous transmettez les journaux de décryptage, assurez-vous que les journaux sont stockés de manière sécurisée car ils contiennent des informations sensibles.

**STEP 3 |** Si vous journalisez des communications TLS réussies en plus des communications TLS avortées, configurez un quota d'espace de stockage de journaux plus important (**Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **Logging and Reporting Settings (Paramètres de journalisation et de rapports)** > **Log Storage (stockage des journaux)**) pour les journaux de décryptage sur le pare-feu.

Le quota par défaut (attribution) est de un pour cent de la capacité de stockage des journaux du périphérique pour les journaux de décryptage et de un pour cent pour le résumé de décryptage

général. Il n'y a pas d'attribution par défaut pour les résumés de décryptage horaires, quotidiens ou hebdomadaires.




De nombreux facteurs déterminent la quantité de stockage dont vous pouvez avoir besoin pour les journaux de décryptage et ils dépendent de votre déploiement. Tenez compte de ces facteurs, par exemple :

- La quantité de trafic TLS qui passe à travers le pare-feu.
- La quantité de trafic TLS que vous décryptez.
- Votre utilisation d'autres journaux (évaluer à partir de quels journaux vous devriez prendre la capacité à allouer aux journaux de décryptage).
- Si vous enregistrez à la fois les communications TLS réussies et avortées, vous avez probablement besoin de beaucoup plus de capacité que si vous n'enregistrez que les communications TLS avortées. En fonction de la quantité de trafic que vous décryptez, les journaux de décryptage pourraient consommer autant de capacité que les journaux de trafic ou les journaux de menaces et pourraient nécessiter un compromis entre eux si la capacité de l'appareil est déjà entièrement souscrite.

***L'allocation totale combinée des quotas de journal ne peut pas dépasser 100 % des ressources de journal de pare-feu disponibles.***

Vous devrez peut-être faire des expériences pour trouver le bon quota pour chaque catégorie de journaux dans votre déploiement particulier. Si vous n'enregistrez que les communications

avortées, vous pouvez commencer par la valeur par défaut ou augmenter l'allocation à deux ou trois pour cent. Si vous enregistrez les communications réussies et avortées, vous pourriez commencer par allouer environ la moitié de l'espace aux journaux de décryptage que vous attribuez aux journaux de trafic. Les journaux à partir desquels vous prenez l'espace à allouer aux journaux de décryptage dépendent de votre trafic, de votre activité et de vos besoins de surveillance.

## Erreurs du journal de décryptage, index d'erreurs et masques

Les colonnes **Error Index (Index d'erreur)** et **Error (Erreur)** dans le journal de décryptage fournissent des informations sur la catégorie et les détails de l'erreur de décryptage, respectivement. Vous pouvez également consulter les informations relatives aux erreurs et à l'index des erreurs dans la section Handshake Details (Détails de la communication) de la vue détaillée du journal (cliquez sur pour n'importe quelle entrée du journal). L'**Error Index (Index d'erreur)** du journal de décryptage indique l'une des huit catégories d'erreurs :

| Index d'erreur | Erreur (erreurs possibles indiquées pour l'index des erreurs) |
|---|---|
| **certificate** | Erreurs telles que des certificats non valides, des certificats expirés, des certificats de clients non pris en charge, des révocations et des échecs de vérification OCSP/CRL, des CA d'émetteurs non approuvés (sessions signées par une racine non approuvée, ce qui inclut des chaînes de certificats incomplètes) et d'autres erreurs de certificats.<br><br>***Lorsque le pare-feu ne dispose pas d'un certificat intermédiaire parce que le site n'a pas envoyé la chaîne complète de certificats, vous pouvez trouver et installer le certificat manquant sur*** Réparation des chaînes de certificats incomplètes. |
| **Chiffrement** | Erreurs de chiffrement non prises en charge où :<br>• Le client tente de négocier un chiffrement que le pare-feu prend en charge mais que le profil de décryptage appliqué au trafic ne prend pas en charge.<br>• Le client tente de négocier un chiffrement que le pare-feu ne prend pas en charge.<br>• (Rare) L'inspection entrante est activée et les capacités du serveur ne correspondent pas aux paramètres du profil de décryptage.<br><br>Le message d'erreur comprend la valeur du masque de chiffrement client pris en charge et la valeur du masque de chiffrement du profil de décryptage pris en charge. Utilisez les valeurs de masque pour identifier le chiffrement que le client a essayé d'utiliser et pour lister les valeurs de chiffrement que le profil de décryptage prend en charge, comme décrit plus loin dans cette rubrique. |
| **Fonctionnalité** | Erreurs telles que des communications TLS surdimensionnées ou des communications inconnues, des chaînes de certificats surdimensionnées (plus de cinq certificats) et d'autres caractéristiques non prises en charge. |

| Index d'erreur | Erreur (erreurs possibles indiquées pour l'index des erreurs) |
|---|---|
| **HSM** | Les erreurs du module de stockage matériel (HSM) telles que les demandes inconnues, les éléments non trouvés dans la configuration, les délais de demande, et autres erreurs et défaillances du HSM. |
| **Protocole** | Erreurs telles que les échecs de la communication TLS, les décalages entre les clés privées et publiques, les erreurs de Heartbleed, les échecs d'échange de clés TLS et autres erreurs du protocole TLS. Les erreurs de protocole apparaissent lorsque le serveur ne prend pas en charge les protocoles que le client prend en charge, que le serveur utilise des types de certificats que le pare-feu ne prend pas en charge et des erreurs générales du protocole TLS. |
| **Ressource** | Erreurs telles que le manque de mémoire suffisante. |
| **Reprendre** | Erreurs de reprise de session concernant les ID et tickets de reprise de session, les entrées de reprise de session dans le cache du pare-feu, et autres erreurs de reprise de session. |
| **Version** | Erreurs concernant le client et la version du profil de décryptage ne correspondent pas et la version du client et du serveur ne correspondent pas.<br>Le message d'erreur comprend des valeurs de masque qui identifient le client pris en charge et les versions de profil de décryptage. Utilisez les valeurs de masque pour identifier le chiffrement que le client a essayé d'utiliser et pour lister les valeurs de chiffrement que le profil de décryptage prend en charge, comme décrit plus loin dans cette rubrique. |

*Si aucune catégorie de description d'erreur appropriée n'existe pour une erreur, le message par défaut est **General TLS protocol error (Erreur générale du protocole TLS)**.*

Les informations sur les erreurs de version et de chiffrement comprennent des valeurs de masque que vous convertissez en valeurs réelles à l'aide de commandes CLI opérationnelles :

- Les valeurs des masques d'erreur de version identifient les discordances entre les versions du protocole TLS que le client et le serveur utilisent et identifient également les discordances du protocole TLS entre le client et le profil de décryptage appliqué au trafic. La commande CLI pour convertir les masque d'erreur de version est :

  ```
  admin@vm1>debug dataplane show ssl-decrypt bitmask-version
   <bitmask-value>
  ```

  La commande renvoie la version TLS qui correspond au masque.

- Les valeurs de masque d'erreur de chiffrement identifient les erreurs de chiffrement et autres correspondances entre le client et le profil de déchiffrement appliqué au trafic.

  ```
  admin@vm1>debug dataplane show ssl-decrypt bitmask-cipher <bitmask-value>
  ```

  La commande renvoie le chiffrement qui correspond au masque.

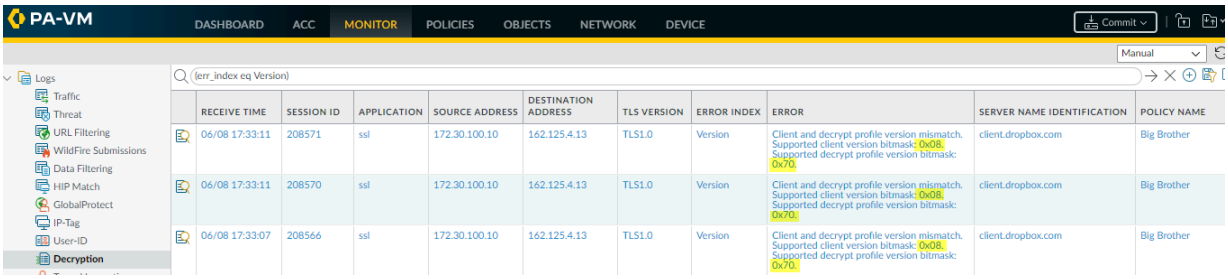
Filtrez le journal de décryptage pour trouver les erreurs de version et de chiffrement, insérez les valeurs du masque pour les sessions comportant des erreurs dans la commande CLI appropriée, obtenez les valeurs de la version du protocole ou du chiffrement qui a causé l'erreur, et utilisez les informations pour mettre à jour la politique ou le profil de décryptage si vous souhaitez autoriser l'accès au site en question.

- Erreurs de version
- Erreurs de chiffrement
- État de la racine « Uninspected » (non inspectée)

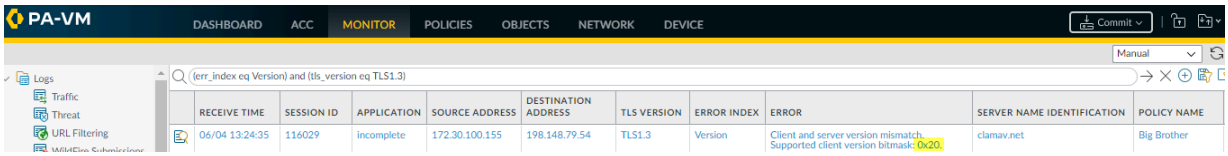
### Erreurs de version

Pour identifier et corriger les erreurs de non-concordance des versions :

1. Filtrez le journal de décryptage pour identifier les erreurs de version à l'aide du filtre **(err_index eq Version)**. Les valeurs mises en évidence sont des valeurs de masque :

   Vous pouvez filtrer le journal de décryptage de plusieurs façons. Par exemple, pour ne voir que les erreurs de la version TLSv1.3, utilisez le filtre **(err_index eq Version) et (tls_version eq TLS1.3)**:

2. Connectez-vous à la CLI et recherchez les valeurs du masque. Les erreurs de version dans la première capture d'écran (les mêmes erreurs pour les trois sessions) montrent un problème de

discordance entre le client et le profil de décryptage, le masque de la version client prise en charge est 0x08 et le masque de la version profil de décryptage prise en charge est 0x70 :

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x08
```

```
TLSv1.0
```

Cette sortie montre que le client ne prend en charge que TLSv1.0.

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x70
```

```
TLSv1.1
```

```
TSLv1.2
```

```
TLSv1.3
```

Cette sortie montre que le profil de décryptage prend en charge TLSv1.1, TLSv1.2 et TLSv1.3, mais pas TLSv1.0. Maintenant vous savez que le problème est que le client ne supporte qu'une très ancienne version du protocole TLS et que le profil de décryptage attaché à la règle de politique de décryptage qui contrôle le trafic n'autorise pas le trafic TLSv1.0.

La prochaine chose à faire est de décider des mesures à prendre. Vous pourriez mettre à jour le client afin qu'il accepte une version TLS plus sûre. Si le client a besoin de TLSv1.0 pour une raison quelconque, vous pouvez continuer à laisser le pare-feu bloquer le trafic, ou vous pouvez mettre à jour le profil de décryptage pour autoriser tout le trafic TLSv1.0 (non recommandé), ou vous pouvez créer une politique et un profil de décryptage qui autorisent TLSv1.0 et l'appliquer uniquement aux périphériques clients qui doivent utiliser TLSv1.0 et ne peuvent pas supporter un protocole plus sûr (option la plus sûre pour autoriser le trafic).

L'erreur de version dans la deuxième capture d'écran montre un problème différent : une discordance entre les versions du client et du serveur. L'erreur indique que le masque du client pris en charge est 0x20 :

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x20
```

```
TLSv1.2
```

La sortie montre que le client ne prend en charge que TLSv1.2. Comme le serveur ne supporte pas TLSv1.2, il peut ne supporter que TLSv1.3 ou il peut ne supporter que TLSv1.1 ou une version inférieure (protocoles moins sécurisés). Vous pouvez utiliser Wireshark ou un autre outil

d'analyse de paquets pour savoir quelle version de TLS le serveur prend en charge. En fonction de ce que le serveur prend en charge, vous pouvez :

- Si le serveur ne supporte que TLSv1.3, vous pouvez modifier le profil de décryptage pour qu'il supporte TLSv1.3.
- Si le serveur ne prend en charge que TLSv1.1 ou une version inférieure, évaluez si vous devez accéder à ce serveur pour des raisons professionnelles. Sinon, envisagez de bloquer le trafic pour accroître la sécurité. Si vous devez accéder au serveur à des fins professionnelles, créez ou ajoutez le serveur à une politique de décryptage qui s'applique uniquement aux serveurs et aux sites auxquels vous devez accéder à des fins professionnelles ; n'autorisez pas l'accès à tous les serveurs qui utilisent des versions TLS moins sûres.

3. Pour trouver la politique de décryptage qui contrôle le trafic de la session, consultez la colonne **Policy Name (Nom de la politique)** dans le journal (ou cliquez sur l'icône de la loupe à côté du journal de décryptage pour voir les informations dans la section générale de la vue détaillée du journal). Dans l'exemple ci-dessus, le nom de la politique de décryptage est Big Brother. Pour trouver la politique et le profil de décryptage, accédez à **Policies (Politiques)** > **Decryption (Décryptage)**, sélectionnez la politique nommée Big Brother, puis sélectionnez l'onglet **Options**. Le **Decryption profile (Profil de décryptage)** affiche le nom du profil de décryptage.

   Accédez à **Objects (Objets)** > **Decryption (Décryptage)** > **Decryption Profile (Profil de décryptage)**, sélectionnez le profil de décryptage approprié, et modifiez-le pour résoudre le problème de la version.

#### Erreurs de chiffrement

L'utilisation du journal de décryptage pour traquer les erreurs de chiffrement est similaire à la chasse aux erreurs de version, vous filtrez le journal pour trouver les erreurs et obtenir des masques d'erreur. Ensuite, vous accédez à la CLI, convertissez le masque à la valeur d'erreur, puis prenez les mesures appropriées pour résoudre le problème. Par exemple :

1. Filtrez le journal de décryptage pour identifier les erreurs de chiffrement à l'aide du filtre **`(err_index eq Cipher)`**. Examinons, par exemple, une erreur de chiffrement avec le message **Error (Erreur)** `Unsupported cipher (Chiffrement non pris en charge). Masque de chiffrement du client pris en charge : 0x80000000. Masque de chiffrement du profil de décryptage pris en charge 0x60f79980.`

2. Connectez-vous à la CLI et recherchez les valeurs du masque :

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-cipher
 0x80000000
```

```
CHACHA_PLY1305_SHA256
```

Cette sortie montre que le client a essayé de négocier un chiffrement que le pare-feu prend en charge (si le masque est entièrement constitué de zéros (`0x0000000`), alors le client a essayé de négocier un chiffrement que le pare-feu ne prend pas en charge) :

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-cipher
 0x80000000
```

```
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS13_WITH_AES_256_GCM_SHA384
TLS13_WITH_AES_128_GCM_SHA256
```

Cette sortie montre que le profil de décryptage qui contrôle le trafic supporte de nombreux chiffrements, mais ne supporte pas le chiffrement que le client essaie d'utiliser.

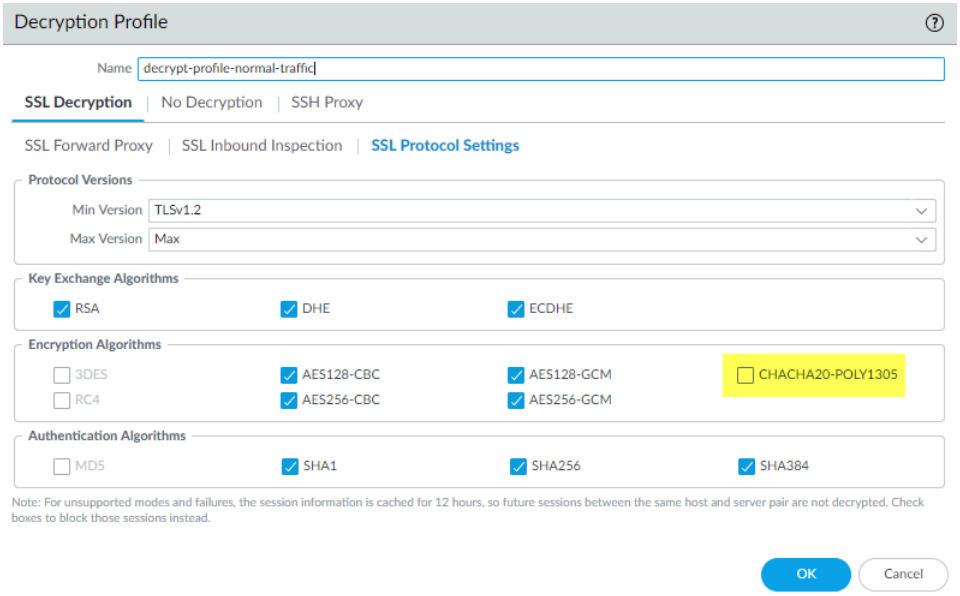
Pour résoudre ce problème afin que le pare-feu autorise et décrypte le trafic, vous devez ajouter la prise en charge du chiffrement manquant au profil de décryptage.

3. Vérifiez le journal de décryptage ou le **Policy Name (Nom de la politique)** de la vue détaillée du journal pour obtenir le nom de la politique de décryptage qui contrôle le trafic. Accédez à **Policies (Politiques)** > **Decryption (Décryptage)** et sélectionnez la politique. Sur l'onglet **Options**, recherchez le nom du profil de décryptage. Accédez ensuite à **Objects (Objets)** > **Decryption**

**(Décryptage)** > **Decryption Profile (Profil de décryptage)**, sélectionnez le profil de décryptage approprié, et modifiez-le pour résoudre le problème de la version.

Dans cet exemple, le profil de décryptage ne prend pas en charge le chiffrement TLS13_WITH_CHACHA_POLY1305_SHA256, le client ne peut donc pas se connecter :




Pour résoudre le problème, sélectionnez l'option d'algorithme de chiffrement **CHACHA20-POLY1305** (le paramètre **Max Version (Version max)** de **Max** signifie que le profil prend déjà en charge TLSv1.3 et le paramètre Authentication Algorithm (Algorithme d'authentification) inclut déjà SHA256, donc seule la prise en charge de l'algorithme de chiffrement était manquante), puis **Commit (Validez)** la configuration. Après avoir validé la configuration, le profil de décryptage prend en charge le chiffrement manquant et les sessions de décryptage pour le trafic réussissent.

*Si le pare-feu ne prend pas en charge une suite de chiffrement et que vous devez autoriser le trafic à des fins professionnelles, créez une politique et un profil de déchiffrement qui s'appliquent uniquement à ce trafic. Dans le profil de décryptage, désactivez l'option **Block sessions with unsupported cipher suites (Bloquer les sessions avec des suites de chiffrement non prises en charge)***

.

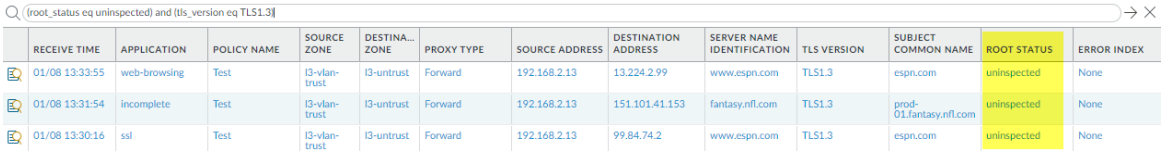
### État de la racine « Uninspected » (non inspectée)

Dans certains cas, la colonne **Root Status (État de la racine)** affiche la valeur **uninspected (non inspectée)**. Il y a plusieurs raisons pour lesquelles le pare-feu n'a pas pu inspecter l'état de la racine, notamment :

- Reprise de session.
- Le trafic n'a pas été décrypté car une politique de non décryptage contrôlait le trafic, donc le pare-feu n'a pas décrypté le trafic.
- Une défaillance de décryptage s'est produite avant que le pare-feu ne puisse inspecter le certificat du serveur.

Filtrez le journal de décryptage **(root_status eq uninspected) et (tls_version eq TLS1.3)** pour voir les sessions de décryptage pour lesquelles le statut de la racine n'est pas inspecté :




| RECEIVE TIME | APPLICATION | POLICY NAME | SOURCE ZONE | DESTINA... ZONE | PROXY TYPE | SOURCE ADDRESS | DESTINATION ADDRESS | SERVER NAME IDENTIFICATION | TLS VERSION | SUBJECT COMMON NAME | ROOT STATUS | ERROR INDEX |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01/08 13:33:55 | web-browsing | Test | l3-vlan-trust | l3-untrust | Forward | 192.168.2.13 | 13.224.2.99 | www.espn.com | TLS1.3 | espn.com | uninspected | None |
| 01/08 13:31:54 | incomplete | Test | l3-vlan-trust | l3-untrust | Forward | 192.168.2.13 | 151.101.41.153 | fantasy.nfl.com | TLS1.3 | prod-01.fantasy.nfl.com | uninspected | None |
| 01/08 13:30:16 | ssl | Test | l3-vlan-trust | l3-untrust | Forward | 192.168.2.13 | 99.84.74.2 | www.espn.com | TLS1.3 | espn.com | uninspected | None |

## Réparation des chaînes de certificats incomplètes

Tous les sites web n'envoient pas leur chaîne de certificats complète, même si la norme RFC 5246 TLSv1.2 exige que les serveurs authentifiés fournissent une chaîne de certificats valide menant à une autorité de certification acceptable. Lorsque vous activez le décryptage et appliquez un profil de décryptage de proxy de transfert qui permet de **bloquer les sessions avec des émetteurs non approuvés** dans la politique de décryptage, si un certificat intermédiaire manque à la liste de certificats que le serveur du site web présente au pare-feu, celui-ci ne peut pas construire la chaîne de certificats jusqu'au certificat supérieur (racine). Dans ces cas, le pare-feu présente son certificat de non-approbation de transfert au client parce que le pare-feu ne peut pas construire la chaîne jusqu'au certificat racine et que la confiance ne peut pas être établie sans le certificat intermédiaire manquant.

*Le pare-feu ne possède que des certificats racine dans son magasin* Default Trusted Certificate Authorities (Autorités de certification de confiance par défaut).

Si un site web avec lequel vous devez communiquer à des fins professionnelles a un ou plusieurs certificats intermédiaires manquants et que le profil de décryptage bloque les sessions avec des émetteurs non fiables, vous pouvez alors trouver et télécharger le certificat intermédiaire manquant et l'installer sur le pare-feu en tant que CA racine de confiance afin que le pare-feu fasse confiance au serveur du site. (L'alternative est de contacter le propriétaire du site web et de lui demander de configurer son serveur de manière à ce qu'il envoie le certificat intermédiaire lors de la communication).

***Si vous autorisez des sessions avec des émetteurs non fiables dans le profil de décryptage, le pare-feu établit des sessions même si l'émetteur n'est pas approuvé ; toutefois, il est préférable de bloquer les sessions avec des émetteurs non approuvés pour une meilleure sécurité.***

**STEP 1 |** Trouvez les sites web qui provoquent des erreurs de chaîne de certificats incomplètes.

1. Filtrez le journal de décryptage pour identifier les sessions de décryptage qui ont échoué en raison d'une chaîne de certificats incomplète.

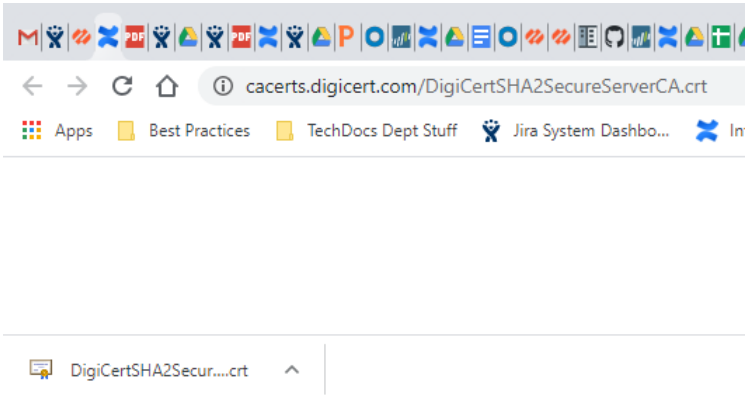
   Dans le champ de filtrage, saisissez la requête **(err_index eq Certificate) et (error contains 'http')**. Cette requête filtre les journaux pour les erreurs de certificat qui contiennent la chaîne « http », qui trouve toutes les entrées d'erreur qui contiennent l'URL de l'émetteur de la CA (souvent appelé URI). L'URL de l'émetteur de la CA est l'information d'accès aux informations de l'autorité (AIA) pour l'émetteur de la CA.

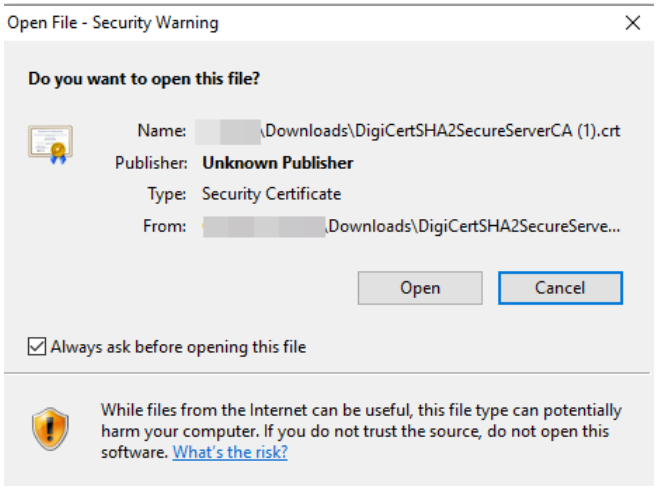
2. Cliquez sur une entrée de la colonne **Error (Erreur)** qui commence par « Received fatal alert UnknownCA from client. CA Issuer URL: » suivi de l'URI.


Le pare-feu ajoute automatiquement l'erreur sélectionnée à la requête et affiche le chemin URI complet (le chemin URI complet peut être tronqué dans la colonne **Error (Erreur)**).

**STEP 2 |** Copiez et collez l'URI dans votre navigateur, puis appuyez sur la touche Entrée pour télécharger le certificat intermédiaire manquant.

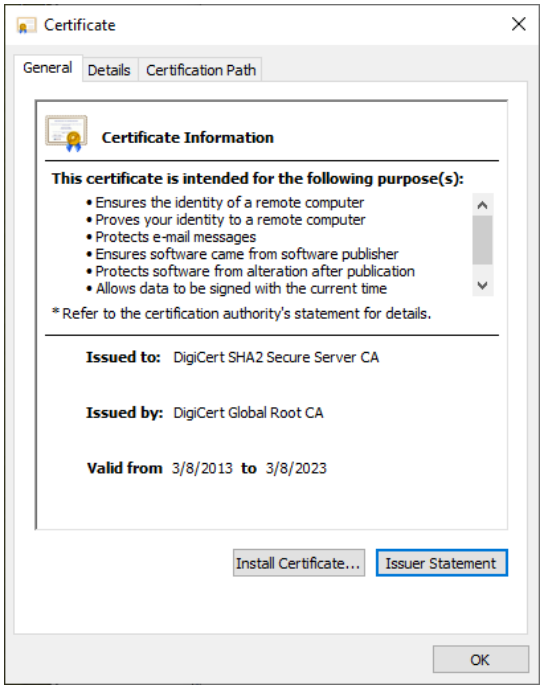



**STEP 3 |** Cliquez sur le certificat pour ouvrir la boîte de dialogue.

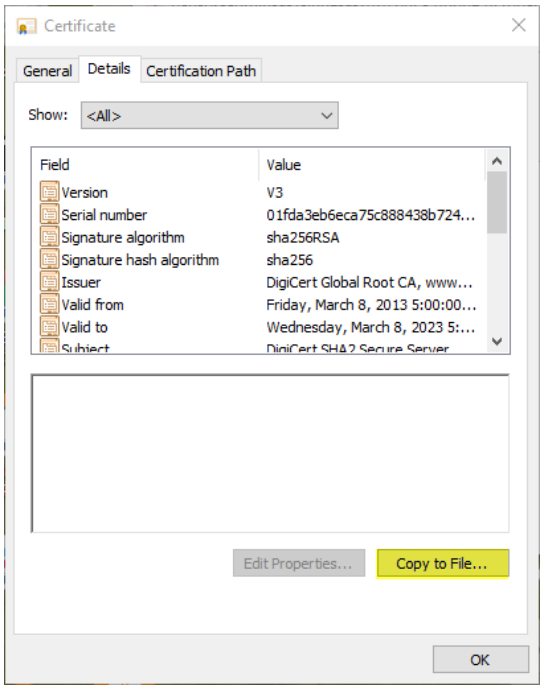


**STEP 4 |** Cliquez sur **Open (Ouvrir)** pour ouvrir le fichier de certificat.



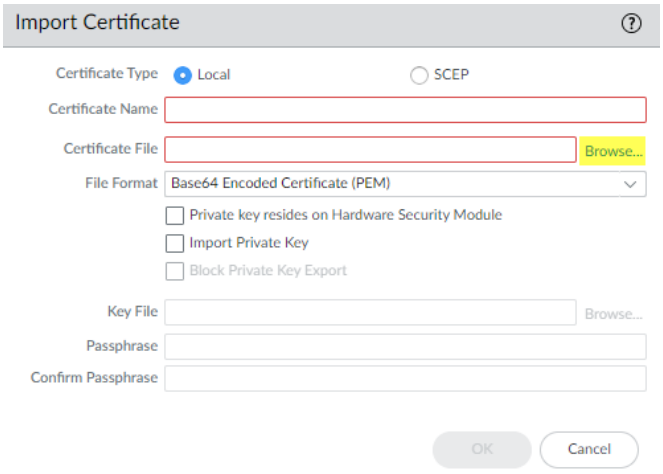

**STEP 5 |** Sélectionnez l'onglet **Details (Détails)** puis cliquez sur **Copy to File... (Copier vers fichier)**.




Suivez les instructions d'exportation. Le certificat est copié dans le dossier que vous avez désigné comme dossier de téléchargement par défaut.

**STEP 6 |** Importez le certificat sur le pare-feu.

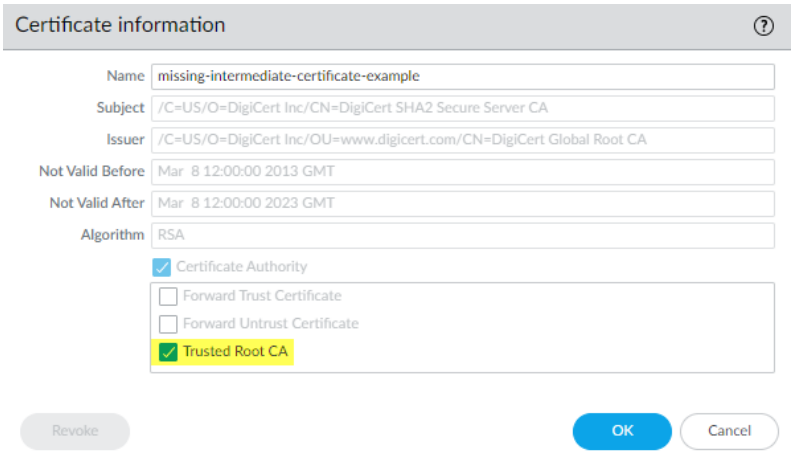
1. Accédez à **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**, puis sélectionnez **Import (Importer)**.
2. **Browse (Parcourez)** le dossier dans lequel vous avez stocké le certificat intermédiaire manquant et sélectionnez-le. Laissez le **File Format (Format du fichier)** sur **Base64 Encoded Certificate (PEM) (Certificat codé en base-64 (PEM))**.




3. Nommez le certificat et indiquez toutes les autres options que vous souhaitez utiliser, puis cliquez sur **OK**.

**STEP 7 |** Lorsque le certificat a été importé, sélectionnez le certificat dans la liste **Device Certificates (Certificats du périphérique)** pour ouvrir la boîte de dialogue Informations sur le certificat.

**STEP 8 |** Sélectionnez **Trusted Root CA (CA racine fiable)** pour marquer le certificat comme une CA racine fiable sur le pare-feu, puis cliquez sur **OK**.




Dans **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats du périphérique)**, le certificat importé figure désormais dans la liste des certificats. Contrôlez la colonne **Usage** pour confirmer que l'état est **Trusted Root CA Certificate (Certificat de CA racine fiable)** pour vérifier que le pare-feu considère le certificat comme une CA racine fiable.

**STEP 9 |** **Commit (Validez)** la configuration.

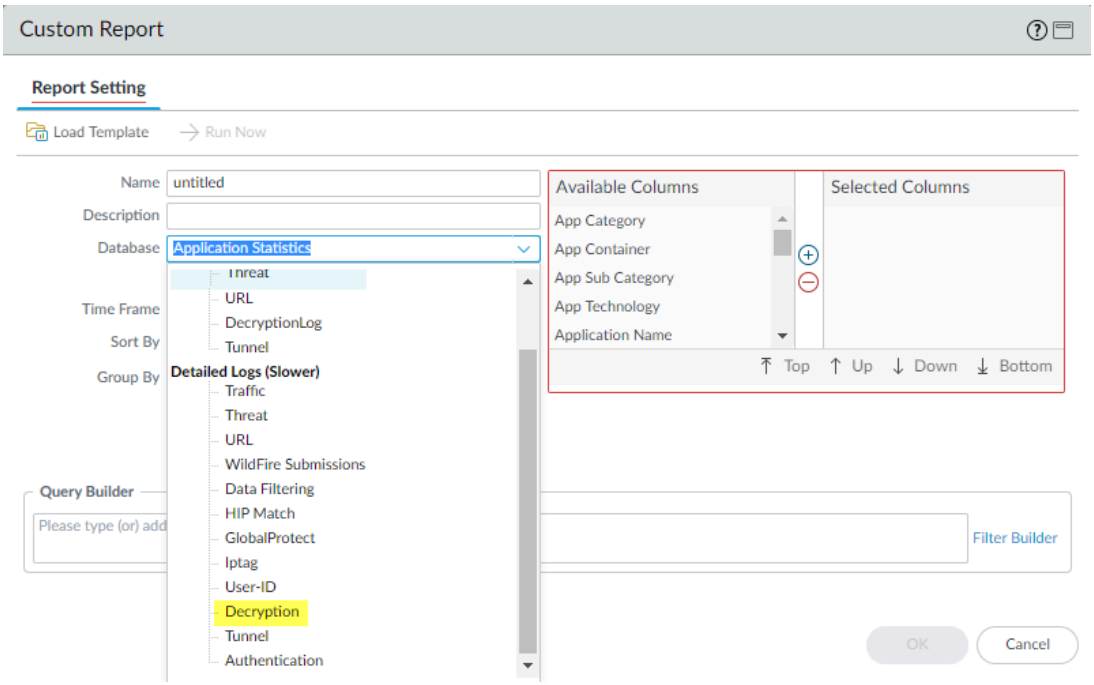
**STEP 10 |** Vous avez maintenant réparé la chaîne de certificats brisée.

Le pare-feu ne bloque pas le trafic parce que l'émetteur de la CA n'est plus non approuvé. Répétez ce processus pour tous les certificats intermédiaires manquants afin de réparer leurs chaînes de certificats.

# Modèles de rapport personnalisé pour le décryptage

Vous pouvez créer des Custom Reports (Rapports personnalisés) et les générer pour les événements de décryptage en vous basant sur les champs du journal de décryptage et les modèles personnalisés. Sélectionnez les champs du journal à inclure dans les rapports personnalisés et sélectionnez des modèles pour affiner la requête du journal :

1. **Monitor (Moniteur)** > **Manage Custom Reports (Gérer les rapports personnalisés)**.
2. **Add (Ajoutez)** un rapport personnalisé.
3. Pour configurer les champs du journal de décryptage à utiliser dans le rapport personnalisé, sélectionnez **Decryption (Décryptage)** comme **Database (Base de données)**.

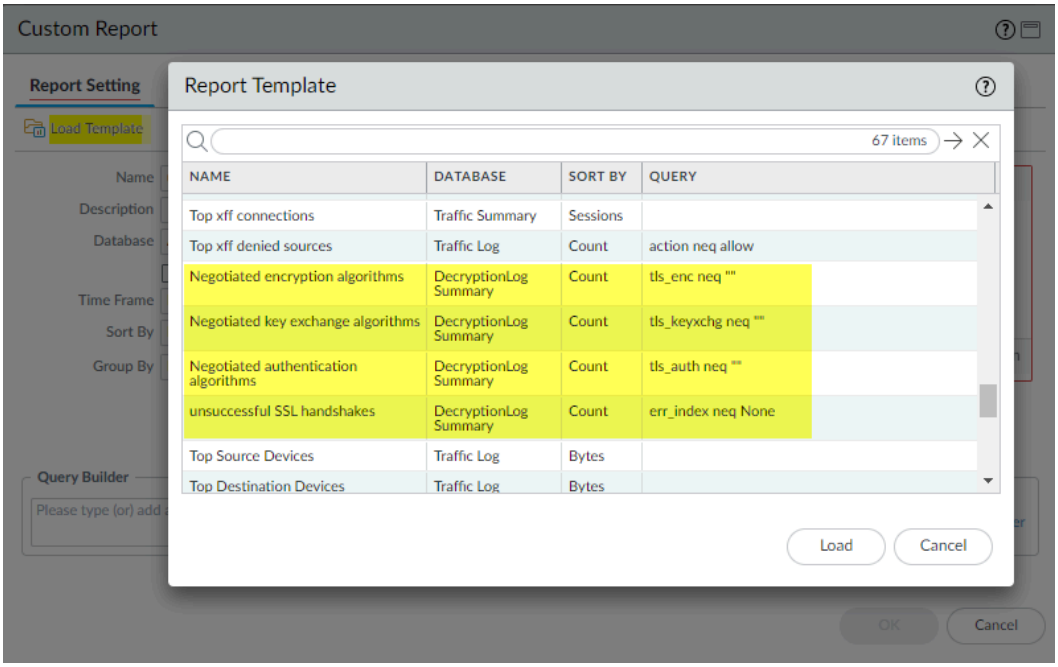



La liste **Available Columns (Colonnes disponibles)** change pour correspondre aux colonnes disponibles dans le journal de décryptage. Sélectionnez et ajoutez les colonnes (informations) que vous souhaitez inclure dans le rapport personnalisé. Si vous ne souhaitez pas affiner davantage le rapport personnalisé, cliquez sur **OK** pour générer le rapport.

4. Si vous le souhaitez, affinez la sortie du rapport de décryptage personnalisé en utilisant le générateur de requêtes et les quatre modèles introduits dans PAN-OS 10.0. Pour sélectionner

un modèle pour filtrer la sortie du rapport, cliquez sur **Load Template (Charger un modèle)** et choisissez parmi les quatre modèles de décryptage :




La colonne **Query (Requête)** montre la requête de filtre que chaque modèle représente. **Load (Chargez)** la requête souhaitée puis cliquez sur **OK** pour générer le rapport personnalisé.

## Paramètres non pris en charge par type de proxy et version TLS

Les champs du journal de décryptage affichent les paramètres de la session de décryptage pour chaque type de proxy de décryptage. Toutefois, pour des raisons telles que la prise en charge des versions, les parties cryptées des communications TLS, la disponibilité des informations, etc., certains paramètres ne sont pas disponibles pour chaque type de proxy ou version TLS. Le tableau suivant présente les paramètres du journal de décryptage non pris en charge par type de proxy et par version TLS.

| Type de proxy | Paramètre non pris en charge | TLS Version (Version TLS) |
|---|---|---|
| Proxy de transfert | Courbe EC négociée | TLSv1.3 |
| Inspection entrante | Identification du nom de serveur<br>Nom commun de la racine | Toutes |
| | Courbe EC négociée | TLSv1.3 |
| Non décryptage (action **No Decrypt (Non décryptage)** dans la règle de politique de décryptage) | Courbe EC négociée<br>Identification du nom de serveur | TLSv1.2 |

| Type de proxy | Paramètre non pris en charge | TLS Version (Version TLS) |
|---|---|---|
| | Courbe EC négociée<br>Identification du nom de serveur<br>Informations sur le certificat (tous les champs d'informations sur le certificat, par exemple, Date de début du certificat, Date de fin du certificat, Type de clé du certificat, etc.) | TLSv1.3 |
| Broker de paquets réseau | Courbe EC négociée | TLSv1.3 |
| Portail GlobalProtect | Identification du nom de serveur<br>Nom commun de la racine<br>Nom de la politique de décryptage<br>App-ID | Toutes |
| Passerelle GlobalProtect | Identification du nom de serveur<br>Nom de la politique de décryptage<br>App-ID | Toutes |
| Clientless SSLVPN | Identification du nom de serveur | Toutes |
| SSH | Journal de décryptage non pris en charge | |
| Texte en clair | Journal de décryptage non pris en charge | |

# Exemples de flux de production de dépannage de décryptage

Le Journal de décryptage et les widgets d'activité SSL dans l'Application Command Center (Centre de commande des applications - ACC) fournissent de puissants outils de dépannage de décryptage qui fonctionnent à la fois indépendamment et ensemble. Lorsque vous aurez compris comment utiliser ces outils, vous pourrez étudier et résoudre un large éventail de problèmes de décryptage.

Les exemples suivants vous montrent comment utiliser les outils de dépannage pour identifier, examiner et résoudre les problèmes de décryptage. Appliquez ces méthodes pour résoudre les problèmes que vous rencontrez dans le déploiement de votre décryptage.

- Enquête sur les raisons de l'échec du décryptage
- Dépannage des suites de chiffrement non prises en charge
- Identification des protocoles et suites de chiffrement faibles
- Identification des certificats CA non approuvés
- Dépannage des certificats expirés

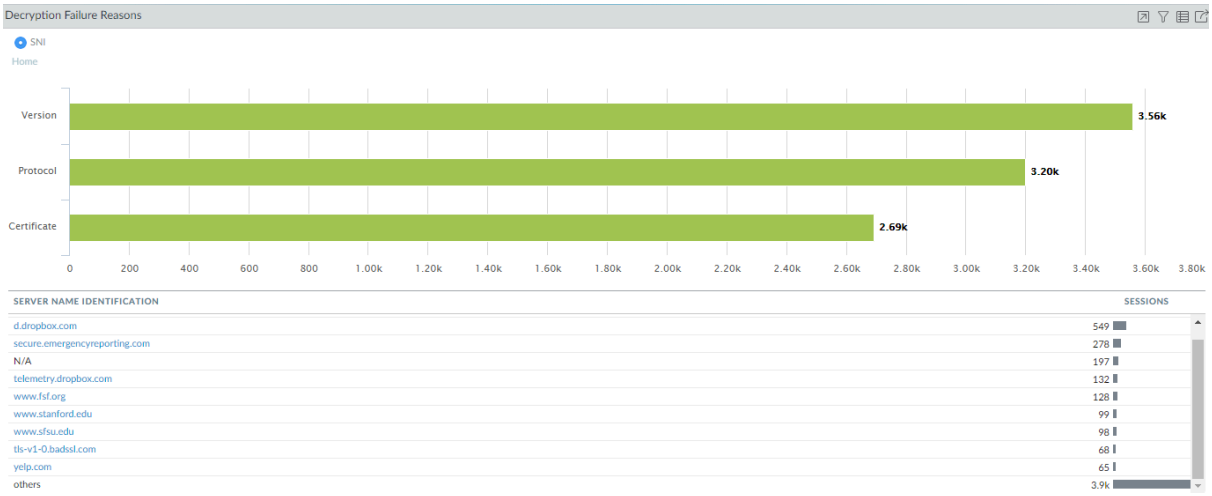
 

- Dépannage des certificats révoqués
- Dépannage des certificats épinglés

## Enquête sur les raisons de l'échec du décryptage

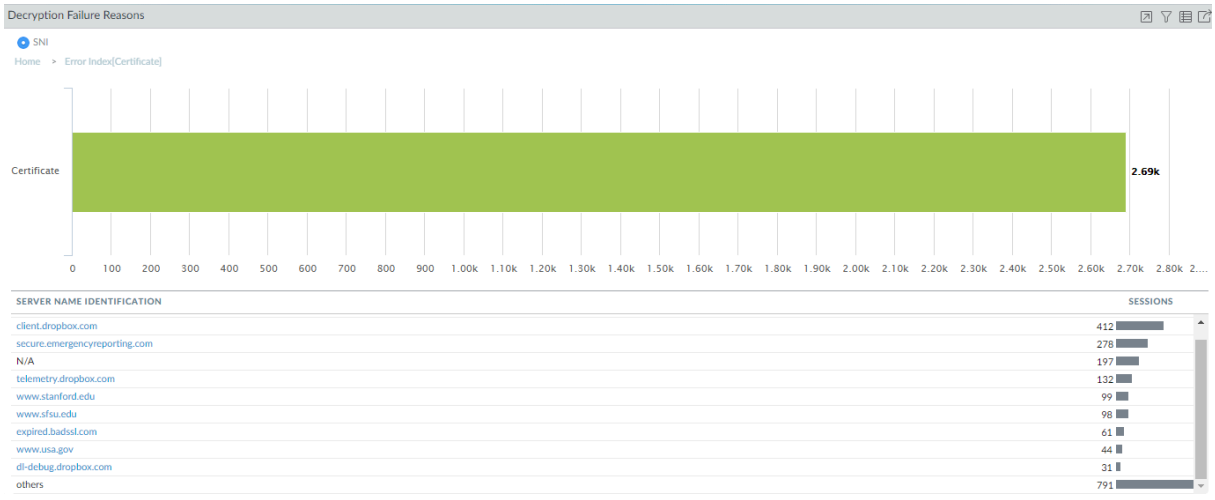
Les raisons les plus courantes des échecs de décryptage sont les erreurs de protocole TLS, les erreurs de version de chiffrement (non-concordance des versions du client et du serveur, et aussi non-concordance des versions du profil de décryptage et du client), et les erreurs de certificat. Pour enquêter sur les erreurs de décryptage, commencez par l'Application Command Center (Centre de commande des applications - ACC) pour identifier les défaillances, puis allez dans les journaux de décryptage pour approfondir les détails.

**STEP 1 |** Commencez votre enquête sur **ACC** > **SSL Activity (Activité SSL)** et observez le widget Raisons de l'échec du décryptage.




Dans cet exemple, nous enquêtons sur les erreurs de certificat. Vous pouvez utiliser le même processus pour enquêter sur les erreurs de version et de protocole.

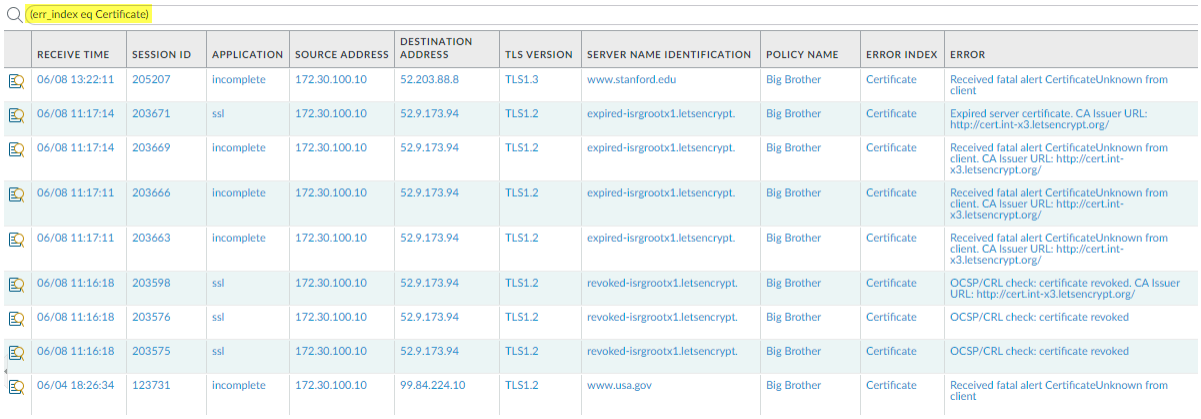
**STEP 2 |** Cliquez sur la barre verte à côté de **Certificate (Certificat)** pour voir quels hôtes (SNI) ont subi des erreurs de certificat et voir une liste des hôtes qui ont subi le plus grand nombre d'erreurs de certificat.



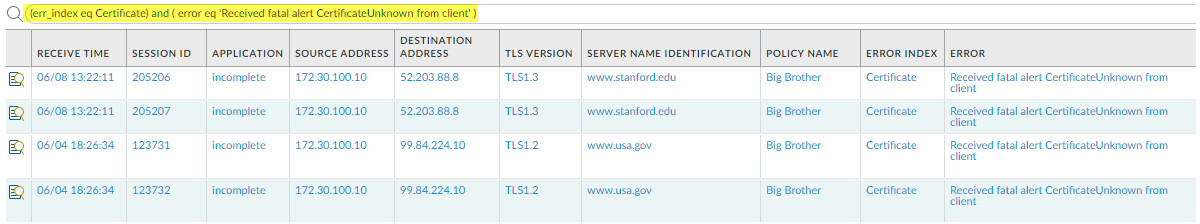
**STEP 3 |** Accédez à **Monitor (Moniteur)** > **Logs (Journaux)** > **Decryption (Décryptage)** pour examiner les journaux de bord.

Utilisez la requête **(err_index eq Certificate)** pour filtrer les journaux de décryptage afin de visualiser toutes les sessions de décryptage qui ont connu des erreurs de certificat.


(err_index eq Certificate)

| RECEIVE TIME | SESSION ID | APPLICATION | SOURCE ADDRESS | DESTINATION ADDRESS | TLS VERSION | SERVER NAME IDENTIFICATION | POLICY NAME | ERROR INDEX | ERROR |
|---|---|---|---|---|---|---|---|---|---|
| 06/08 13:22:11 | 205207 | incomplete | 172.30.100.10 | 52.203.88.8 | TLS1.3 | www.stanford.edu | Big Brother | Certificate | Received fatal alert CertificateUnknown from client |
| 06/08 11:17:14 | 203671 | ssl | 172.30.100.10 | 52.9.173.94 | TLS1.2 | expired-isrgrootx1.letsencrypt. | Big Brother | Certificate | Expired server certificate. CA Issuer URL: http://cert.int-x3.letsencrypt.org/ |
| 06/08 11:17:14 | 203669 | incomplete | 172.30.100.10 | 52.9.173.94 | TLS1.2 | expired-isrgrootx1.letsencrypt. | Big Brother | Certificate | Received fatal alert CertificateUnknown from client. CA Issuer URL: http://cert.int-x3.letsencrypt.org/ |
| 06/08 11:17:11 | 203666 | incomplete | 172.30.100.10 | 52.9.173.94 | TLS1.2 | expired-isrgrootx1.letsencrypt. | Big Brother | Certificate | Received fatal alert CertificateUnknown from client. CA Issuer URL: http://cert.int-x3.letsencrypt.org/ |
| 06/08 11:17:11 | 203663 | incomplete | 172.30.100.10 | 52.9.173.94 | TLS1.2 | expired-isrgrootx1.letsencrypt. | Big Brother | Certificate | Received fatal alert CertificateUnknown from client. CA Issuer URL: http://cert.int-x3.letsencrypt.org/ |
| 06/08 11:16:18 | 203598 | ssl | 172.30.100.10 | 52.9.173.94 | TLS1.2 | revoked-isrgrootx1.letsencrypt. | Big Brother | Certificate | OCSP/CRL check: certificate revoked. CA Issuer URL: http://cert.int-x3.letsencrypt.org/ |
| 06/08 11:16:18 | 203576 | ssl | 172.30.100.10 | 52.9.173.94 | TLS1.2 | revoked-isrgrootx1.letsencrypt. | Big Brother | Certificate | OCSP/CRL check: certificate revoked |
| 06/08 11:16:18 | 203575 | ssl | 172.30.100.10 | 52.9.173.94 | TLS1.2 | revoked-isrgrootx1.letsencrypt. | Big Brother | Certificate | OCSP/CRL check: certificate revoked |
| 06/04 18:26:34 | 123731 | incomplete | 172.30.100.10 | 99.84.224.10 | TLS1.2 | www.usa.gov | Big Brother | Certificate | Received fatal alert CertificateUnknown from client |

La colonne **Error (Erreur)** indique la raison de l'erreur de certificat. Pour filtrer toutes les sessions de décryptage qui présentent la même erreur, cliquez sur le message d'erreur pour l'ajouter à la requête, puis exécutez la requête. Par exemple, pour trouver toutes les erreurs basées sur la réception d'une alerte fatale du client, le fait de cliquer sur l'erreur produit la requête **(err_index eq Certificate) et (error eq 'Received fatal alert CertificateUnknown from client')**:

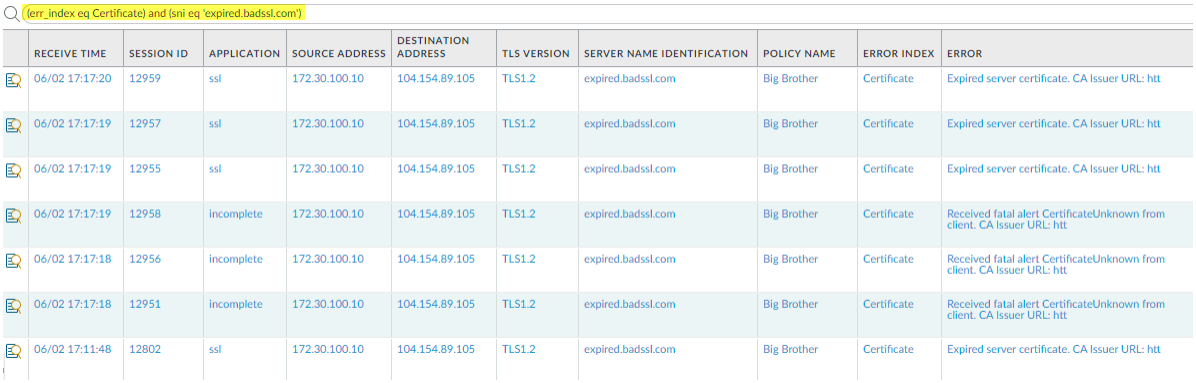

(err_index eq Certificate) and ( error eq 'Received fatal alert CertificateUnknown from client' )

| RECEIVE TIME | SESSION ID | APPLICATION | SOURCE ADDRESS | DESTINATION ADDRESS | TLS VERSION | SERVER NAME IDENTIFICATION | POLICY NAME | ERROR INDEX | ERROR |
|---|---|---|---|---|---|---|---|---|---|
| 06/08 13:22:11 | 205206 | incomplete | 172.30.100.10 | 52.203.88.8 | TLS1.3 | www.stanford.edu | Big Brother | Certificate | Received fatal alert CertificateUnknown from client |
| 06/08 13:22:11 | 205207 | incomplete | 172.30.100.10 | 52.203.88.8 | TLS1.3 | www.stanford.edu | Big Brother | Certificate | Received fatal alert CertificateUnknown from client |
| 06/04 18:26:34 | 123731 | incomplete | 172.30.100.10 | 99.84.224.10 | TLS1.2 | www.usa.gov | Big Brother | Certificate | Received fatal alert CertificateUnknown from client |
| 06/04 18:26:34 | 123732 | incomplete | 172.30.100.10 | 99.84.224.10 | TLS1.2 | www.usa.gov | Big Brother | Certificate | Received fatal alert CertificateUnknown from client |

Pour filtrer les erreurs de certificat qu'un hôte spécifique a reçues, ajoutez ce SNI à la requête au lieu d'ajouter un texte de message d'erreur. Par exemple, pour trouver toutes les erreurs de

certificat pour expired.badssl.comm, utilisez la requête **(err_index eq Certificate) et (sni eq 'expired.badssl.com')** :




| RECEIVE TIME | SESSION ID | APPLICATION | SOURCE ADDRESS | DESTINATION ADDRESS | TLS VERSION | SERVER NAME IDENTIFICATION | POLICY NAME | ERROR INDEX | ERROR |
|---|---|---|---|---|---|---|---|---|---|
| 06/02 17:17:20 | 12959 | ssl | 172.30.100.10 | 104.154.89.105 | TLS1.2 | expired.badssl.com | Big Brother | Certificate | Expired server certificate. CA Issuer URL: htt |
| 06/02 17:17:19 | 12957 | ssl | 172.30.100.10 | 104.154.89.105 | TLS1.2 | expired.badssl.com | Big Brother | Certificate | Expired server certificate. CA Issuer URL: htt |
| 06/02 17:17:19 | 12955 | ssl | 172.30.100.10 | 104.154.89.105 | TLS1.2 | expired.badssl.com | Big Brother | Certificate | Expired server certificate. CA Issuer URL: htt |
| 06/02 17:17:19 | 12958 | incomplete | 172.30.100.10 | 104.154.89.105 | TLS1.2 | expired.badssl.com | Big Brother | Certificate | Received fatal alert CertificateUnknown from client. CA Issuer URL: htt |
| 06/02 17:17:18 | 12956 | incomplete | 172.30.100.10 | 104.154.89.105 | TLS1.2 | expired.badssl.com | Big Brother | Certificate | Received fatal alert CertificateUnknown from client. CA Issuer URL: htt |
| 06/02 17:17:18 | 12951 | incomplete | 172.30.100.10 | 104.154.89.105 | TLS1.2 | expired.badssl.com | Big Brother | Certificate | Received fatal alert CertificateUnknown from client. CA Issuer URL: htt |
| 06/02 17:11:48 | 12802 | ssl | 172.30.100.10 | 104.154.89.105 | TLS1.2 | expired.badssl.com | Big Brother | Certificate | Expired server certificate. CA Issuer URL: htt |

La colonne **Error (Erreur)** indique la raison spécifique de chaque erreur de certificat associée à expired.badssl.com.

Une fois que vous connaissez la raison de l'émission du certificat qui a causé l'échec du décryptage, vous pouvez y remédier. Par exemple, si la chaîne de certificats est incomplète, vous pouvez réparer la chaîne de certificat incomplète. Si un certificat est expiré, vous pouvez en informer l'administrateur du site ou créer une exception basée sur la politique si vous avez besoin d'accéder au site.

## Dépannage des suites de chiffrement non prises en charge

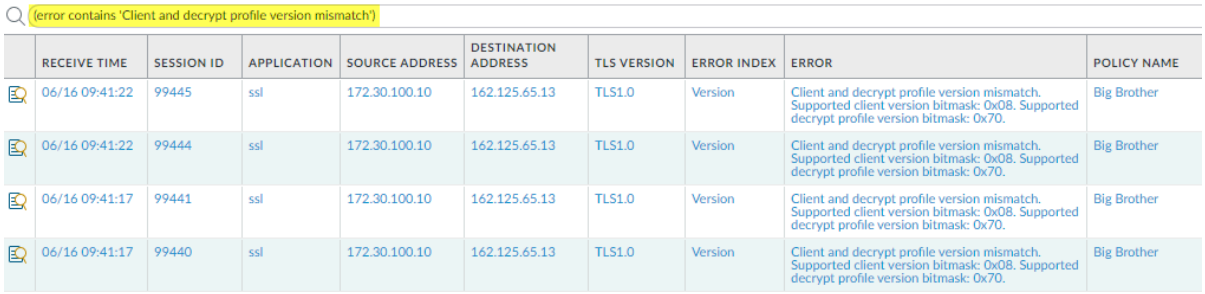
L'identification et le dépannage des suites de chiffrement non prises en charge dans le journal de décryptage est un aspect de l'investigation des erreurs de version qui mérite d'être examiné seul.

**STEP 1 |** Dans le journal de décryptage (**Monitor (Moniteur)** > **Logs (Journaux)** > **Decryption (Décryptage)**), utilisez la requête **(error contains 'Client and decrypt profile**

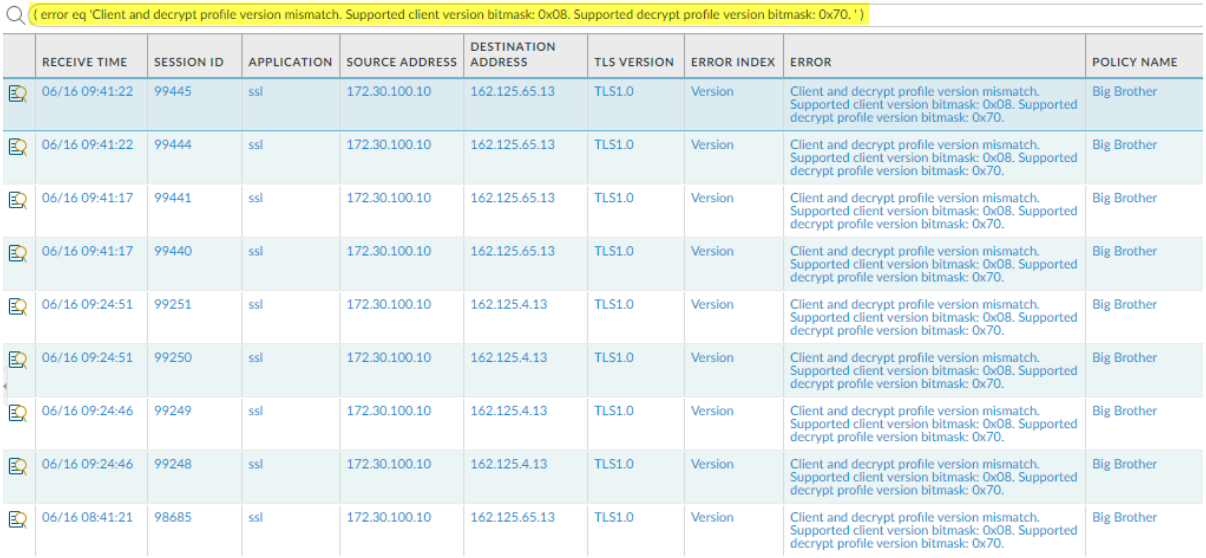
**`mismatch')`** pour identifier toutes les incompatibilités entre les versions de la suite de chiffrement.

Le filtrage des journaux pour ces incompatibilités permet de trouver tous les cas où le client et le profil de décryptage pris en charge par la suite de chiffrement ne correspondent pas.


(error contains 'Client and decrypt profile version mismatch')

| RECEIVE TIME | SESSION ID | APPLICATION | SOURCE ADDRESS | DESTINATION ADDRESS | TLS VERSION | ERROR INDEX | ERROR | POLICY NAME |
|---|---|---|---|---|---|---|---|---|
| 06/16 09:41:22 | 99445 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:41:22 | 99444 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:41:17 | 99441 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:41:17 | 99440 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |

Pour trouver toutes les sessions de décryptage qui ont connu la même erreur, cliquez sur le message d'erreur pour l'ajouter à la requête et supprimer la requête originale, par exemple :


( error eq 'Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. ' )

| RECEIVE TIME | SESSION ID | APPLICATION | SOURCE ADDRESS | DESTINATION ADDRESS | TLS VERSION | ERROR INDEX | ERROR | POLICY NAME |
|---|---|---|---|---|---|---|---|---|
| 06/16 09:41:22 | 99445 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:41:22 | 99444 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:41:17 | 99441 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:41:17 | 99440 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:24:51 | 99251 | ssl | 172.30.100.10 | 162.125.4.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:24:51 | 99250 | ssl | 172.30.100.10 | 162.125.4.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:24:46 | 99249 | ssl | 172.30.100.10 | 162.125.4.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 09:24:46 | 99248 | ssl | 172.30.100.10 | 162.125.4.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |
| 06/16 08:41:21 | 98685 | ssl | 172.30.100.10 | 162.125.65.13 | TLS1.0 | Version | Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70. | Big Brother |

Les codes hexadécimaux identifient la version exacte que le client prend en charge et la version exacte que le profil de décryptage prend en charge.

**STEP 2 |** Connectez-vous à la CLI et recherchez les valeurs du masque.

Les erreurs montrent une incompatibilité entre le client et le profil de décryptage. Le masque de bit client pris en charge est 0x08 et le masque de bit du profil de décryptage pris en charge est 0x70 :

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x08
```

```
TLSv1.0
```

Cette sortie montre que le client ne prend en charge que TLSv1.0.

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x70
```

```
TLSv1.1
```

```
TSLv1.2
```

```
TLSv1.3
```

Cette sortie montre que le profil de décryptage prend en charge TLSv1.1, TLSv1.2 et TLSv1.3, mais pas TLSv1.0. Maintenant vous savez que le client ne supporte qu'une ancienne version du protocole TLS et que le profil de décryptage attaché à la règle de politique de décryptage qui contrôle le trafic n'autorise pas cette versions.

**STEP 3 |** Décidez des mesures à prendre.

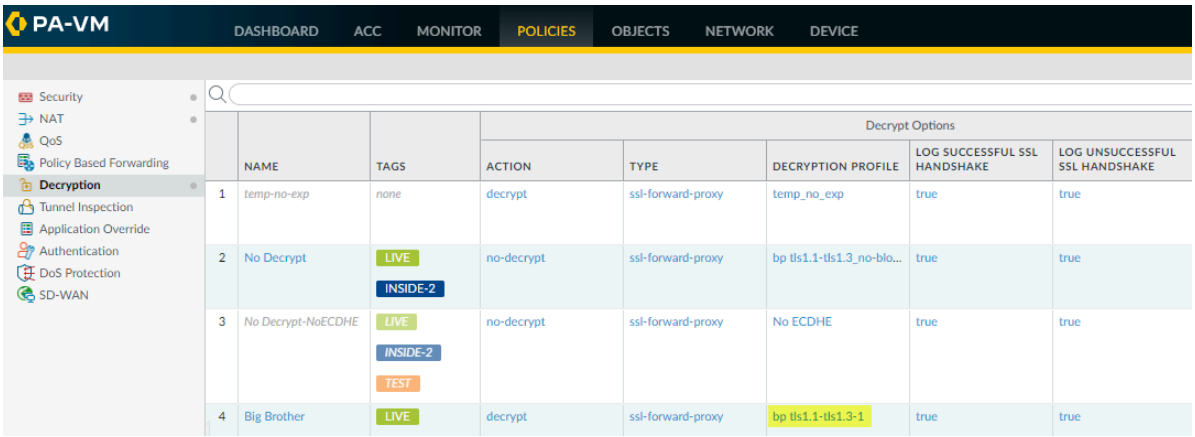
Vous pourriez mettre à jour le client afin qu'il accepte une version TLS plus sûre. Si le client a besoin de TLSv1.0 pour une raison quelconque, vous pouvez continuer à laisser le pare-feu bloquer le trafic, ou vous pouvez mettre à jour le profil de décryptage pour autoriser tout le trafic TLSv1.0 (non recommandé), ou vous pouvez créer une politique et un profil de décryptage qui autorisent TLSv1.0 et l'appliquer uniquement aux périphériques clients qui doivent utiliser TLSv1.0 et ne peuvent pas supporter un protocole plus sûr (option la plus sûre pour autoriser le trafic).

**STEP 4 |** Si vous choisissez de modifier le profil de décryptage, pour trouver la politique de décryptage qui contrôle le trafic de la session, consultez la colonne **Policy Name (Nom de la politique)**

dans le journal (ou cliquez sur l'icône de la loupe à côté du journal de décryptage pour voir les informations dans la section générale de la vue détaillée du journal).

1. Dans cet exemple, le nom du profil de décryptage est Big Brother ; pour trouver le profil de décryptage, accédez à **Policies (Politiques)** > **Decryption (Décryptage)** et vérifiez la colonne **Decryption Profile (Profil de décryptage)**.



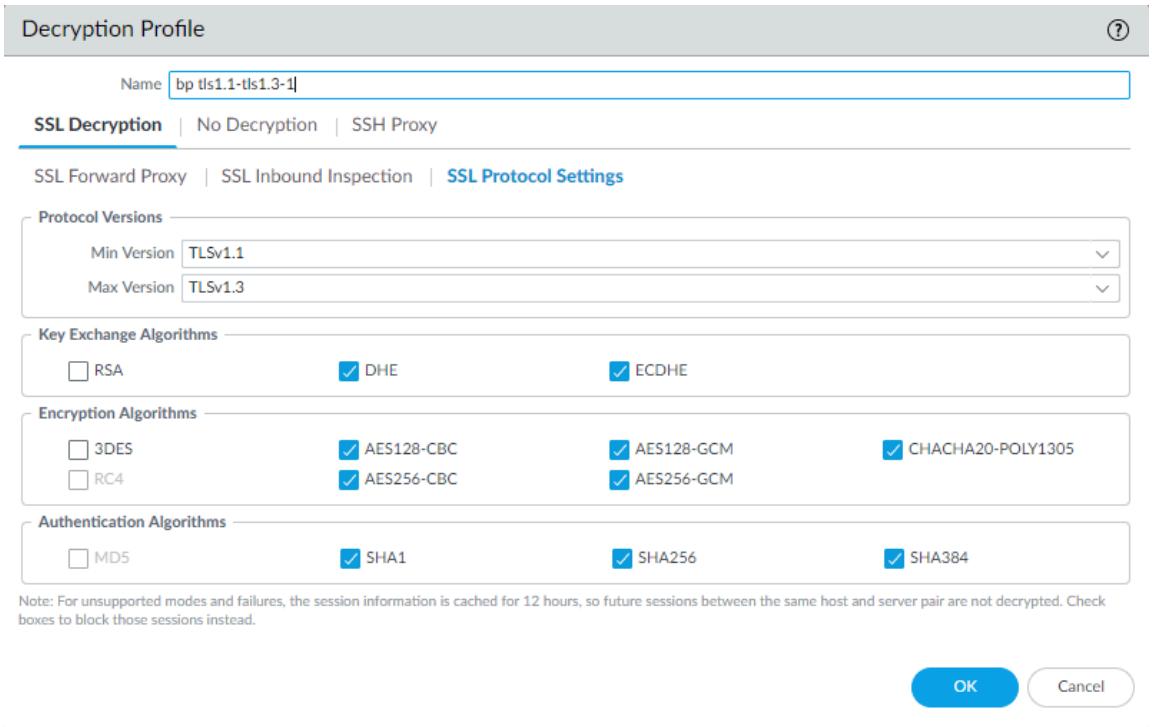

   Le nom du profil de décryptage est **bp tls1.1-tls1.3-1**. Vous pouvez aussi sélectionner la politique Big Brother puis sélectionner l'onglet **Options** pour voir le nom du profil de décryptage.

   Accédez à **Objects (Objets)** > **Decryption (Décryptage)** > **Decryption Profile (Profil de décryptage)**, sélectionnez le profil de décryptage approprié, et modifiez-le pour résoudre le problème de la version.

2. Accédez à **Objects (Objets)** > **Decryption (Décryptage)** > **Decryption Profile (Profil de décryptage)**.

   Sélectionnez le profil de décryptage **bp tls1.1-tls1.3-1** et cliquez sur l'onglet **SSL Protocol Settings (Paramètres du protocole SSL)**.




La version minimum du protocole TLS (**Min Version**) que le profil prend en charge est TLSv1.1. Pour autoriser le trafic qui est bloqué par l'incompatibilité de version, vous pourriez modifier la **Min Version (Version min)** en TLSv1.0. Toutefois, une option plus sûre consiste à mettre à jour le client pour qu'il utilise une version récente du protocole TLS. Si vous ne pouvez pas mettre à jour le client, vous pouvez créer une politique et un profil de décryptage qui s'appliquent uniquement à cet utilisateur, ce périphérique ou cette adresse source (et à tous les utilisateurs, périphériques ou adresses sources similaires de sorte qu'une seule politique et un seul profil contrôlent tout ce trafic) au lieu d'appliquer une politique de décryptage générale qui autorise le trafic TLSv1.0.

## Identification des protocoles et suites de chiffrement faibles

Les protocoles TLS faibles et les suites de chiffrement faibles (algorithmes de chiffrement, algorithmes d'authentification, algorithmes d'échange de clés et courbes EC négociées) affaiblissent votre posture de sécurité et sont plus faciles à exploiter pour les mauvais acteurs que les protocoles TLS forts et les suites de chiffrement fortes.

Cinq champs dans les entrées du journal de décryptage indiquent les suites de protocole et de chiffrement pour une session de décryptage :

| TLS VERSION | ENCRYPTION ALGORITHM | KEY EXCHANGE | AUTHENTICATI... ALGORITHM | NEGOTIATED EC CURVE |
|---|---|---|---|---|
| TLS1.2 | AES_128_GCM | ECDHE | SHA256 | secp256r1 |
| TLS1.2 | AES_256_GCM | ECDHE | SHA384 | secp256r1 |

Retrouvez les anciennes versions et suites de chiffrement TLS vulnérables afin que vous puissiez prendre des décisions éclairées sur l'autorisation ou non de connexions avec des serveurs et des applications susceptibles de compromettre votre posture de sécurité.

Les exemples présentés dans cette rubrique montrent comment :

- Identifier le trafic qui utilise des versions moins sûres du protocole TLS.
- Identifier le trafic qui utilise un algorithme d'échange de clés particulier.
- Identifier le trafic qui utilise un algorithme d'authentification particulier.
- Identifier le trafic qui utilise un algorithme de cryptage particulier.

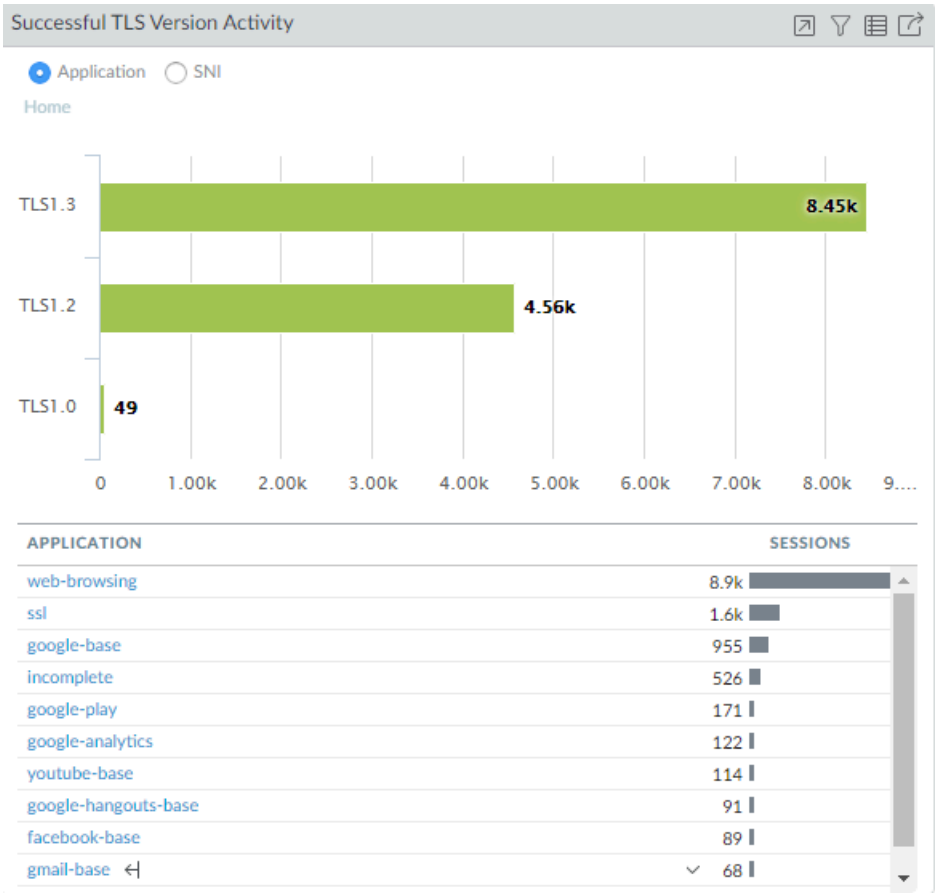
Ces exemples vous montrent comment utiliser les outils de dépannage de décryptage de différentes manières afin que vous puissiez apprendre à les utiliser pour résoudre les problèmes de décryptage que vous pourriez rencontrer.

***Vous pouvez utiliser Wireshark ou d'autres analyseurs de paquets pour vérifier si le client ou le serveur a causé un problème, les versions du client et du serveur TLS, et d'autres informations sur la suite de chiffrement. Cela peut aider à analyser les décalages entre les versions et d'autres problèmes.***

- **TLS Protocols (Protocoles TLS)** : identifiez le trafic qui utilise des versions plus anciennes et moins sûres du protocole TLS afin que vous puissiez évaluer s'il faut autoriser l'accès aux serveurs et aux applications qui utilisent des protocoles faibles.
    1. Commencez par vérifier l'Application Command Center (Centre de commande des applications - ACC) pour voir si le pare-feu autorise les protocoles faibles (**ACC** > **SSL**

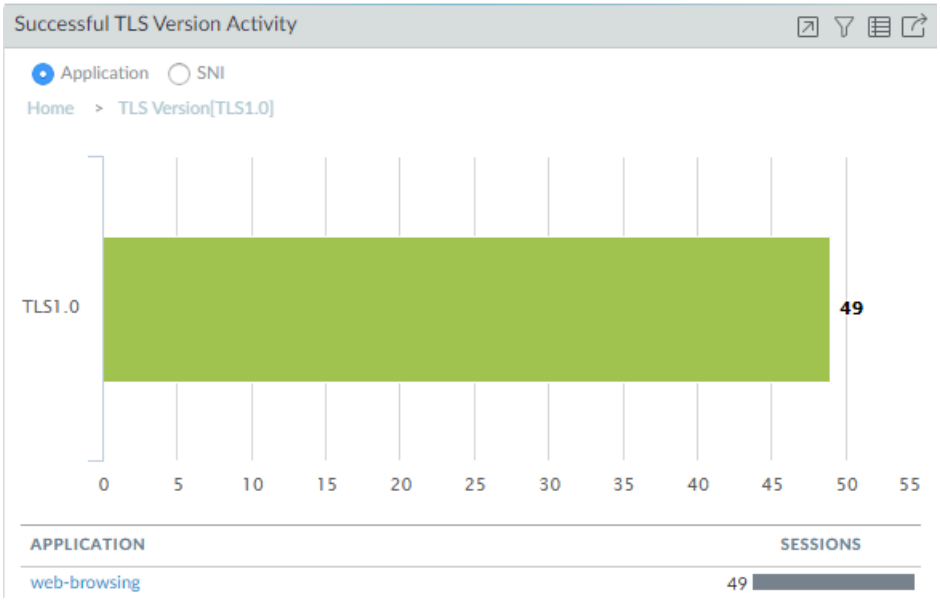
**Activity (Activité SSL)** > **Successful TLS Version Activity (Activité de version TLS réussie)**) et pour avoir une vue d'ensemble de l'activité.




La majorité des activités TLS réussies dans cet exemple sont des activités TLSv1.2 et TLSv1.3. Toutefois, il existe quelques cas de trafic TLSv1.0 autorisé. Cliquons sur le

numéro **49** pour approfondir l'activité TLSv1.0 et voir quelles applications établissent des connexions TLSv1.0 réussies :

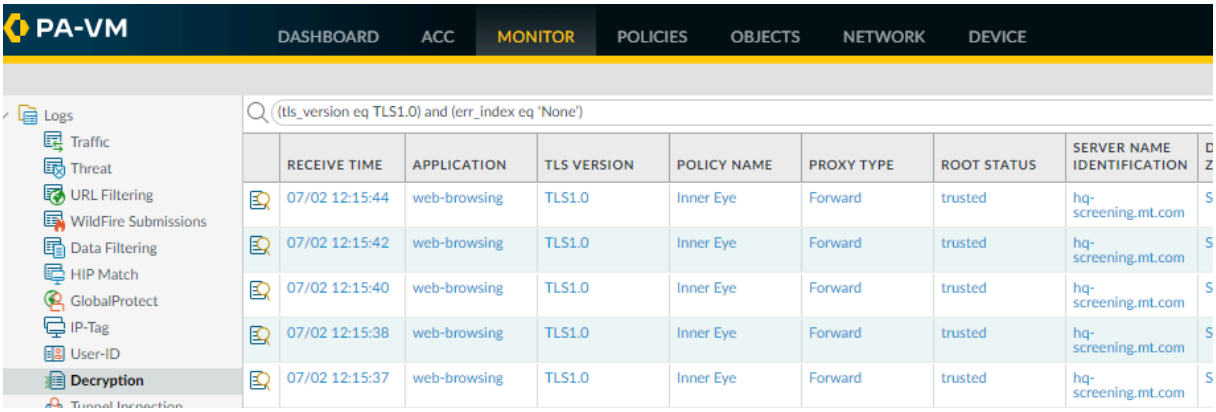



Nous voyons que le pare-feu autorise un trafic identifié comme du trafic de navigation sur le web. Pour mieux comprendre ce qu'est ce trafic de navigation sur le web TLSv1.0 et pourquoi il est autorisé, passons ensuite aux journaux de décryptage.

2. Filtrez le journal de décryptage pour vérifier les détails de l'activité TLSv1.0.

   Utilisez la requête **`(tls_version eq TLS1.0) et (err_index eq 'None')`** pour montrer des sessions de décryptage TLSv1.0 réussies.

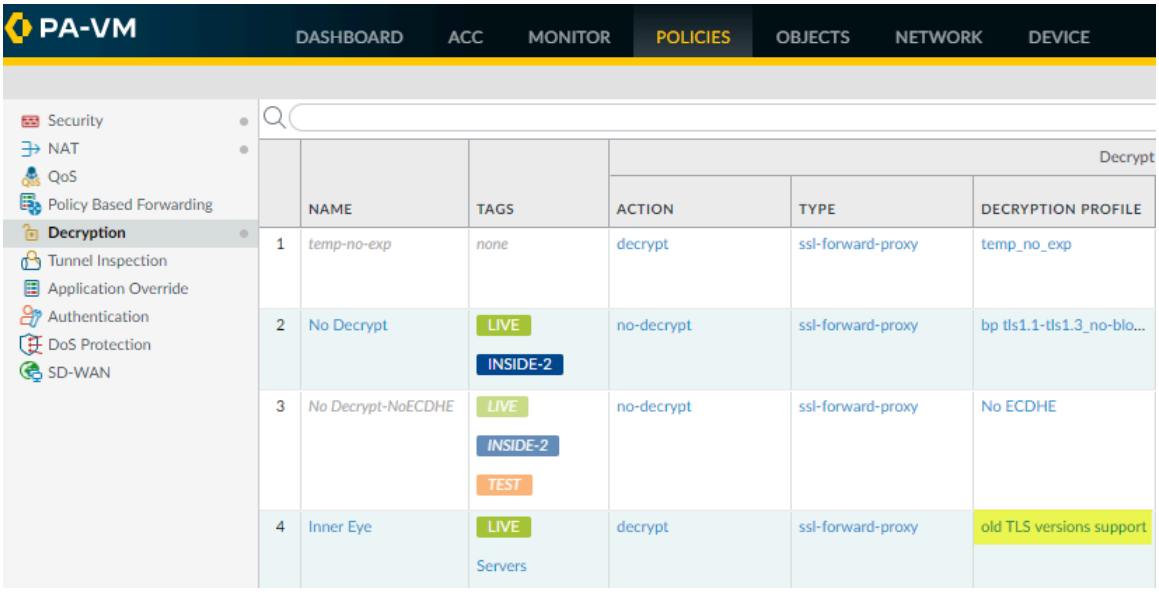
   *Les journaux de décryptage n'indiquent une activité TLS réussie que si vous activez la journalisation des communications TLS réussies dans la politique de décryptage lorsque vous Configuration de la journalisation de décryptage. Si l'enregistrement des communications TLS réussies est désactivé, vous ne pouvez pas vérifier cette information.*




Le journal de décryptage nous montre que le nom de la politique de décryptage qui contrôle le trafic est **Inner Eye** et que le nom de l'hôte est **hq-screening.mt.com**. Nous connaissons maintenant le site qui utilise TLSv1.0 et nous pouvons vérifier la politique

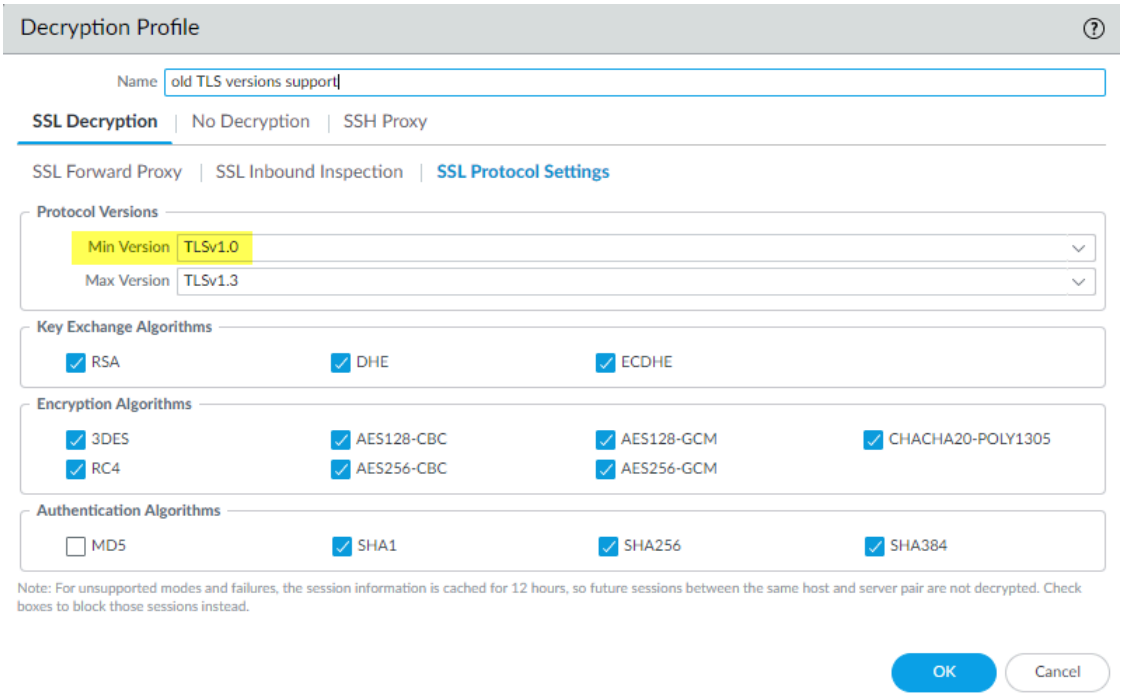
de décryptage (**Policies (Politiques)** > **Decryption (Décryptage)**) pour trouver le profil de décryptage qui contrôle le trafic et savoir pourquoi le trafic est autorisé :




Nous voyons que le profil de décryptage associé à la politique est **old TLS versions support (prise en charge d'anciennes versions TLS)**. Nous contrôlons le profil (**Objects (Objets)** > **Decryption (Décryptage)** > **Decryption Profile (Profil de décryptage)**) et

consultons les paramètres du protocole SSL pour savoir exactement quel trafic le profil permet :




Le profil permet le trafic TLSv1.0. La prochaine chose à faire est de décider si vous voulez autoriser l'accès au site (avez-vous besoin d'un accès à des fins professionnelles ?) ou si vous voulez le bloquer.

Un autre scénario courant qui fait que le pare-feu autorise un trafic utilisant des protocoles moins sûrs est celui où ce trafic n'est pas décrypté. Lorsque vous filtrez le journal de décryptage pour le trafic TLSv1.0, si la colonne **Proxy Type (Type de proxy)** contient la valeur **No Decrypt (Non décryptage)**, cela signifie qu'une politique de non décryptage contrôle le trafic, de sorte que le pare-feu ne le décrypte pas et ne l'inspecte pas. Si vous

ne voulez pas autoriser le protocole faible, modifiez le profil de décryptage afin qu'il bloque le trafic TLSv1.0.

Il existe de nombreuses façons de filtrer le journal de décryptage pour trouver les applications et les sites qui utilisent des protocoles faibles, par exemple :

- Au lieu de filtrer uniquement les communications TLSv1.0 réussies, filtrez les communications TLSv1.0 réussies et avortées à l'aide de la requête **`(tls_version eq TLS1.0).`**
- Filtrez uniquement les communications TLSv1.0 avortées à l'aide de la requête **`(tls_version eq TLS1.0) et (err_index neq 'None')`**.
- Filtrez tous les protocoles moins sûrs (TLSv1.1 et antérieurs) à l'aide de la requête **`(tls_version leq tls1.1)`**.

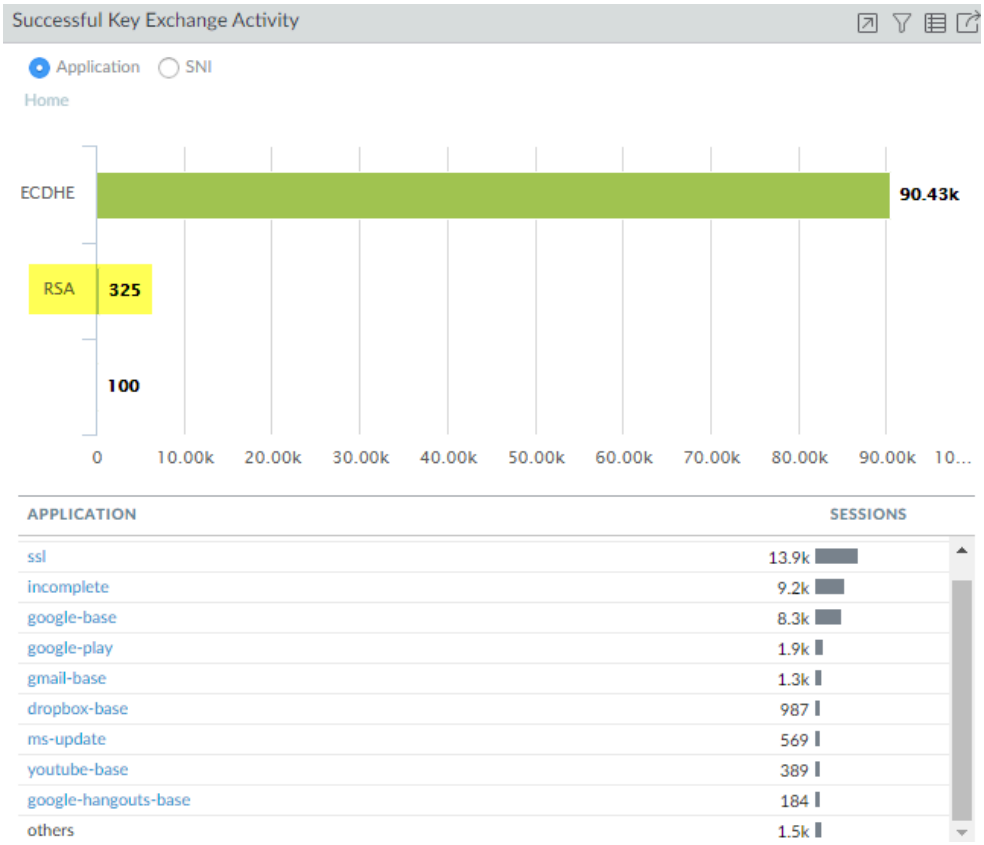
Si vous souhaitez filtrer les journaux pour d'autres versions de TLS, il suffit de remplacer **`TLS1.0`** ou **`TLS1.1`** par une autre version TLS.

3. Décider des mesures à prendre pour les sites qui utilisent des protocoles TLS faibles.
   - Si vous n'avez pas besoin d'accéder au site à des fins professionnelles, la mesure la plus sûre consiste à bloquer l'accès au site en modifiant la politique de décryptage et le profil de décryptage qui contrôlent le trafic. La colonne **Policy Name (Nom de la politique)** du journal de décryptage fournit le nom de la politique et la politique de décryptage indique le profil de décryptage joint (onglet **Options**).
   - Si vous devez accéder au site à des fins professionnelles, envisagez de créer une politique de décryptage et un profil de décryptage qui s'appliquent uniquement à ce site (ou à ce site et à d'autres sites similaires) et bloquez tout autre trafic qui utilise des protocoles moins sûrs.

- **Key Exchange (Échange de clés)** : identifiez le trafic qui utilise des algorithmes d'échange de clés moins sûrs.
  1. Commencez par vérifier l'Application Command Center (Centre de commande des applications - ACC) pour voir quels sont les algorithmes d'échange de clés autorisés par le

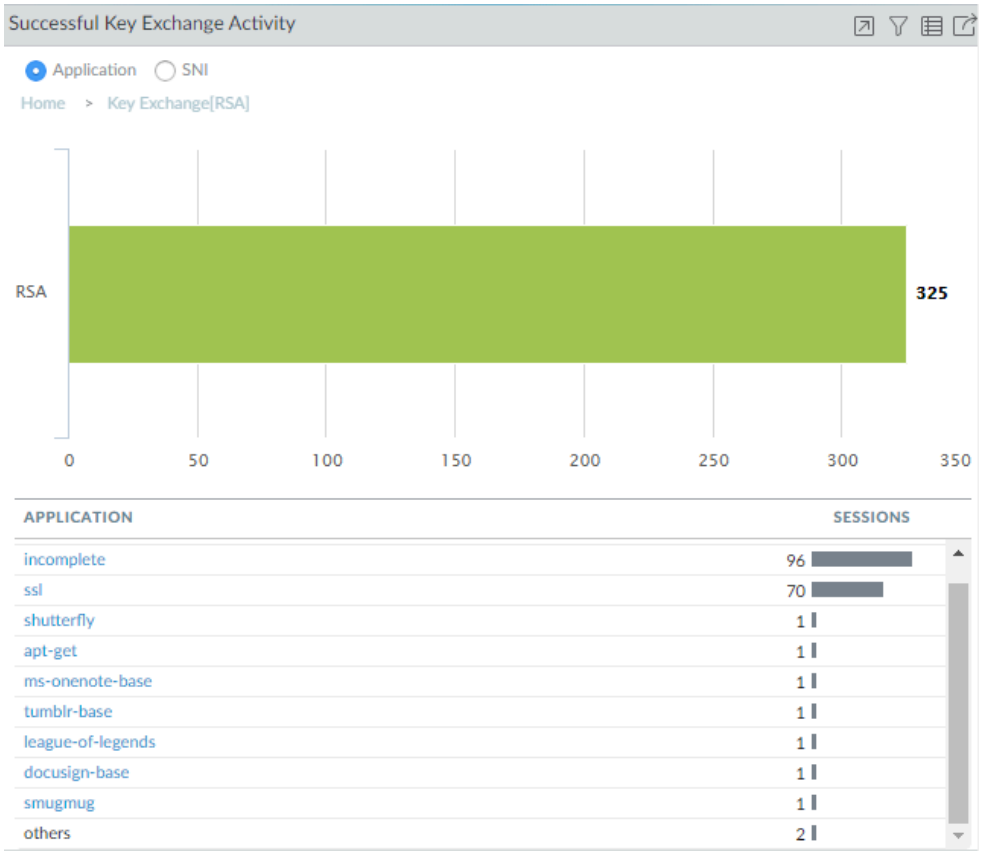
pare-feu (**ACC** > **SSL Activity (Activité SSL)** > **Successful Key Exchange Activity (Activité d'échange de clés réussie)**) et pour avoir une vue d'ensemble de l'activité.




La majorité des échanges de clés utilisent l'algorithme sécurisé d'échange de clés ECDHE. Cependant, certaines sessions d'échange de clés utilisent l'algorithme RSA, moins sûr, et quelques-unes utilisent un autre algorithme de clé. Pour commencer à enquêter sur le

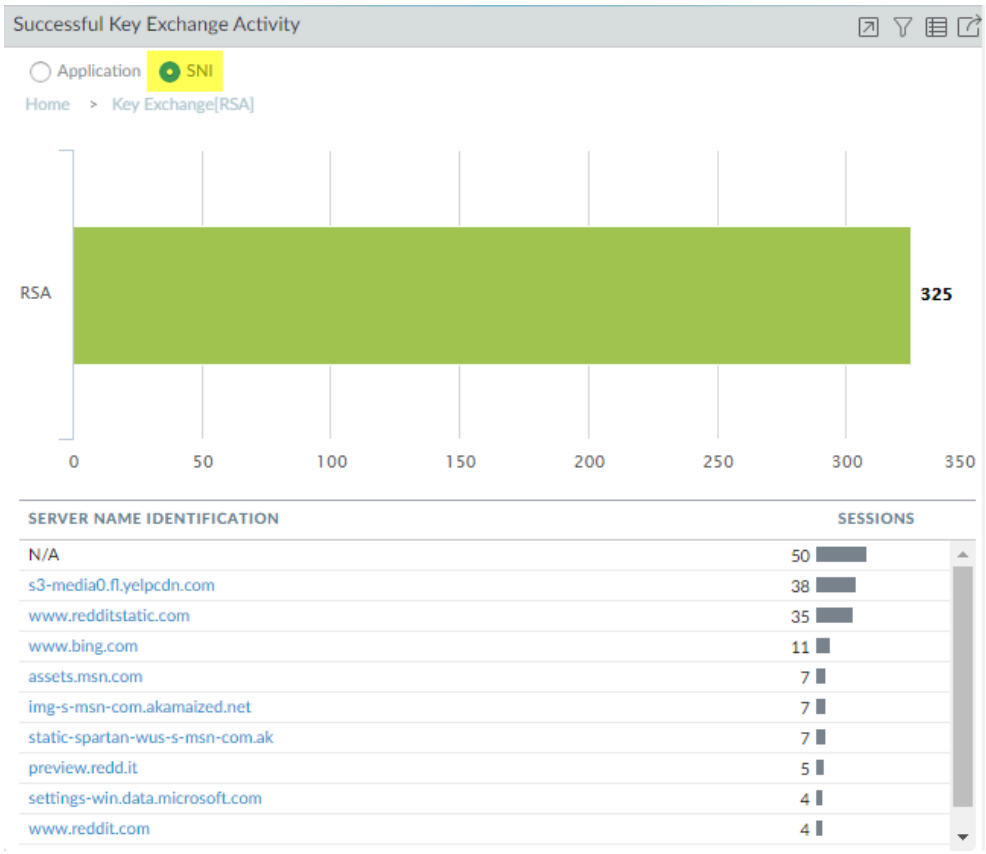
 

trafic qui utilise les échanges de clés RSA, par exemple, cliquez sur le chiffre **325** pour approfondir les données.




L'analyse descendante montre les applications qui utilisent les échanges de clés RSA. Nous pouvons également cliquer sur le bouton radio **SNI** pour voir les échanges de clés RSA par SNI :




Grâce à ces informations, nous pouvons consulter les journaux pour mieux comprendre l'utilisation des échanges de clés RSA.

2. Accédez au journal de décryptage (**Monitor (Moniteur)** > **Logs (Journaux)** > **Decryption (Décryptage)**) et filtrez-les par sessions de décryptage qui utilisent l'échange de clés RSA en utilisant la requête **`(tls_keyxchg eq RSA)`**:

(tls_keyxchg eq RSA)

| | RECEIVE TIME | SESSION ID | APPLICATION | SOURCE ADDRESS | DESTINATION ADDRESS | TLS VERSION | ERROR INDEX | ERROR | POLICY NAME |
|---|---|---|---|---|---|---|---|---|---|
| | 06/04 09:29:50 | 92884 | ssl | 172.30.200.30 | 185.31.128.129 | TLS1.2 | None | | No Decrypt |
| | 06/04 09:29:50 | 92887 | ssl | 172.30.200.30 | 185.31.128.129 | TLS1.2 | None | | No Decrypt |
| | 06/04 09:29:44 | 92998 | ssl | 172.30.200.30 | 74.120.19.22 | TLS1.2 | None | | No Decrypt |
| | 06/04 09:29:24 | 92882 | ssl | 172.30.200.30 | 192.132.33.46 | TLS1.2 | Certificate | Expired server certificate | No Decrypt |
| | 06/04 09:29:24 | 92880 | ssl | 172.30.200.30 | 192.132.33.46 | TLS1.2 | Certificate | Expired server certificate | No Decrypt |
| | 06/04 09:29:23 | 92874 | ssl | 172.30.200.30 | 192.132.33.46 | TLS1.2 | Certificate | Expired server certificate | No Decrypt |
| | 06/04 09:29:23 | 92873 | ssl | 172.30.200.30 | 192.132.33.46 | TLS1.2 | Certificate | Expired server certificate | No Decrypt |
| | 06/03 22:30:11 | 36522 | vudu | 172.30.100.155 | 208.79.221.210 | TLS1.2 | None | | Big Brother |
| | 06/03 20:08:57 | 16896 | ssl | 172.30.200.30 | 66.117.28.86 | TLS1.2 | None | | No Decrypt |
| | 06/03 20:08:22 | 16947 | ssl | 172.30.200.30 | 185.31.128.129 | TLS1.2 | None | | No Decrypt |

Dans la colonne **Policy Name (Nom de politique)** du journal, nous voyons que la politique de décryptage **No Decrypt (Non décryptage)** contrôle la majeure partie du trafic qui utilise

les échanges de clés RSA et peut en déduire que le pare-feu ne décrypte pas le trafic et l'autorise sans inspection. Comme le trafic n'est pas décrypté, le pare-feu ne peut pas identifier l'application et la répertorie comme **ssl**. Si vous ne voulez pas autoriser le trafic qui utilise les échanges de clés RSA, modifiez le profil de décryptage joint à la politique de décryptage qui contrôle le trafic.

Vous pouvez ajouter à la requête pour filtrer davantage les résultats pour un SNI ou une application particulière que vous avez vu dans l'ACC ou dans la première requête de journal de décryptage.

3. Décidez des mesures à prendre pour le trafic qui utilise des algorithmes d'échange de clés moins sûrs.

   Bloquez l'accès aux sites qui utilisent des protocoles d'échange de clés moins sûrs, sauf si vous devez y accéder pour des raisons professionnelles. Pour ces sites, envisagez de créer une politique de décryptage et un profil de décryptage qui s'appliquent uniquement à ce site (ou à ce site et à d'autres sites similaires) et bloquez tout autre trafic qui utilise des algorithmes d'échange de clés moins sûrs.

- Utilisez les journaux de décryptage pour identifier les sessions qui utilisent des algorithmes d'authentification plus anciens et moins sûrs.

  Filtrez le journal de décryptage pour identifier les algorithmes d'authentification plus anciens et moins sûrs.

  Par exemple, pour identifier toutes les sessions qui utilisent l'algorithme SHA1, utilisez la requête **`(tls_auth eq SHA)`** :

  
  (tls_auth eq SHA)

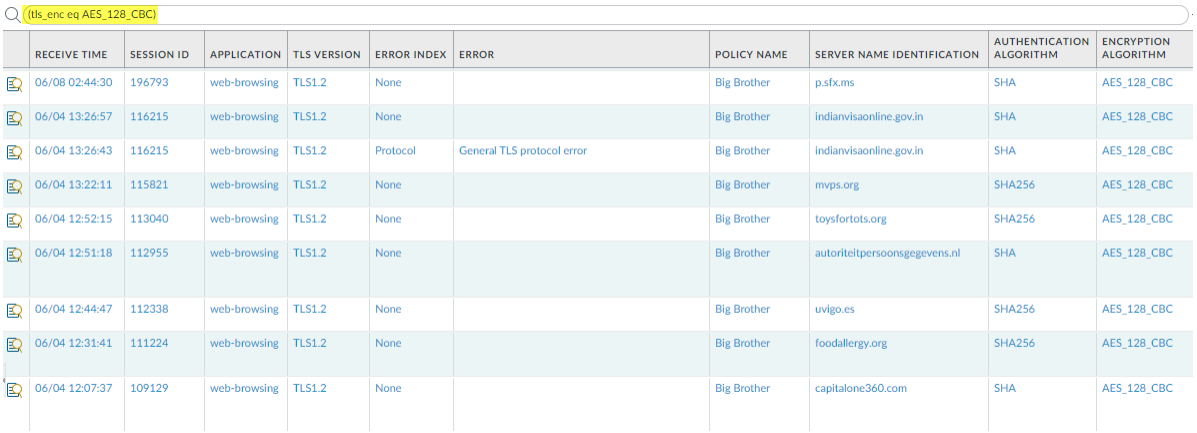
  | RECEIVE TIME | SESSION ID | APPLICATION | TLS VERSION | ERROR INDEX | ERROR | POLICY NAME | SERVER NAME IDENTIFICATION | AUTHENTICATION ALGORITHM |
  |---|---|---|---|---|---|---|---|---|
  | 06/08 23:12:02 | 213635 | ssl | TLS1.2 | None | | No Decrypt | | SHA |
  | 06/08 11:16:02 | 203438 | incomplete | TLS1.2 | None | | Big Brother | p.sfx.ms | SHA |
  | 06/08 11:16:02 | 203439 | web-browsing | TLS1.2 | None | | Big Brother | p.sfx.ms | SHA |
  | 06/08 11:15:01 | 203437 | web-browsing | TLS1.2 | None | | Big Brother | p.sfx.ms | SHA |
  | 06/08 02:45:32 | 196795 | incomplete | TLS1.2 | None | | Big Brother | p.sfx.ms | SHA |
  | 06/08 02:44:30 | 196794 | web-browsing | TLS1.2 | None | | Big Brother | p.sfx.ms | SHA |
  | 06/08 02:44:30 | 196793 | web-browsing | TLS1.2 | None | | Big Brother | p.sfx.ms | SHA |
  | 06/04 13:38:36 | 117329 | web-browsing | TLS1.2 | None | | Big Brother | inegi.org.mx | SHA |
  | 06/04 13:35:01 | 116980 | web-browsing | TLS1.2 | None | | Big Brother | rupress.org | SHA |

  Vous pouvez ajouter à la requête pour approfondir les résultats. Par exemple, vous pouvez ajouter un SNI particulier, une version d'échange de clés (comme le filtrage pour les sessions SHA1 qui utilisent également les échanges de clés RSA), une version TLS, ou toute autre métrique trouvée dans une colonne de journal de décryptage.

- Utilisez les journaux de décryptage pour identifier les sessions qui utilisent un algorithme de cryptage particulier.

  Par exemple, pour identifier toutes les sessions qui utilisent l'algorithme de cryptage AES-128-CBC, utilisez la requête **`(tls_enc eq AES_128_CBC)`** :


(tls_enc eq AES_128_CBC)

| RECEIVE TIME | SESSION ID | APPLICATION | TLS VERSION | ERROR INDEX | ERROR | POLICY NAME | SERVER NAME IDENTIFICATION | AUTHENTICATION ALGORITHM | ENCRYPTION ALGORITHM |
|---|---|---|---|---|---|---|---|---|---|
| 06/08 02:44:30 | 196793 | web-browsing | TLS1.2 | None | | Big Brother | p.sfx.ms | SHA | AES_128_CBC |
| 06/04 13:26:57 | 116215 | web-browsing | TLS1.2 | None | | Big Brother | indianvisaonline.gov.in | SHA | AES_128_CBC |
| 06/04 13:26:43 | 116215 | web-browsing | TLS1.2 | Protocol | General TLS protocol error | Big Brother | indianvisaonline.gov.in | SHA | AES_128_CBC |
| 06/04 13:22:11 | 115821 | web-browsing | TLS1.2 | None | | Big Brother | mvps.org | SHA256 | AES_128_CBC |
| 06/04 12:52:15 | 113040 | web-browsing | TLS1.2 | None | | Big Brother | toysfortots.org | SHA256 | AES_128_CBC |
| 06/04 12:51:18 | 112955 | web-browsing | TLS1.2 | None | | Big Brother | autoriteitpersoonsgegevens.nl | SHA | AES_128_CBC |
| 06/04 12:44:47 | 112338 | web-browsing | TLS1.2 | None | | Big Brother | uvigo.es | SHA256 | AES_128_CBC |
| 06/04 12:31:41 | 111224 | web-browsing | TLS1.2 | None | | Big Brother | foodallergy.org | SHA256 | AES_128_CBC |
| 06/04 12:07:37 | 109129 | web-browsing | TLS1.2 | None | | Big Brother | capitalone360.com | SHA | AES_128_CBC |

  Vous pouvez ajouter à la requête pour approfondir les résultats.

  Voici quelques exemples de requêtes pour trouver d'autres anciens algorithmes de cryptage : **`(tls_enc eq DES_CBC)`**, **`(tls_enc eq 3DES_EDE_CBC)`** et **`(tls_enc eq DES40_CBC)`**.

- Utilisez cette méthodologie et le constructeur de filtre de journal pour créer des requêtes afin d'étudier les courbes ECC négociées et toute autre information que vous trouvez dans le journal de décryptage.

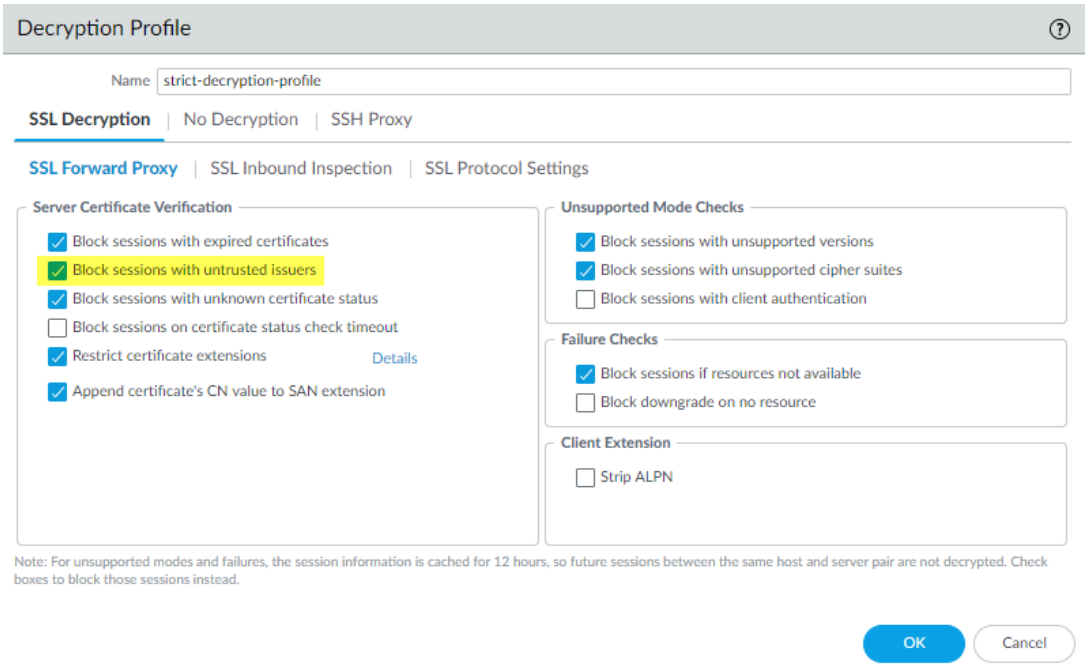
## Identification des certificats CA non approuvés

Le blocage de l'accès aux sites avec des certificats CA non approuvés et des certificats auto-signés par une CA racine non approuvée est une bonne pratique car les sites avec des CA non approuvées fiables peuvent indiquer une attaque de type homme du milieu, une attaque par rediffusion ou toute autre activité malveillante.

**STEP 1 |** Assurez-vous de **Block sessions with untrusted issuers (Bloquer les sessions avec des émetteurs non approuvés)** dans le profil de décryptage du proxy de transfert (**Objects (Objets)**

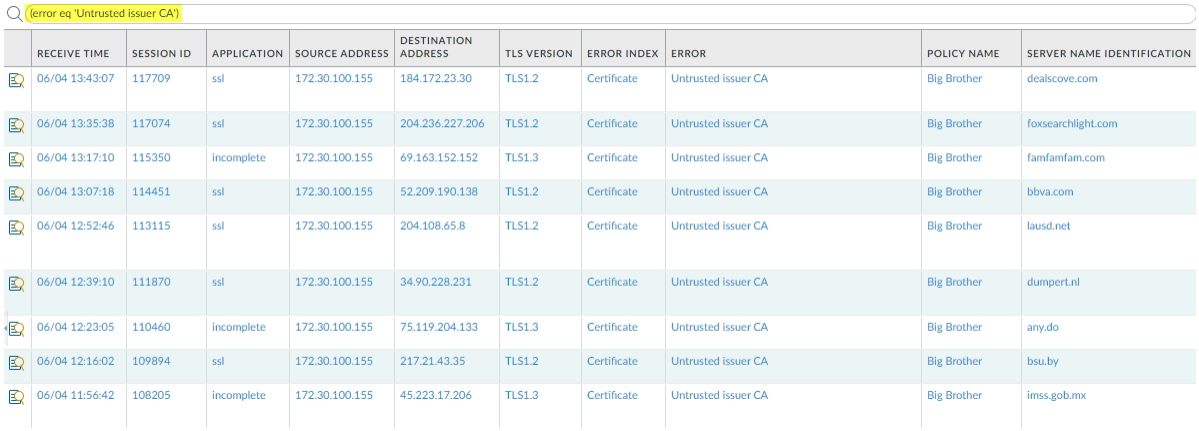
 

> **Decryption (Décryptage)** > **Decryption Profiles (Porifls de décryptage)**) pour bloquer les sites avec des CA non approuvées.




Lorsque vous bloquez des sessions avec des émetteurs non approuvés dans le profil de décryptage, le journal de décryptage (**Monitor (Moniteur)** > **Logs (Journaux)** > **Decryption (Décryptage)**) enregistre l'erreur.

**STEP 2 |** Filtrez le journal pour identifier les sessions qui ont échoué en raison de certificats révoqués à l'aide de la requête **`(error eq 'Untrusted issuer CA'`**).


(error eq 'Untrusted issuer CA')

| RECEIVE TIME | SESSION ID | APPLICATION | SOURCE ADDRESS | DESTINATION ADDRESS | TLS VERSION | ERROR INDEX | ERROR | POLICY NAME | SERVER NAME IDENTIFICATION |
|---|---|---|---|---|---|---|---|---|---|
| 06/04 13:43:07 | 117709 | ssl | 172.30.100.155 | 184.172.23.30 | TLS1.2 | Certificate | Untrusted issuer CA | Big Brother | dealscove.com |
| 06/04 13:35:38 | 117074 | ssl | 172.30.100.155 | 204.236.227.206 | TLS1.2 | Certificate | Untrusted issuer CA | Big Brother | foxsearchlight.com |
| 06/04 13:17:10 | 115350 | incomplete | 172.30.100.155 | 69.163.152.152 | TLS1.3 | Certificate | Untrusted issuer CA | Big Brother | famfamfam.com |
| 06/04 13:07:18 | 114451 | ssl | 172.30.100.155 | 52.209.190.138 | TLS1.2 | Certificate | Untrusted issuer CA | Big Brother | bbva.com |
| 06/04 12:52:46 | 113115 | ssl | 172.30.100.155 | 204.108.65.8 | TLS1.2 | Certificate | Untrusted issuer CA | Big Brother | lausd.net |
| 06/04 12:39:10 | 111870 | ssl | 172.30.100.155 | 34.90.228.231 | TLS1.2 | Certificate | Untrusted issuer CA | Big Brother | dumpert.nl |
| 06/04 12:23:05 | 110460 | incomplete | 172.30.100.155 | 75.119.204.133 | TLS1.3 | Certificate | Untrusted issuer CA | Big Brother | any.do |
| 06/04 12:16:02 | 109894 | ssl | 172.30.100.155 | 217.21.43.35 | TLS1.2 | Certificate | Untrusted issuer CA | Big Brother | bsu.by |
| 06/04 11:56:42 | 108205 | incomplete | 172.30.100.155 | 45.223.17.206 | TLS1.3 | Certificate | Untrusted issuer CA | Big Brother | imss.gob.mx |

**STEP 3 |** (Facultatif) Vérifiez la date d'expiration du certificat sur le site Qualys SSL Labs.

Saisissez le nom d'hôte du serveur (colonne **Server Name Identification (Identification du nom de serveur)** du journal de décryptage) dans le champ **Hostname (Nom d'hôte)** et **Submit (Soumettre)** pour afficher les informations du certificat pour l'hôte.

## Dépannage des certificats expirés

Si vous suivez les meilleures pratiques de décryptage et **bloquez les sessions avec des certificats expirés** dans le profil de décryptage du proxy de transfert ou dans le profil de non décryptage, alors si un serveur présente un certificat expiré, le pare-feu bloque la session. Toutefois, si un site auquel vous devez accéder pour des raisons professionnelles voit son certificat expirer, les connexions à ce site peuvent être bloquées et vous ne savez peut-être pas pourquoi.

Vous pouvez utiliser le journal de décryptage pour vérifier les certificats expirés et les certificats qui expireront bientôt afin d'être informé de la situation et de prendre les mesures appropriées.

**STEP 1 |** Filtrez le journal de décryptage des certificats expirés à l'aide de la requête **`(error eq 'Expired server certificate')`**.

(error eq 'Expired server certificate')

| RECEIVE TIME | SESSION ID | APPLICATION | SOURCE ADDRESS | DESTINATION ADDRESS | TLS VERSION | ERROR INDEX | ERROR | SERVER NAME IDENTIFICATION | POLICY NAME |
|---|---|---|---|---|---|---|---|---|---|
| 06/04 16:19:49 | 121352 | incomplete | 172.30.100.10 | 34.225.62.221 | TLS1.3 | Certificate | Expired server certificate | www.stanford.edu | Big Brother |
| 06/04 13:43:26 | 117747 | incomplete | 172.30.100.155 | 104.197.149.89 | TLS1.3 | Certificate | Expired server certificate | phone.com | Big Brother |
| 06/04 13:41:03 | 117572 | incomplete | 172.30.100.155 | 208.117.9.16 | TLS1.3 | Certificate | Expired server certificate | netcarshow.com | Big Brother |
| 06/04 13:38:51 | 117379 | ssl | 172.30.100.155 | 69.172.200.184 | TLS1.2 | Certificate | Expired server certificate | royal.gov.uk | Big Brother |
| 06/04 13:36:27 | 117150 | ssl | 172.30.100.155 | 107.21.104.61 | TLS1.2 | Certificate | Expired server certificate | www.uthscsa.edu | Big Brother |
| 06/04 13:34:53 | 117004 | incomplete | 172.30.100.155 | 66.115.56.251 | TLS1.3 | Certificate | Expired server certificate | gunsamerica.com | Big Brother |
| 06/04 13:33:17 | 116853 | incomplete | 172.30.100.155 | 34.107.140.234 | TLS1.3 | Certificate | Expired server certificate | skiplagged.com | Big Brother |
| 06/04 13:32:45 | 116798 | ssl | 172.30.100.155 | 104.236.4.58 | TLS1.2 | Certificate | Expired server certificate | uploading.com | Big Brother |
| 06/04 13:31:28 | 116655 | incomplete | 172.30.100.155 | 35.186.201.59 | TLS1.3 | Certificate | Expired server certificate | shared.com | Big Brother |
| 06/04 13:29:32 | 116507 | ssl | 172.30.100.155 | 147.139.136.53 | TLS1.2 | Certificate | Expired server certificate | beautynesia.id | Big Brother |
| 06/04 13:28:56 | 116426 | incomplete | 172.30.100.155 | 45.55.105.190 | TLS1.3 | Certificate | Expired server certificate | designbundles.net | Big Brother |

Cette requête identifie les serveurs qui génèrent des erreurs de **`certificat de serveur expiré`**. Le pare-feu bloque l'accès à ces serveurs en raison de l'expiration du certificat.

**STEP 2 |** (Facultatif) Vérifiez la date d'expiration du certificat sur le site Qualys SSL Labs.

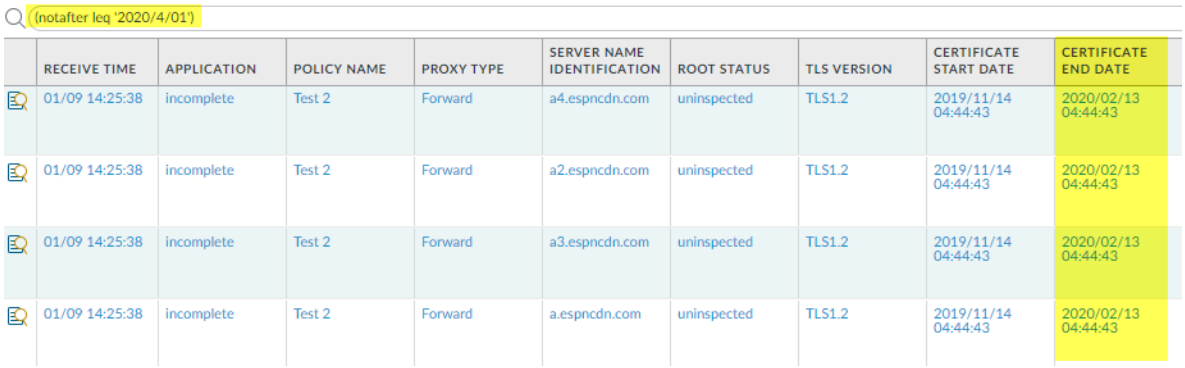
Saisissez le nom d'hôte du serveur (colonne **Server Name Identification (Identification du nom de serveur)** du journal de décryptage) dans le champ **Hostname (Nom d'hôte)** et **Submit (Soumettre)** pour afficher les informations du certificat pour l'hôte.

**STEP 3 |** Filtrez le journal de décryptage (**Monitor (Moniteur)** > **Logs (Journaux)** > **Decryption (Décryptage)**) pour les certificats qui expireront bientôt, en utilisant une requête qui identifie les dates de fin de certificat à venir.

Par exemple, si la date d'aujourd'hui est le 1er février 2020 et que vous voulez vous donner deux mois pour évaluer et préparer le cas où les sites ne mettraient pas à jour leurs certificats,

interrogez le journal de décryptage pour les certificats qui expirent le 1er avril 2020 ou avant (**`notafter leq '2020/4/01')`**) :




| | RECEIVE TIME | APPLICATION | POLICY NAME | PROXY TYPE | SERVER NAME IDENTIFICATION | ROOT STATUS | TLS VERSION | CERTIFICATE START DATE | CERTIFICATE END DATE |
|---|---|---|---|---|---|---|---|---|---|
| | 01/09 14:25:38 | incomplete | Test 2 | Forward | a4.espncdn.com | uninspected | TLS1.2 | 2019/11/14 04:44:43 | 2020/02/13 04:44:43 |
| | 01/09 14:25:38 | incomplete | Test 2 | Forward | a2.espncdn.com | uninspected | TLS1.2 | 2019/11/14 04:44:43 | 2020/02/13 04:44:43 |
| | 01/09 14:25:38 | incomplete | Test 2 | Forward | a3.espncdn.com | uninspected | TLS1.2 | 2019/11/14 04:44:43 | 2020/02/13 04:44:43 |
| | 01/09 14:25:38 | incomplete | Test 2 | Forward | a.espncdn.com | uninspected | TLS1.2 | 2019/11/14 04:44:43 | 2020/02/13 04:44:43 |

La colonne **Certificate End Date (Date de fin de certificat)** indique la date exacte à laquelle le certificat expire.

**STEP 4 |** Déterminez les mesures à prendre pour les sites dont les certificats ont expiré.

- Si vous n'avez pas besoin d'accéder au site à des fins professionnelles, la mesure la plus sûre est de continuer à bloquer l'accès au site.
- Si vous avez besoin d'accéder au site à des fins professionnelles, prenez l'une des mesures suivantes :
  - Contactez l'administrateur du site dont le certificat a expiré et informez-le qu'il doit mettre à jour ou renouveler son certificat.
  - Créez une politique de décryptage qui s'applique uniquement aux sites dont les certificats ont expiré et dont vous avez besoin à des fins professionnelles, ainsi qu'un profil de décryptage qui autorise les sites dont les certificats ont expiré. N'appliquez pas cette politique à des sites dont vous n'avez pas besoin à des fins professionnelles. Lorsqu'un site met à jour son certificat, il faut le retirer de la politique.

## Dépannage des certificats révoqués

Un certificat révoqué n'est plus valable. Cela peut indiquer qu'un site présente des problèmes de sécurité et que le certificat n'est pas digne de confiance, bien qu'il existe également des raisons bénignes pour lesquelles un certificat peut être révoqué.

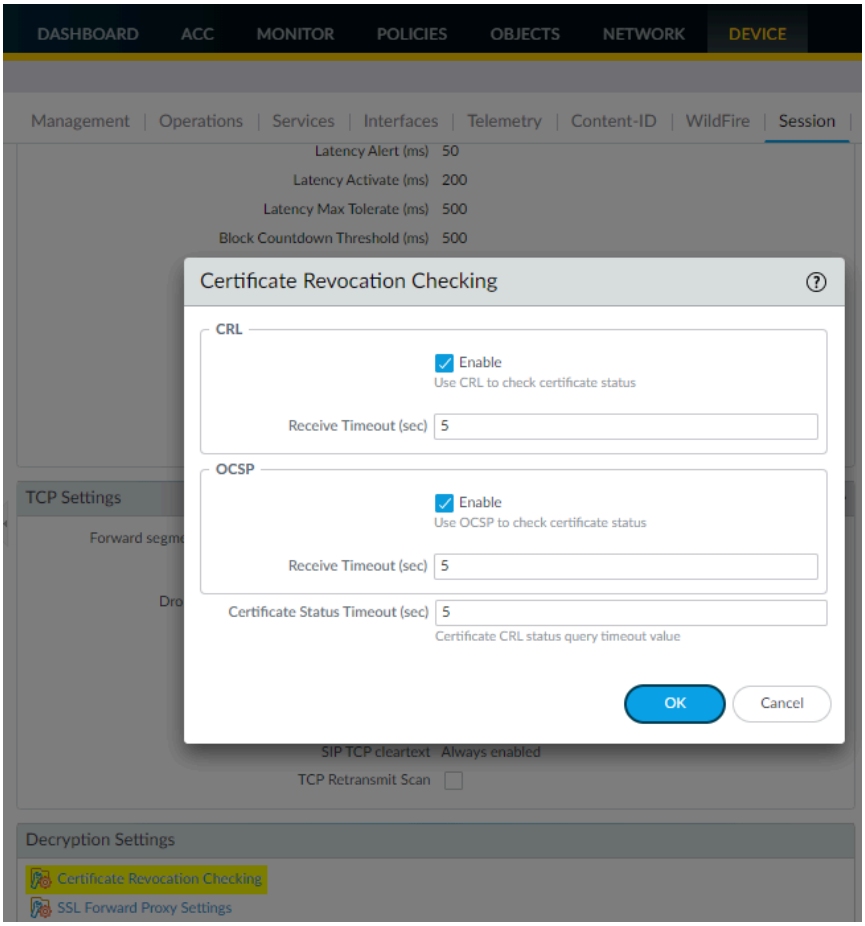
***Ne vous fiez pas aux certificats révoqués ; activez la vérification de la révocation des certificats pour refuser l'accès aux sites dont les certificats sont révoqués.***

Afin d'abandonner les sessions avec des certificats révoqués et de dépanner les certificats révoqués, vous devez activer la vérification de la révocation des certificats. Si vous n'activez pas la vérification de la révocation des certificats, le pare-feu ne vérifie pas les certificats révoqués et vous ne saurez pas si un site possède un certificat révoqué.

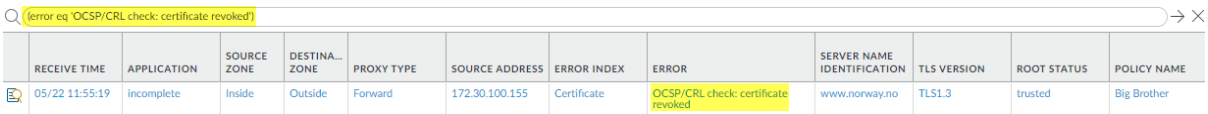
**STEP 1 |** Activez la vérification de la révocation des certificats si vous ne l'avez pas déjà fait.

1. Accédez à **Device (Périphérique)** > **Setup (Configuration)** > **Session** > **Decryption Settings (Paramètres de décryptage)**.
2. Activer la vérification des certificats OCSP et CRL.




Si vous **bloquez des sessions sur le délai d'expiration de vérification de l'état du certificat** dans le profil de décryptage du proxy de transfert et que vous craignez que 5 secondes ne suffisent pas et puissent entraîner un trop grand nombre de sessions bloquées par des délais d'expiration, réglez le **Receive Timeout (Délai d'expiration de réception) (seconde)** sur une durée plus longue.

**STEP 2 |** Filtre le journal de décryptage (**Monitor (Moniteur)** > **Logs (Journaux)** > **Decryption (Décryptage)**) pour trouver les erreurs de révocation de certificat en utilisant la requête **`(error eq 'OCSP/CRL check: certificate revoked')`**.




**STEP 3 |** (Facultatif) Vérifiez la date d'expiration du certificat sur le site Qualys SSL Labs.

Saisissez le nom d'hôte du serveur (colonne **Server Name Identification (Identification du nom de serveur)** du journal de décryptage) dans le champ **Hostname (Nom d'hôte)** et **Submit (Soumettre)** pour afficher les informations du certificat pour l'hôte.

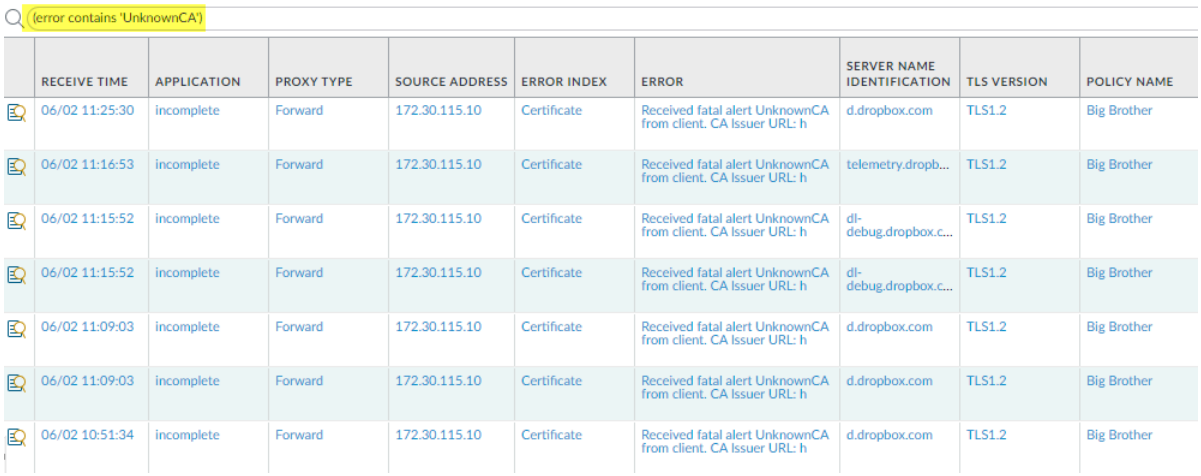
## Dépannage des certificats épinglés

L'épinglage du certificat oblige l'application client à valider le certificat du serveur par rapport à une copie connue afin de s'assurer que ce certificat provient bien du serveur. Le but des certificats épinglés est de protéger contre les attaques de type homme au milieu (MITM) où un dispositif entre le client et le serveur remplace le certificat du serveur par un autre certificat.

Bien que cela empêche les acteurs malveillants d'intercepter et de manipuler les connexions, cela empêche également le décryptage du proxy de transfert car le pare-feu crée un certificat d'usurpation d'identité au lieu du certificat de serveur à présenter au client. Au lieu d'une session qui connecte directement le client et le serveur, le proxy de transfert crée deux sessions, une entre le client et le pare-feu et une autre entre le pare-feu et le serveur. Cela permet d'établir la confiance avec le client afin que le pare-feu puisse décrypter et inspecter le trafic.

Cependant, lorsqu'un certificat est épinglé, le pare-feu ne peut pas décrypter le trafic car le client n'accepte pas le certificat d'usurpation d'identité du pare-feu : le client n'accepte que le certificat qui est épinglé à l'application.

**STEP 1 |** Filtrez le journal de décryptage (**Monitor (Moniteur)** > **Logs (Journaux)** > **Decryption (Décryptage)**) pour trouver les certificats épinglés en utilisant la requête **`(error contains 'UnknownCA')`**.




L'application génère un code d'erreur TLS (Alerte) lorsqu'elle ne parvient pas à vérifier le certificat du serveur. Les différentes applications peuvent utiliser des codes d'erreur différents pour indiquer un certificat épinglé. Les indicateurs d'erreur les plus courants pour les certificats épinglés sont UnknownCA et BadCertificate. Après avoir lancé la requête **`(error contains 'UnknownCA')`**, lancez la requête **`(error contains 'BadCertificate')`** pour détecter d'autres erreurs de certificats épinglés.

*Vous pouvez utiliser Wireshark ou d'autres analyseurs de paquets pour revérifier l'erreur. Recherchez le client qui coupe la connexion immédiatement après la communication TLS pour confirmer qu'il s'agit d'une émission de certificat épinglé.*

**STEP 2 |** Décidez de ce qu'il faut faire des certificats épinglés.

Si vous n'avez pas besoin d'un accès à des fins professionnelles, vous pouvez laisser le pare-feu continuer à bloquer l'accès. Si vous avez besoin de l'accès, vous pouvez Exclure un serveur du déchiffrement pour des raisons techniques en l'ajoutant à la liste d'exclusion du décryptage SSL

(**Device (Périphérique)** > **Certificate Management (Gestion de certificat)** > **SSL Decryption Exclusion (Exclusion du décryptage SSL)**.

Le pare-feu contourne le décryptage pour les sites figurant sur la liste d'exclusion de décryptage SSL. Le pare-feu ne peut pas inspecter le trafic, mais le trafic est autorisé.

# Activation des licences gratuites pour le déchiffrement

Aucune licence n'est requise pour décrypter le SSH traffic (trafic SSH) et le trafic SSL (SSL internet traffic (trafic Internet SSL) ou SSL traffic to an internal server (trafic SSL vers un serveur interne)). Cependant, vous devez activer une licence gratuite pour activer la Decryption Mirroring (mise en miroir du décryptage). La licence gratuite garantit que cette fonctionnalité ne puisse être utilisée qu'une fois que le personnel autorisé a volontairement activé la licence associée.

*Dans PAN-OS 10.1, la fonctionnalité Decryption Broker et la licence libre ont été remplacées par Network Packet Broker (voir le Networking Administrator's Guide (Guide de l'administrateur réseau)),qui étend les capacités du broker au trafic TLS non déchiffré et au trafic non TLS en plus du trafic TLS déchiffré. Les Network Packet Broker licenses (licences Network Packet Broker) peuvent également être téléchargées et installées gratuitement à partir du Customer Support Portal (portail de support client).*

Suivez ces étapes sur le portail d'assistance client de Palo Alto Networks pour activer une licence de mise en miroir de décryptage.

**STEP 1 |** Ouvrez une session dans le portail de support client.

**STEP 2 |** Sélectionnez **Assets (Ressources)** > **Devices (Périphériques)** sur le panneau de navigation de gauche.

**STEP 3 |** Trouvez le périphérique sur lequel vous souhaitez activer la mise en miroir du port de décryptage, puis sélectionnez **Actions** (l'icône en forme de crayon).

**STEP 4 |** Sous Activate Licenses (Activer les licences), sélectionnez **Activate Feature License (Activer la licence de fonctionnalité)**.

**STEP 5 |** Sélectionnez la fonctionnalité pour laquelle vous souhaitez activer une licence gratuite : **Decryption Port Mirror (Miroir du port de décryptage)**.

**STEP 6 |** **Agree and Submit (Accepter et envoyer)**.

**STEP 7 |** Installez la licence de mise en miroir de déchiffrement sur le pare-feu.

1. Sélectionnez **Device (Périphérique)** > **Licenses (Licences)**.
2. Cliquez sur **Retrieve license keys from license server (Récupérer les clés de licence auprès du serveur de licences)**.
3. Vérifiez que la licence **Decryption Port Mirror (port de déchiffrement en miroir)** est maintenant active sur le pare-feu.
4. Redémarrez le pare-feu (**Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)**). La mise en miroir des ports de déchiffrement n'est pas disponible pour la configuration tant que le pare-feu ne se recharge pas.

# Filtrage des URL

La solution de filtrage des URL de Palo Alto Networks vous permet de surveiller et de contrôler les sites auxquels les utilisateurs peuvent accéder, pour empêcher les attaques par hameçonnage en contrôlant les sites sur lesquels les utilisateurs peuvent envoyer des informations d'identification professionnelles valides, et d'appliquer la recherche sécurisée pour les moteurs de recherche comme Google et Bing.

# À propos du filtrage d'URL

Le filtrage des URL de Palo Alto Networks vous protège contre les menaces Web en vous offrant un moyen d'activer l'accès Web en toute sécurité tout en contrôlant l'interaction de vos utilisateurs avec le contenu en ligne. Vous pouvez créer des règles de stratégie pour limiter l'accès aux sites en fonction des URL categories (catégories d'URL), des utilisateurs et des groupes. (Voir URL Filtering Use Cases (Cas d'utilisation du filtrage d'URL) pour connaître les différentes façons dont vous pouvez tirer parti du filtrage d'URL pour répondre aux besoins de votre organisation en matière de sécurité Web.)

Lorsque le filtrage des URL est activé, tout le trafic web (HTTP et HTTPS) sur n'importe quel port est :

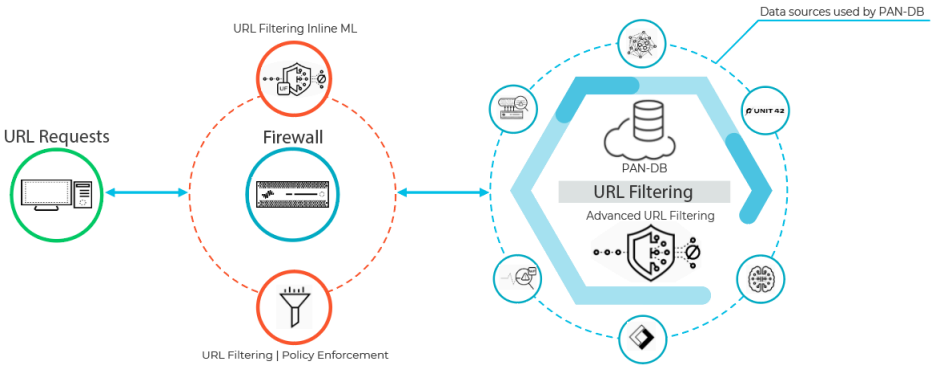
- Comparé à la base de données de filtrage des URL, qui répertorie des millions de sites Web qui ont été catégorisés. Vous pouvez utiliser ces catégories d'URL dans les profils de filtrage d'URL ou comme critères de correspondance pour appliquer la politique de sécurité. Vous pouvez également utiliser le filtrage des URL pour appliquer les paramètres de recherche sécurisée pour vos utilisateurs et empêcher le vol identifiants sur la base de la catégorie d'URL. Avec l'ajout d'une Filtrage d'URL avancé licence, les URL présentant des qualités suspectes sont analysées simultanément en temps réel à l'aide de l'apprentissage machine pour fournir une protection contre les menaces nouvelles et inconnues qui n'existent pas actuellement dans la base de données de filtrage d'URL.
- Inspecté pour détecter le hameçonnage et les JavaScript malveillants grâce à l'apprentissage machine Inline (ML), une solution d'analyse basée sur un pare-feu, qui peut bloquer en temps réel les pages web malveillantes inconnues.

La solution de filtrage d'URL de Palo Alto Networks, PAN-DB, vous permet de choisir entre le ***PAN-DB Public Cloud*** et le ***PAN-DB Private Cloud,***, utilisez la solution de cloud public si les pare-feu de nouvelle génération de Palo Alto Networks sur votre réseau peuvent accéder directement à Internet. Si les exigences de sécurité du réseau de votre entreprise interdisent aux pare-feu d'accéder directement à Internet, vous pouvez déployer un cloud privé PAN-DB sur un ou plusieurs périphériques M-600 qui fonctionnent en tant que serveurs PAN-DB dans votre réseau.

# Fonctionnement du filtrage des URL

PAN-DB—la base de données de filtrage des URL dans le cloud—classifie les sites Web selon le contenu, les fonctions et la sécurité du site. Une URL peut compter un maximum de quatre catégories d'URL, y compris les catégories de risque (élevé, modéré et facile) qui indique la probabilité que le site vous expose à des menaces. Comme PAN-DB catégorise les sites, les pare-feu sur lesquels le filtrage des URL est activé peuvent tirer profit de ces connaissances pour appliquer les politiques de sécurité de votre organisation. En plus de la protection offerte par la base de données PAN-DB, Filtrage d'URL avancé fournit une analyse en temps réel à l'aide du langage machine pour se défendre contre les menaces nouvelles et inconnues.




Lorsqu'un utilisateur demande une page Web, le pare-feu interroge les exceptions ajoutées par l'utilisateur et PAN-DB pour la catégorie de risque du site. PAN-DB utilise les informations d'URL de l'unité 42, WildFire, DNS passif, données de télémétrie Palo Alto Networks, données de la Cyber Threat Alliance, et applique divers analyseurs pour déterminer la catégorie. Si l'URL affiche des caractéristiques risquées ou malveillantes, elle est également soumise à un filtrage d'URL avancé dans le cloud pour une analyse en temps réel et génère des données d'analyse supplémentaires. La catégorie de risque qui en résulte est ensuite récupérée par le pare-feu et est utilisée pour appliquer les règles d'accès Web en fonction de la configuration de votre politique. En outre, le pare-feu met en cache les informations de catégorisation du site pour les nouvelles entrées afin de permettre une récupération rapide des demandes ultérieures, tout en supprimant les URL auxquelles les utilisateurs n'ont pas accédé récemment afin de refléter avec précision le trafic de votre réseau. En outre, des contrôles intégrés aux requêtes PAN-DB dans le cloud garantissent que le pare-feu reçoit les dernières informations de catégorisation des URL. Si vous ne disposez pas d'une connectivité Internet ou d'une licence de filtrage d'URL PAN-DB active, aucune requête n'est adressée à PAN-DB.


Le pare-feu détermine la catégorie d'URL d'un site Web en la comparant aux entrées de 1) catégories d'URL personnalisées, 2) listes dynamiques externes (EDL) et 3) catégories d'URL prédéfinies, par ordre de priorité.

Les pare-feu configurés pour analyser les URL en temps réel à l'aide de l'apprentissage automatique sur le plan de données fournissent une couche de sécurité supplémentaire contre les sites web de hameçonnage et les exploitations JavaScript. Les modèles Inline ML utilisés pour identifier ces menaces basées sur des URL s'étendent aux menaces actuellement inconnues ainsi qu'aux futures variantes de menaces qui correspondent aux caractéristiques que Palo Alto Networks a identifiées comme malveillantes. Afin d'être au courant des dernières évolutions des menaces, les modèles Inline ML sont ajoutés ou mis à jour via des communiqués de contenu.

Lorsque que le pare-feu vérifie une URL auprès de PAN-DB, il cherche également des mises à jour critiques, notamment les URL qui, préalablement, étaient bénignes, mais qui sont désormais malveillantes.

Si vous croyez que PAN-DB a mal catégorisé un site, vous pouvez soumettre une demande de changement de catégorie d'URL dans votre navigateur via le site d'essai A ou directement dans les journaux du pare-feu.

***Le saviez-vous ?***

*Techniquement, le pare-feu met les URL en mémoire tampon sur le plan de gestion et le plan de données :*

- *PAN-OS 9.0 et les versions ultérieures ne téléchargent pas les bases de données PAN-DB initiales. Au lieu, lors de l'activation de la licence de filtrage des URL, le pare-feu remplit le cache au fur et à mesure que les requêtes d'URL sont transmises.*
- *Le plan de gestion contient plus d'URL et communique directement avec PAN-DB Quand le pare-feu ne peut pas trouver la catégorie d'une URL dans sa mémoire tampon et effectue une recherche dans PAN-DB, il cache l'information de catégorie dans le plan de gestion. Le plan de gestion passe l'information au plan de données, qui la met aussi en mémoire tampon pour appliquer les politiques.*
- *Le plan de données contient moins d'URL et reçoit les informations du plan de gestion Après que le pare-feu ait vérifié les URL category exception lists (listes d'exception de catégories d'URL) (catégories d'URL personnalisées et listes dynamiques externes) pour une URL, l'endroit qu'il examine est le plan de données Si seulement le pare-feu ne peut pas trouver la catégorie d'URL dans le plan de données, le pare-feu vérifie le plan de gestion et si l'information de la catégorie n'y est pas, PAN-DB.*

# Filtrage d'URL avancé

Le filtrage avancé des URL est un service d'abonnement qui complète la solution de filtrage d'URL PAN-DB pour fournir une analyse d'URL en temps réel à l'aide de techniques d'apprentissage automatique afin de générer une analyse plus précise des URL que possible avec les techniques traditionnelles de filtrage de base de données Web seules. Cela offre une protection contre les URL malveillantes qui sont mises à jour ou introduites avant que les bases de données de filtrage d'URL aient la possibilité d'analyser et d'ajouter le contenu, donnant aux attaquants une période ouverte à partir de laquelle ils peuvent lancer des campagnes d'attaque de précision. Le filtrage avancé des URL compense les lacunes de couverture inhérentes aux solutions de base de données en fournissant une analyse d'URL en temps réel par demande. Les modèles basés sur le ML utilisés par le filtrage avancé des URL ont été formés et sont continuellement mis à jour pour détecter diverses URL malveillantes, pages Web de phishing et C2. Lorsqu'un utilisateur visite une URL désignée comme étant risquée, le pare-feu soumet l'URL au service de filtrage d'URL avancé pour analyse à l'aide de l'apprentissage automatique afin de déterminer sa catégorie de menace. À l'aide de ce verdict, le pare-feu applique des règles d'accès Web en fonction de la configuration de votre politique. Une licence de filtrage d'URL avancée active est requise pour Activer le filtrage d'URL avancé. En outre, vous devez définir une stratégie de trafic Web dans votre profil de filtrage d'URL pour contrôler le trafic en fonction des politiques d'utilisation Web de votre organisation.

Le site Web Test A Site de filtrage d'URL (une ressource de base de données cloud de filtrage d'URL en ligne) exploite également les données du filtrage d'URL avancé pour améliorer la catégorisation des URL.

Ce service d'abonnement est disponible sur les pare-feux fonctionnant sous PAN-OS 9.0 et versions ultérieures, avec l'installation de la version de contenu 8390-6607.

***L'abonnement de sécurité Filtrage d'URL avancé n'est pas disponible sur les pare-feux de la série CN.***

# Filtrage des URL Inline ML

Le filtrage des URL Inline ML permet au plan de données du pare-feu d'appliquer l'apprentissage machine sur les pages web pour alerter les utilisateurs lorsque des variantes de hameçonnage sont détectées tout en empêchant des variantes malveillantes d'exploits JavaScript de pénétrer sur votre réseau. Inline ML analyse et détecte dynamiquement le contenu malveillant en évaluant divers détails des pages web à l'aide d'une série de modèles ML. Chaque modèle Inline ML détecte les contenus malveillants en évaluant les détails des fichiers, y compris les champs et les modèles du décodeur, afin de formuler une classification et un verdict de haute probabilité, qui sont ensuite utilisés dans le cadre de votre politique de sécurité web plus large. Les URL classées comme malveillantes sont transmises à PAN-DB pour une analyse et une validation supplémentaires. En outre, vous pouvez également spécifier des exceptions d'URL pour exclure tout faux positif qui pourrait être rencontré. Cela vous permet de créer des règles plus granulaires pour vos profils afin de répondre à vos besoins spécifiques en matière de sécurité. Afin d'être au courant des dernières évolutions des menaces, les modèles Inline ML sont régulièrement mis à jour et ajoutés via des communiqués de contenu. Une licence de filtrage d'URL PAN-DB active est requise pour configure URL Filtering inline ML (configurer le filtrage d'URL en ligne ML).

La protection basée sur Inline ML peut également être activée pour détecter les fichiers PE et les scripts PowerShell malveillants en temps réel dans le cadre de la configuration de votre profil antivirus. Pour en savoir plus, reportez-vous à la section : WildFire Inline ML

***Le filtrage des URL Inline ML n'est pas pris en charge sur l'appareil virtuel VM-50 ou VM50L.***

# Cas pratiques du filtrage des URL

Il existe de nombreuses façons d'utiliser le filtrage des URL. Celui-ci ne se limite pas à bloquer et à autoriser certains sites. Par exemple, vous pouvez utiliser plusieurs catégories par URL pour autoriser les utilisateurs à accéder à un site, tout en bloquant certaines fonctions, comme la soumission des informations d'identification d'entreprise ou le téléchargement des fichiers. Vous pouvez également utiliser les catégories d'URL pour appliquer différents types de politiques, comme l'authentification, le décryptage, la QoS et la sécurité.

Lisez-en davantage sur les différentes façons d'utiliser le filtrage des URL.

### Contrôlez l'accès Web en fonction d'une catégorie d'URL

Vous pouvez créer un profil de filtrage des URL qui précise une action pour chaque catégorie d'URL et associer le profil à une règle de politique. Le pare-feu applique la politique au trafic en fonction des paramètres définis dans le profil. Par exemple, pour bloquer tous les sites de jeux, vous pouvez définir l'action bloquer pour la catégorie d'URL ***games (jeux)*** dans le profil de filtrage des URL d'URL et l'associer à la ou aux règles de politique de sécurité qui autorisent l'accès au Web.

### Filtrage des URL de plusieurs catégories

Chaque URL peut compter un maximum de quatre catégories, y compris une catégorie de risque qui indique la probabilité que le site vous expose à des menaces. Des catégorisations d'URL plus granulaires signifient que vous pouvez passer à une approche qui dépasse le simple fait « de bloquer ou d'autoriser » l'accès Web. Vous pouvez plutôt contrôler l'interaction des utilisateurs avec le contenu en ligne qui, bien que nécessaire à des fins d'affaires, est le plus à risque d'être utilisé dans le cadre d'une cyberattaque.

Par exemple, vous pourriez considérer que certaines catégories d'URL sont plus risquées pour votre organisation, mais vous pourriez hésiter à les bloquer immédiatement, car elles offrent des ressources ou des services précieux (comme des services de stockage dans le cloud ou des blogues). Vous pouvez maintenant autoriser les utilisateurs à visiter des sites qui correspondent à ces types de catégories d'URL, tout en protégeant votre réseau par le déchiffrement et l'inspection du trafic et en appliquant l'accès en lecture seule au contenu.

Pour une catégorie d'URL que vous souhaitez contrôler étroitement, définissez l'action du profil de filtrage d'URL sur alerter dans le cadre des étapes visant à Configure URL Filtering (Configurer le filtrage des URL). Puis continuer à suivre les URL Filtering best practices (Pratiques exemplaires en matière de filtrage des URL) : déchiffrez la catégorie d'URL, bloquez les téléchargements de fichiers dangereux et activez la prévention contre le hameçonnage des informations d'identification.

### Bloquez ou autorisez la soumission des informations d'identification d'entreprise en fonction de la catégorie d'URL

Prevent credential phishing(Évitez l'hameçonnage des identifiants) en activant la détection des soumissions d'informations d'identification d'entreprise aux sites par le pare-feu, puis contrôlez ces soumissions en fonction de la catégorie d'URL. Empêchez les utilisateurs d'envoyer des informations d'identification à des sites malveillants et non validés, avertissez-les contre la saisie d'informations d'identification professionnelles sur des sites inconnus ou contre la réutilisation d'informations d'identification professionnelles sur des sites hors travail, et autorisez explicitement les utilisateurs à envoyer leurs informations d'identification sur les sites de l'entreprise et les sites validés.

### Application des paramètres de recherche sécurisée

De nombreux moteurs de recherche incluent un paramètre de recherche sécurisée qui filtre les images et vidéos réservées aux adultes dans les résultats de recherche. Vous pouvez autoriser le pare-feu à bloquer des résultats de la recherche si l'utilisateur final n'utilise pas les paramètres de recherche sécurisée les plus stricts dans sa recherche, et vous pouvez mettre en œuvre la recherche sécurisée transparente pour vos utilisateurs. Le pare-feu peut appliquer la recherche sécurisée pour les moteurs de recherche suivants : Google, Yahoo, Bing, Yandex et YouTube. Voyez comment commencer à Mise en œuvre de la recherche sécurisée.

### Autoriser l'accès par mot de passe à certains sites

Vous pouvez bloquer l'accès de la plupart des utilisateurs à un site, tout en permettant à certains utilisateurs d'y accéder. Consultez allow password access to certain sites (autoriser l'accès par mot de passe à certains sites).

### Bloquez les téléchargements de fichiers à risque élevé de certaines catégories d'URL

Vous pouvez bloquer les téléchargements de fichiers à risque élevé de certaines catégories d'URL donnée en créant une politique de sécurité et en y associant un File Blocking profile (profil de blocage des fichiers).

### Politiques d'application de sécurité, de déchiffrement, d'authentification et de QoS basées sur la catégorie d'URL

Vous pouvez appliquer différents types de politiques de pare-feu en fonction des catégories d'URL. Par exemple, si vous avez activé le Déchiffrement, mais que vous souhaitez exclure certaines informations personnelles du décryptage. Dans ce cas, vous pourriez créer une règle de politique de décryptage qui exclut du décryptage les sites Web qui correspondent aux catégories d'URL ***financial-services*** et ***health-and-medicine***. Dans un autre exemple, vous pourriez utiliser la catégorie d'URL ***streaming-media*** dans une politique de QoS pour appliquer des contrôles de bande passante à tous les sites Web qui correspondent à cette catégorie.

Le tableau suivant décrit les politiques qui acceptent des catégories d'URL comme critère de correspondance :

| Type de politique | Description |
|---|---|
| **Décryptage** | Vous pouvez également utiliser les catégories d'URL pour introduire graduellement le déchiffrement, et pour exclure les catégories d'URL qui peuvent contenir des renseignements sensibles ou personnels du déchiffrement (comme les sites relatifs à des services financiers et à la santé et aux médicaments).<br><br>Prévoyez de déchiffrer le trafic le plus à risque dans un premier temps (catégories d'URL les plus susceptibles de contenir du trafic malveillant, comme les jeux ou à risque élevé), puis d'en déchiffrer davantage lorsque vous acquérez de l'expérience. Vous pouvez éventuellement déchiffrer les catégories d'URL qui n'affectent pas votre entreprise dans un premier temps (si quelque chose ne se passe pas comme prévu, cela n'affecte pas l'entreprise), par exemple, de nouveaux flux d'informations. Dans les deux cas, déchiffrez quelques catégories d'URL, tenez compte |

| Type de politique | Description |
|---|---|
| | des commentaires des utilisateurs, exécutez les rapports pour vous assurer que le déchiffrement fonctionne comme prévu, puis déchiffrez progressivement quelques catégories d'URL supplémentaires, etc. Planifiez de faire des exclusions de déchiffrement pour exclure les sites du déchiffrement, si vous ne pouvez les déchiffrer pour des raisons techniques ou parce que vous choisissez de ne pas les déchiffrer.<br><br>***Le déchiffrement du trafic en fonction des catégories d'URL est une pratique recommandée pour le filtrage des URL et le déchiffrement.*** |
| **Authentification** | Pour vous assurer que les utilisateurs s'authentifient avant d'être autorisés à accéder à une catégorie spécifique, vous pouvez associer une catégorie d'URL comme critère de correspondance pour les règles de politique d'authentification. |
| **QoS** | Utilisez des catégories d'URL pour allouer des niveaux de débit à des catégories de sites Web spécifiques. Par exemple, vous pouvez autoriser la catégorie ***streaming-media***, mais limiter le débit en ajoutant la catégorie d'URL à la règle de politique QoS. |
| **Sécurité** | Dans les Règles de politique de sécurité, vous pouvez utiliser des catégories d'URL de deux façons :<br>• Appliquer la politique en fonction des catégories d'URL que vous sélectionnez en tant que critères de correspondance.<br>• Associer un profil de filtrage des URL qui spécifie l'action de la politique à prendre à l'égard de chaque catégorie.<br><br>Si, par exemple, le groupe de sécurité informatique de votre entreprise doit avoir accès à la catégorie ***hacking***, mais que tous les autres utilisateurs ne doivent pas pouvoir y accéder, vous devez créer les règles suivantes :<br>• Une règle de politique de sécurité qui autorise le groupe de sécurité informatique à accéder au contenu catégorisé en tant que ***hacking***. La règle de politique de sécurité fait référence à la catégorie ***hacking*** dans l'onglet **Service/URL Category (Catégorie de service/d'URL)** et au groupe de sécurité informatique dans l'onglet **Users (Utilisateurs)**.<br>• Une autre règle de politique de sécurité qui autorise un accès Web général pour tous les utilisateurs. Vous associez à cette règle un profil de filtrage des URL qui bloque la catégorie ***hacking***.<br><br>La politique autorisant l'accès au ***piratage*** doit être affichée avant celle bloquant le ***piratage***. Ceci est dû au fait que la pare-feu évalue les règles de politique du haut vers le bas. Ainsi, lorsqu'un utilisateur qui fait partie du groupe de sécurité essaie d'accéder à un site de ***hacking (piratage)***, le pare-feu évalue la règle de politique qui autorise l'accès en premier, puis |

| Type de politique | Description |
| --- | --- |
| | accorde l'accès à l'utilisateur. Le pare-feu évalue les utilisateurs en les comparant à la règle d'accès Web générale qui bloque l'accès aux sites de *piratage*. |

# Catégories d'URL

PAN-DB classifie les sites Web selon le contenu, les fonctions et la sécurité du site. Une URL peut compter un maximum de quatre catégories, y compris les catégories de risque (élevé, modéré et facile) qui indique la probabilité que le site vous expose à des menaces. Pour une liste complète des catégories d'URL prédéfinies, consultez PAN-DB URL Filtering Categories (Catégories de filtrage d'URL PAN-DB).

Visitez Tester le site A pour voir comment PAN-DB catégorise une URL et pour apprendre tout au sujet des catégories URL disponibles. Vous pouvez également utiliser le Test du Site A pour soumettre une demande de modification de catégorie URL, ou vous pouvez soumettre la demande directement dans le pare-feu : sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** et ouvrez les détails d'une entrée de journal. Sous la catégorie d'URL, vous verrez l'option de soumettre une demande de modification.

Continuez de lire pour en apprendre davantage sur les catégories d'URL :

- Cas pratiques du filtrage des URL
- Catégories d'URL axées sur la sécurité
- Catégories d'URL malveillantes
- Catégories d'URL vérifiées
- Actions de politiques que vous pouvez prendre à l'égard d'une catégorie d'URL

## Catégories d'URL axées sur la sécurité

Les catégories d'URL axées sur la sécurité peuvent vous aider à réduire votre surface d'attaque en fournissant un déchiffrement et une application ciblés pour les sites qui présentent différents niveaux de risque, sans que l'on ait confirmé qu'ils sont malveillants. Les sites Web sont classés sous une catégorie liée à la sécurité tant qu'ils respectent les critères de cette catégorie ; comme le contenu des sites changent, l'application des politiques s'adapte de façon dynamique. Vous ne pouvez pas soumettre une demande de changement pour des catégories d'URL axées sur la sécurité.

| Catégories d'URL axées sur la sécurité | |
|---|---|
| **À risque élevé** | Voici des exemple de sites à risque élevé :<br>• Sites précédemment confirmés comme étant des logiciels malveillants, du hameçonnage ou des sites C2. Ces sites resteront dans cette catégorie pendant au moins 30 jours.<br>• Les domaines inconnus sont classés comme étant à risque élevé jusqu'à ce que PAN-DB termine l'analyse et la catégorisation du site.<br>• Les sites qui sont associés à des activités malveillantes confirmées. Par exemple, une page pourrait être catégorisée à risque élevé s'il y a des hôtes malveillants sur le même domaine, même si la page en tant que telle ne contient pas de contenu malveillant. |

| Catégories d'URL axées sur la sécurité | |
|---|---|
| | • Sites hébergés par un fournisseur de services Internet à toute épreuve<br>• Domaines classés comme DDNS en raison de la présence d'une configuration DNS dynamique active.<br>• Les sites hébergés sur des IP de ASN qui sont connus pour laisser passer le contenu malveillant.<br>**Action de la politique par défaut et recommandée : alert (alerter)** |
| **À risque modéré** | Voici des exemple de sites à risque modéré :<br>• Tous les sites de stockage dans le cloud (avec la catégorie d'URL **online-storage-and-backup [stockage et sauvegarde en ligne]**).<br>• Les sites qui ont déjà été confirmés comme étant des sites malveillants, de hameçonnage ou C2 qui présentent uniquement des activités bénignes depuis au moins 30 jours. Ces sites resteront dans cette catégorie pendant 60 jours supplémentaires.<br>• Les adresses IP inconnues sont classées comme étant à risque modéré jusqu'à ce que PAN-DB termine l'analyse et la catégorisation du site.<br>**Action de la politique par défaut et recommandée : alert (alerter)** |
| **À risque faible** | Les sites qui ne sont pas classés à risque modéré ou à risque élevé sont considérés comme étant à risque faible. Ces sites affichent une activité bénigne depuis au moins 90 jours.<br>**Action de la politique par défaut et recommandée : allow (autoriser)** |
| **Domaines nouvellement enregistrés** | Identifie les sites qui ont été enregistrés au cours des 32 derniers jours. Il arrive fréquemment que les nouveaux domaines soient utilisés comme outils dans les campagnes malveillantes.<br>**Action de la politique par défaut : alert (alerter)**<br>**Action recommandée de la politique : Bloquer**<br>  *Les domaines nouvellement enregistrés sont souvent générées volontairement ou par les algorithmes de génération de domaines et utilisés pour mener des activités malveillantes. Il est recommandé de bloquer cette catégorie d'URL* |

# Catégories d'URL malveillantes

Nous vous recommandons fortement de bloquer les catégories d'URL qui identifient du contenu malveillant ou à risque. Pour commencer, vous pouvez cloner le profil de filtrage des URL par défaut, qui bloque les catégories d'URL malveillants, de hameçonnage et de commandement et contrôle par défaut. Le profil de filtrage des URL par défaut bloque également les catégories D'URL relatives à la toxicomanie, aux sites destinés aux adultes, aux jeux, au piratage et aux armes ainsi que celles qui sont discutables. Le décision de bloquer ces catégories dépend de vos exigences d'affaires. Par exemple, une université ne voudra probablement pas restreindre l'accès de ses étudiants à la plupart de ces sites parce que la disponibilité est importante, mais une entreprise qui valorise la sécurité avant tout pourrait en bloquer une partie ou la totalité.

- **Command-and-control (Commande et contrôle)** : Les URL et les domaines de commande et contrôle utilisés par les logiciels malveillants et autres systèmes compromis pour communiquer discrètement avec le serveur à distance d'un pirate afin de recevoir des commandes malveillantes ou d'exfiltrer des données.
- **malware (logiciel malveillant)** : sites qui sont reconnus pour héberger des logiciels malveillants ou qui sont utilisés pour du trafic de commande et de contrôle (C2). Ils peuvent également contenir des kits d'attaque.
- **phishing (hameçonnage)** : sites qui sont reconnus pour héberger des pages de phishing pour obtenir les informations de connexion ou pour tenter d'obtenir les identifiants personnels par hameçonnage. Cela inclut le contenu Web qui tente secrètement de tromper l'utilisateur afin de collecter des informations, y compris les informations de connexion, les informations de carte de crédit - volontairement ou involontairement, les numéros de compte, les codes PIN et toute information considérée comme une information personnellement identifiable (PII) des victimes via les réseaux sociaux. techniques d'ingénierie. Les escroqueries au support technique et les scarewares sont également inclus comme hameçonnage.
- **logiciel indésirable** : les sites web et les services qui ne répondent pas à la définition d'un virus ou qui constituent une menace directe pour la sécurité, mais qui affichent un comportement envahissant et incitent les utilisateurs à accorder un accès à distance ou à effectuer d'autres actions non autorisées. Les logiciels indésirables comprennent les escroqueries, les activités illégales, les activités criminelles, les sites « devenez riches rapidement », les logiciels publicitaires et autres applications indésirables ou non sollicitées, telles que les crypto-mineurs intégrés ou les pirates qui modifient les éléments du navigateur. Les domaines de typosquattage qui ne font pas preuve de malveillance et qui ne sont pas détenus par le domaine ciblé seront classés dans la catégorie des logiciels indésirables. Avant la version de contenu 8206, le pare-feu plaçait les logiciels indésirables dans la catégorie des URL malveillantes ou douteuses. Si vous n'êtes pas certain de devoir bloquer les logiciels indésirables, commencez par placer des alertes à l'égard des logiciels indésirables et enquêter sur les alertes, puis décider si vous devez bloquer les logiciels indésirables ou continuer à recevoir des alertes à leur égard.
- **dynamic-DNS (DNS dynamique)** : noms d'hôtes et de domaines de systèmes dont les adresses IP sont dynamiquement attribuées et qui sont souvent utilisés pour transmettre des charges utiles malveillantes ou du trafic C2. De plus, les domaines DNS dynamiques ne passent pas par le même processus de contrôle que les domaines qui sont enregistrés par une société spécialisée dans l'enregistrement de noms de domaine qui est digne de confiance ; ils sont dont moins fiable.
- **Unknown (inconnu)** : sites qui n'ont pas encore été identifiés par PAN-DB. Si la disponibilité est importante pour votre entreprise et que vous devez autoriser le trafic, demandez qu'une

alerte soit envoyée en présence de sites inconnus, appliquez au trafic les profils de sécurité recommandés et enquêtez sur les alertes.

> *Les mises à jour en temps réel de PAN-DB prennent connaissance des sites inconnus après la première tentative d'accès à ces derniers. Les URL inconnues sont donc identifiées rapidement et deviennent des URL connues que le pare-feu peut gérer en fonction de la véritable catégorie d'URL.*

- **newly-registered-domain (domaine nouvellement enregistré)** : les domaines nouvellement enregistrés sont souvent générées volontairement ou par les algorithmes de génération de domaines et utilisés pour mener des activités malveillantes.
- **Copyright-infringement (infraction au droit d'auteur)** : domaines dont le contenu est illégal, par exemple du contenu qui permet le téléchargement illégal de logiciels ou d'autres propriétés intellectuelles, ce qui présente un risque de responsabilité eventuel. Cette catégorie a été ajoutée pour assurer le respect des lois en matière de protection des enfants au sein de l'industrie de l'éducation ainsi que des lois des pays qui exigent que les fournisseurs Internet empêchent les utilisateurs de partager du matériel protégé par des droits d'auteur via leur service.
- **Extremism (extrémisme)** : les sites Web faisant la promotion du terrorisme, du racisme, du fascisme ou d'autres points de vue extrémistes discriminant des gens ou des groupes d'origines ethniques différentes, d'autres religions ou d'autres croyances. Cette catégorie a été ajoutée pour assurer le respect des lois en matière de protection des enfants au sein de l'industrie de l'éducation. Dans certaines régions, les lois et règlements peuvent interdire l'accès aux sites extrémistes, et l'autorisation de l'accès peut présenter un risque de responsabilité.
- **proxy-avoidance-and-anonymizers (contournement des proxy et anonymiseurs)** : URL et services qui sont souvent utilisés pour contourner des produits de filtrage de contenu.
- **douteux** : sites web contenant de l'humour de mauvais goût, des contenus offensants ciblant des groupes ou des individus spécifiques.
- **parked (en parking)** : domaines enregistrés par des personnes ; on découvre souvent plus tard qu'ils ont servi à usurper des informations de connexion . Ces domaines peuvent ressembler à des domaines légitimes, par exemple, pal0alto0netw0rks.com ; ils servent toutefois à usurper des informations de connexion ou des informations personnelles. Il peut également s'agir de domaines pour lesquels une personne a acheté les droits dans l'espoir qu'un jour ils aient de la valeur, par exemple panw.net.

Pour les catégories pour lesquelles vous optez pour une alerte, plutôt que le blocage, vous pouvez contrôler très strictement la façon dont les utilisateurs interagissent avec le contenu du site. Par exemple, donnez aux utilisateurs l'accès aux ressources dont ils ont besoin (comme les blogs des développeurs à des fins de recherche ou aux services de stockage cloud), mais prenez les précautions suivantes pour réduire l'exposition aux menaces Web :

- Suivez les meilleures pratiques antispyware, en matière de protection contre les vulnérabilités et de blocage des fichiers. Une mesure de protection consisterait à bloquer les téléchargements de types de fichiers dangereux et à bloquer le JavaScript obscurs pour les sites pour lesquels vous optez pour les alertes.
- Ciblez le déchiffrement en fonction de la catégorie d'URL. Le déchiffrement des sites à risque élevé et à risque modéré serait un bon commencement.
- Affichez une page de réponse aux utilisateurs lorsqu'ils visitent des sites à risque élevé et à risque modéré. Avisez-les que le site auquel ils tentent d'accéder est potentiellement malveillant, et informez-les des précautions à prendre s'ils décident de poursuivre leur consultation du site.

- Mettez un terme au vol d'identifiants en empêchant les utilisateurs de soumettre leurs identifiants d'entreprise à des sites y compris ceux qui sont considérés à risque élevé et à risque modéré.

## Catégories d'URL vérifiées

Les URL qui sont vérifiées par Palo Alto Networks pour faire partie d'un groupe spécifique de catégories ne possèdent pas de niveau de risque associé ; les niveaux de risque ne sont applicables qu'aux URL qui n'ont ***pas*** été vérifiées. Les URL vérifiées dans certaines catégories (voir ci-dessous) sont considérées comme malveillantes et sont bloquées par défaut car l'accès à ces URL présente un risque qui dépasse un niveau acceptable pour la plupart des environnements. Les adresses IP privées (et les hôtes) sont uniques à l'environnement hôte et ne sont pas visibles pour PAN-DB ; par conséquent, une évaluation des risques n'est pas générée.

| Catégorie | Action par défaut |
|---|---|
| **Logiciel malveillant** | Bloquer |
| **Hameçonnage** | |
| **Commande et contrôle** | |
| **Grayware (Logiciel indésirable)** | |
| **Adresses IP privées** | Autorisées (aucune action par défaut) |

*Pour plus d'informations sur les catégories d'URL actuelles, reportez-vous à :* Liste complète des catégories de filtrage des URL de PAN-DB

## Actions de politiques que vous pouvez prendre en fonction de catégories d'URL

Sur le pare-feu, vous pouvez utiliser un profil de filtrage des URL pour spécifier la manière dont vous souhaitez appliquer les catégories d'URL. Par défaut, l'accès au site pour toutes les catégories d'URL est défini sur allow (autorisé) lorsque vous create a new URL Filtering profile (Créez un nouveau profil de filtrage des URL). Cela signifie que les utilisateurs peuvent consulter librement tous les sites et que le trafic n'est pas journalisé. Personnalisez le profil de filtrage des URL en décidant le type de **Site Access (Accès aux sites)** que vous souhaitez appliquer pour chaque catégorie. Pour prevent credential phishing (empêcher le hameçonnage des informations d'identification), vous pouvez autoriser ou refuser les **User Credential Submissions (Envois des informations d'identification de l'utilisateur)** selon la catégorie d'URL (par exemple, vous pouvez bloquer la soumission des informations d'identification de l'utilisateur aux sites présentant un risque modéré à élevé). Les utilisateurs peuvent toujours accéder à ces sites, mais ne peuvent y soumettre leurs identifiants d'entreprise.

Pour commencer à appliquer les actions que vous avez définies dans un filtrage des URL, vous devez associer le profil à une règle de politique de sécurité. Le pare-feu applique les actions du profil au trafic qui correspond à la règle de politique de sécurité (pour obtenir de plus amples renseignements, reportez-vous à la section Configuration du filtrage des URL).

*Apprenez-en davantage sur la configuration d'un Profil de filtrage des URL suivant les meilleures pratiques pour assurer une protection contre les URL qui ont été signalées comme hébergeant du contenu malveillant ou à risque.*

| Action | Description |
|---|---|
| Accès au site | |
| **alert (alerter)** | Le site Web est autorisé et une entrée de journal est créée dans le journal de filtrage des URL.<br><br>*Définissez **alert (alerter)** comme Action des catégories ou du trafic que vous ne bloquez pas pour le journaliser ou obtenir une visibilité du trafic.* |
| **allow (autoriser)** | Le site Web est autorisé et aucune entrée de journal n'est créée.<br><br>*Ne définissez pas **allow (autoriser)** comme Action des catégories ou du trafic que vous ne bloquez, car vous perdez la visibilité du trafic que vous ne journalisez pas. Optez plutôt pour l'option **alert (alerter)** comme Action des catégories ou du trafic que vous ne bloquez pas pour le journaliser ou obtenir une visibilité du trafic.* |
| **block** | Le site Web est bloqué, une page de réponse va s'afficher et l'utilisateur ne pourra pas continuer sa visite sur ce site Web. Une entrée de journal est créée dans le journal de filtrage des URL.<br><br>Le blocage de l'accès au site pour une catégorie d'URL définit également les envois des informations d'identification de l'utilisateur pour cette catégorie d'URL sur block (bloquer). |
| **continue (continuer)** | Une page de réponse va s'afficher en indiquant que le site a été bloqué en raison de la politique de sécurité de l'entreprise, mais l'utilisateur pourra choisir de continuer sa visite sur ce site Web. L'action **continue (continuer)** est généralement utilisée pour les catégories qui sont considérées comme étant bénignes et permet d'améliorer l'expérience utilisateur en lui permettant de continuer s'il estime que le site n'a pas été correctement catégorisé. Le message de la page de réponse peut être personnalisé afin d'inclure des informations spécifiques à votre entreprise. Une entrée de journal est créée dans le journal de filtrage des URL.<br><br>*La page Continue (Continuer) ne s'affiche pas correctement sur les machines client configurées pour utiliser un serveur proxy.* |

| Action | Description |
| --- | --- |
| **override (contrôle prioritaire)** | Une page de réponse va s'afficher en indiquant qu'un mot de passe est requis pour autoriser l'accès aux sites Web d'une catégorie donnée. Grâce à cette option, l'administrateur de sécurité ou l'employé du service de support doit fournir un mot de passe autorisant un accès temporaire à tous les sites Web d'une catégorie donnée. Une entrée de journal est créée dans le journal de filtrage des URL. Consultez Autoriser l'accès par mot de passe à certains sites.<br><br>Dans les versions antérieures. le contrôle prioritaire des catégories de filtrage des URL plaçait l'application de la politique devant les catégories d'URL personnalisées. Dans le cadre de la mise à niveau vers PAN-OS 9.0, les contrôles prioritaires des catégories sont convertis en catégories d'URL personnalisées. L'application de la politique n'est plus prioritaire par rapport aux catégories d'URL personnalisées. Plutôt que l'action que vous avez définie pour le contrôle prioritaire des catégories dans les versions précédentes, la nouvelle catégorie d'URL personnalisée est appliquée par la règle de politique de sécurité disposant de l'action du profil de filtrage des URL la plus stricte. De la plus stricte à la moins stricte, les actions du profil de filtrage des URL sont les suivantes : bloquer, appliquer un contrôle prioritaire, continuer, alerter et autoriser.<br><br>Cela signifie que, si vous appliquiez des contrôles prioritaires sur les catégories d'URL avec l'action autoriser, il se peut que les contrôles prioritaires soient bloqués après être convertis à la catégories d'URL personnalisée dans PAN-OS 9.0.<br><br>*La page Override (Remplacer) ne s'affiche pas correctement sur les machines client configurées pour utiliser un serveur proxy.* |
| **none (aucun)** | L'action **none (aucune)** s'applique uniquement aux catégories d'URL personnalisées. Sélectionner **none (aucune)** permet de s'assurer que, si plusieurs profils de filtrage d'URL existent, la catégorie personnalisée n'affecte pas les autres profils. Par exemple, si vous possédez deux profils de filtrage d'URL et que la catégorie d'URL personnalisée de l'un des profils est définie sur **block (bloquer)**, vous devez définir l'action sur **none (aucun)** si vous ne voulez pas que l'action de blocage s'applique à l'autre profil.<br><br>De plus, pour supprimer une catégorie d'URL personnalisée, elle doit être définie sur **none (aucune)** dans un profil que vous utilisez. |
| Autorisations relatives aux informations d'identification de l'utilisateur<br><br>*Ces paramètres exigent que vous set up credential phishing prevention (Configuriez la prévention du hameçonnage des informations d'identification) au préalable.* | |

| Action | Description |
|---|---|
| alert (alerter) | Permettez aux utilisateurs d'envoyer des informations d'identification professionnelles dans cette catégorie d'URL, mais générez un journal d'alerte de filtrage des URL chaque fois que cela se produit. |
| allow (par défaut) | Permettez aux utilisateurs d'envoyer des informations d'identification professionnelles dans cette catégorie d'URL. |
| block | Empêchez les utilisateurs d'envoyer des informations d'identification professionnelles dans cette catégorie. Une page de réponse anti-hameçonnage par défaut s'affiche pour les utilisateurs lorsqu'ils accèdent à des sites pour lesquels les envois d'informations d'identification professionnelles sont bloqués. Vous pouvez choisir de créer une page de blocage personnalisée à afficher. |
| continue (continuer) | Affiche une page de réponse aux utilisateurs qui les invite à sélectionner Continuer pour saisir des informations d'identification afin d'accéder au site. Par défaut, la page de poursuite anti-hameçonnage s'affiche pour l'utilisateur lorsqu'il accède à des sites pour lesquels les envois d'informations d'identification sont déconseillés. Vous pouvez également choisir de créer une page de réponse personnalisée à afficher, par exemple si vous souhaitez avertir les utilisateurs contre les tentatives de hameçonnage ou la réutilisation de leurs informations d'identification sur d'autres sites Web. |

# Planifiez votre déploiement de filtrage des URL

Pour commencer à déployer le Filtrage des URL dans votre réseau, nous vous recommandons de commencer par procéder à une configuration de base qui vous donnera une visibilité des tendances de son activité Web tout en bloquant le contenu malveillant confirmé :

- Commencez par un profil de filtrage des URL (pratiquement) passif qui envoie des alertes pour la plupart des catégories. Un tel profil vous donne une visibilité des sites auxquels vos utilisateurs accèdent. Vous pouvez donc décider ce que vous souhaitez autoriser, limiter et bloquer.
- Bloquez les catégories d'URL qui sont mauvaises : logiciels malveillants, C2 et hameçonnage.

Comme le signalement de toute l'activité Web peut créer une grande quantité de fichiers de journaux, vous pourriez décider de procéder ainsi lors du déploiement initial du filtrage des URL.

*À ce stade, vous pouvez également réduire le nombre de journaux de filtrage des URL en activant l'option **Log container page only (Page conteneur de journaux uniquement)** dans le profil de filtrage des URL. Seule la page principale correspondant à la catégorie sera alors journalisée, mais pas les pages/catégories suivantes pouvant être chargées dans la page conteneur.*

**STEP 1 |** À tout moment, vous pouvez utiliser Test A Site (Tester un site) pour voir comment PAN-DB, la base de données de filtrage des URL dans le cloud, catégorise une URL spécifique et pour découvrir toutes les catégories d'URL possibles.

Vous pouvez également utiliser un site de test A pour soumettre une demande de changement, si vous êtes en désaccord avec la catégorisation d'une URL donnée.

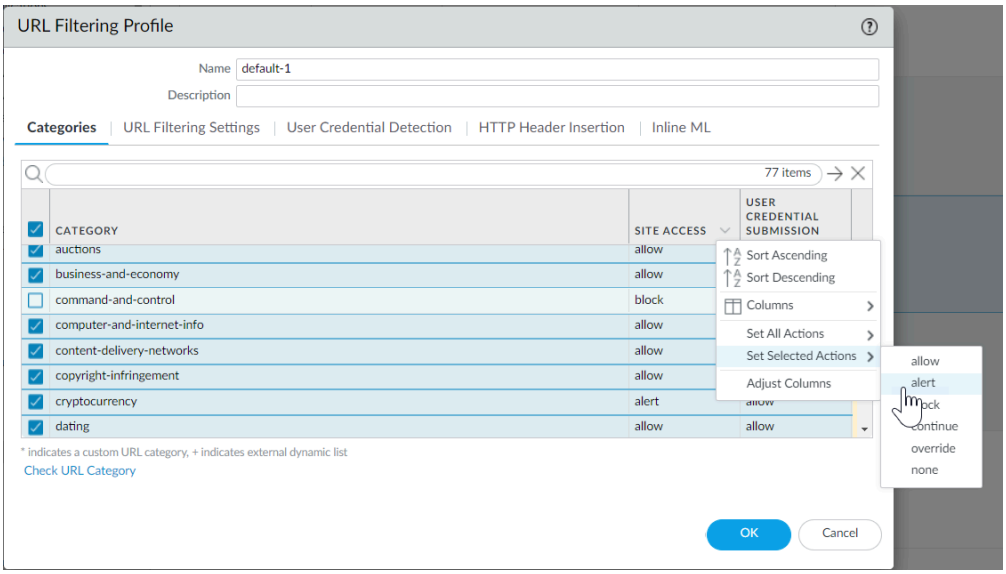
**STEP 2 |** Créez un profil de filtrage des URL passif qui envoie des alertes pour toutes les catégories et vous donne ainsi un aperçu de votre trafic Web.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profil de sécurité)>URL Filtering (Filtrage des URL)**.
2. Sélectionnez le profil par défaut, puis cliquez sur **Clone (Cloner)**. Le nouveau profil sera nommé **default-1 (default-1)**.
3. Sélectionnez le profil **défaut-1 (défaut-1)** et renommez-le. Par exemple, renommez-le Surveillance-URL.

**STEP 3 |** Configurez l'action sur **alert (alerter)** pour toutes les catégories, sauf pour les fichiers malveillants, la commande et contrôle et l'hameçonnage, qui doivent rester bloqués.

1. Dans la section qui répertorie toutes les catégories d'URL, sélectionnez toutes les catégories, puis désélectionnez les logiciels malveillants, la commande et le contrôle et le hameçonnage.
2. À droite de l'en-tête de la colonne ***Action (Action)***, cliquez sur la flèche vers le bas, puis sélectionnez **Set Selected Actions (Paramétrer les actions sélectionnées)** et **alert (alerter)**.




3. **Block (Bloquez)** l'accès aux catégories d'URL dangereuses.

   *Bloquez l'accès aux catégories d'URL suivantes : logiciels malveillants, phishing, DNS dynamiques, commandes et contrôles, extrémisme,violation des droits d'auteur, contournement des proxy et des anonymiseurs, domaine nouvellement enregistré, logiciel indésirable et URL en parking.*

4. Cliquez sur **OK** pour enregistrer le profil.

**STEP 4 |** Appliquez le profil de filtrage des URL à la ou aux Règles de politique de sécurité qui autorisent le trafic Web pour les utilisateurs.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et sélectionnez la politique de Sécurité adéquate pour la modifier.
2. Cliquez sur l'onglet **Actions (Actions)** puis, dans la section **Profile Setting (Paramètre de profil)**, cliquez sur la liste déroulante **URL Filtering (Filtrage des URL)** et sélectionnez le nouveau profil.
3. Cliquez sur **OK (OK)** pour enregistrer les paramètres.

**STEP 5 |** Enregistrer la configuration.

Cliquez sur **Commit (Valider)**.

**STEP 6 |** Affichez les journaux de filtrage des URL pour voir toutes les catégories de sites Web que consultent vos utilisateurs. Les catégories que vous avez décidé de bloquer sont également journalisées.

Pour plus d'informations sur l'affichage des journaux et la génération de rapports, reportez-vous à la section Surveillance de l'activité Web.

Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **URL Filtering (Filtrage des URL)**. Une entrée de journal sera créée pour tout site Web figurant dans la base de données de filtrage des URL et dont la catégorie est configurée sur une action autre que **allow (autoriser)**. Les rapports de filtrage des URL vous donnent un aperçu de l'activité Web qui s'est produite sur une période de 24 heures. ( **Monitor (Surveillance)** > **Reports (Rapports)**).

**STEP 7 |** Étapes suivantes :

- PAN-DB catégorise chaque URL avec un maximum de quatre catégories, et chaque URL comporte une catégorie de risque (élevé, modéré ou faible). Bien que le caractère malveillant des sites à risque élevé et modéré n'ait pas été confirmé, ils sont étroitement liés aux sites malveillants. Par exemple, ils peuvent se trouver sur le même domaine que des sites malveillants ou ont pu héberger du contenu malveillant jusqu'à tout récemment. Pour tout ce que vous n'autorisez pas ou ne bloquez pas, vous pouvez utiliser des catégories de risques pour rédiger une politique simple basée sur la sécurité des sites web.

  Vous pouvez prendre des mesures préventives pour restreindre l'interaction de vos utilisateurs avec les sites à risque élevé, car, dans certaines situations, vous pourriez vouloir accorder à vos utilisateurs un accès à des sites qui pourraient également poser des problèmes de sécurité (par exemple, vous pourriez autoriser vos développeurs à utiliser des blogues de développeurs à des fins de recherche, même si les blogues font partie des catégories qui hébergent fréquemment des logiciels malveillants).
- Associez le filtrage des URL avec User-ID pour contrôler l'accès Web en fonction de l'organisation ou du département et pour bloquer l'envoi d'identifiants d'entreprise à des sites non approuvés :
  - Le filtrage des URL empêche le vol des identifiants en détectant l'envoi d'identifiants d'entreprise à des sites en fonction de la catégorie de site. Empêchez les utilisateurs d'envoyer des informations d'identification à des sites malveillants et non validés, avertissez-les contre la saisie d'informations d'identification professionnelles sur des sites inconnus ou avertissez-les contre la réutilisation d'informations d'identification professionnelles sur des sites hors travail, et autorisez explicitement les utilisateurs à envoyer leurs informations d'identification sur les sites de l'entreprise.
  - Ajoutez ou mettez à jour une Règle de politique de sécurité à l'aide du profil de filtrage des URL passif, pour qu'elle s'applique à un groupe d'utilisateurs au sein d'un département, par exemple, le Marketing ou l'Ingénierie ( **Policies [Politiques]** > **Security [Sécuritaire]** > **User [Utilisateur]**). Surveillez l'activité du département et recueillez les commentaires des membres du département pour comprendre les ressources Web qui sont essentielles à leur travail.
- Songez à toutes les façons dont vous pouvez utiliser le filtrage des URL pour réduire votre surface d'attaque et contrôler l'utilisation Web. Par exemple, si vous êtes une école, vous pouvez utiliser le filtrage des URL pour appliquer des paramètres de recherche sécurisée rigoureux, où les moteurs de recherche filtrent et excluent les images et vidéos destinées aux adultes dans les résultats de recherche. Ou, si vous possédez un centre de gestion de la

sécurité, vous pourriez donner aux analystes des menaces un accès par mot de passe aux sites dangereux ou compromis à des fins de recherche, sites que vous ne voudriez pas autrement ouvrir à des équipes entières ou à toute l'organisation.

- Suivez les URL Filtering best practices (bonnes pratiques de filtrage d'URL).

# Bonnes pratiques en matière de filtrage des URL

Le filtrage des URL de Palo Alto Networks vous protège contre les menaces Web et vous procure une façon simple de surveiller l'activité Web et de la contrôler. Pour tirer le meilleur parti du filtrage des URL, vous devez commencer par créer des règles d'autorisation pour les applications desquelles vous dépendez pour exercer vos activités. Examinez ensuite les catégories d'URL qui classent le contenu malveillant et à risque. Nous vous recommandons ces types de catégories immédiatement. Ensuite, pour les autres types de contenus, ces bonnes pratiques peuvent vous servir de guide pour la réduction de votre exposition aux menaces Web, sans limiter l'accès de vos utilisateurs au contenu Web dont ils ont besoin.

- Avant de commencer à utiliser le filtrage des URL, identifiez les applications que vous souhaitez autoriser et créez des règles d'autorisation des applications dans le cadre de l'élaboration d'une politique de sécurité des passerelles Internet.

  La liste des applications autorisées comprend non seulement les applications que vous obtenez et gérez à des fins d'infrastructure ou d'entreprise, mais également les autres applications que vos utilisateurs pourraient devoir utiliser pour accomplir leur travail ainsi que les applications que vous pourriez décider d'autoriser à des fins personnelles.

  Après que vous ayez identifié ces applications d'entreprise, vous pouvez utiliser le filtrage des URLs pour contrôler et sécuriser toute l'activité web qui n'est pas sur la liste d'autorisation.
- Obtenez de la visibilité de l'activité web de vos utilisateurs, afin que vous puissiez planifier la politique de filtrage URL la plus efficace pour votre entreprise, et la mettre en œuvre. Cela inclut:
  - À tout moment, vous pouvez utiliser un Test A Site pour voir comment PAN-DB, la base de données de filtrage des URL dans le cloud, catégorise une URL spécifique et pour découvrir toutes les catégories d'URL possibles.
  - Commencez par un profil de filtrage des URL (pratiquement) passif qui envoie des alertes pour la plupart des catégories. Un tel profil vous donne une visibilité des sites auxquels vos utilisateurs accèdent. Vous pouvez donc décider ce que vous souhaitez autoriser, limiter et bloquer.
  - Surveillez l'activité web pour évaluer les sites que vous utilisateurs accèdent et voir s'ils sont alignés avec vos besoins métier.
- Bloquer les catégories d'URLs qui correspondent à du contenu malicieux ou d'exploitations. Bien que nous sachions que ces catégories sont dangereuses, gardez toujours à l'esprit que les catégories d'URLs que vous décidez de bloquer peuvent dépendre de vos besoins métier.
- Vous pouvez également utiliser les catégories d'URL pour introduire graduellement le déchiffrement, et pour exclure les catégories d'URL qui peuvent contenir des renseignements sensibles ou personnels du déchiffrement (comme les sites relatifs à des services financiers et à la santé et aux médicaments).

  Prévoyez de déchiffrer le trafic le plus à risque dans un premier temps (catégories d'URL les plus susceptibles de contenir du trafic malveillant, comme les jeux ou à risque élevé), puis d'en déchiffrer davantage lorsque vous acquérez de l'expérience. Vous pouvez éventuellement déchiffrer les catégories d'URL qui n'affectent pas votre entreprise dans un premier temps (si quelque chose ne se passe pas comme prévu, cela n'affecte pas l'entreprise), par exemple, de nouveaux flux d'informations. Dans les deux cas, déchiffrez quelques catégories d'URL, tenez compte des commentaires des utilisateurs, exécutez les rapports pour vous assurer que le

déchiffrement fonctionne comme prévu, puis déchiffrez progressivement quelques catégories d'URL supplémentaires, etc. Planifiez de faire des exclusions de déchiffrement pour exclure les sites du déchiffrement, si vous ne pouvez les déchiffrer pour des raisons techniques ou parce que vous choisissez de ne pas les déchiffrer.

***Affiner le déchiffrement en fonction des catégories d'URLs est aussi une bonne pratique du** Décryptage*.

- Prevent credential theft (Évitez le vol des identifiants) en activant la détection des soumissions d'informations d'identification d'entreprise aux sites par le pare-feu, puis contrôlez ces soumissions en fonction de la catégorie d'URL. Empêchez les utilisateurs d'envoyer des informations d'identification à des sites malveillants et non validés, avertissez-les contre la saisie d'informations d'identification professionnelles sur des sites inconnus ou contre la réutilisation d'informations d'identification professionnelles sur des sites hors travail, et autorisez explicitement les utilisateurs à envoyer leurs informations d'identification sur les sites de l'entreprise et les sites validés.
- Bloquez les variantes malveillantes des exploits JavaScript et des attaques de hameçonnage en temps réel. L'activation de Filtrage des URL Inline ML vous permet d'analyser dynamiquement des pages web en utilisant l'apprentissage machine sur le pare-feu.
- Déchiffrer, inspecter et limiter strictement comment les utilisateurs interagissent avec le high-risk and medium-risk content (contenu à haut et moyen risque) (si vous décidez de ne bloquer aucune de ces malicious URL categories (catégories d'URL malveillantes) pour des raisons commerciales, vous devriez aussi limiter strictement les interactions des utilisateurs avec ces catégories

  Le contenu web que vous approuvez et les catégories d'URLs malicieuses que vous bloquer sont juste une portion de l'ensemble du trafic web Le reste du contenu auquel accèdent vos utilisateurs est une combinaison de contenu bénin (risque faible) et contenu risqué (haut et moyen risque). Bien que le caractère malveillant des sites à risque élevé et modéré n'ait pas été confirmé, ils sont étroitement liés aux sites malveillants. Par exemple, une URL à haut risque peut être du même domaine qu'un site malicieux, ou peut avoir héberger du contenu malicieux par le passé.

  Cependant, beaucoup des sites qui représentent un risque pour votre entreprise peuvent aussi fournir des services et ressources intéressantes à vos utilisateurs (les services de stockage Cloud sont un bon exemple) Bien que ces ressources et services soient nécessaires pour le métier, ils peuvent aussi vraisemblablement être utilisé lors d'une cyberattaque. Voici comment contrôler comment les utilisateurs interagissent avec ce contenu potentiellement dangereux, tout en fournissant une bonne expérience utilisateur :

  - Dans un profil de filtrage des URLs, configurez les catégories haut risque et moyen risque à **continue** pour afficher une page de réponse qui avertit les utilisateurs lorsqu'ils visitent un site potentiellement dangereux. Conseillez-les sur comment prendre leurs précautions s'ils décident de poursuivre sur le site. Si vous ne souhaitez pas afficher une page de réponse pour vos utilisateurs, alertez sur le contenu à haut et moyen risque à la place.
  - Décryptez les sites à risque élevé et à risque modéré.
  - Suivez les bonnes pratiques antispyware, en matière de protection contre les vulnérabilités et de blocage des fichiers. Une mesure de protection consisterait à bloquer les téléchargements de types de fichiers dangereux et à bloquer le JavaScript obscurs pour les sites pour lesquels vous optez pour les alertes.

- Mettez un terme au vol d'identifiants en empêchant les utilisateurs de soumettre leurs identifiants d'entreprise à des sites y compris ceux qui sont considérés à risque élevé et à risque modéré.

- Les écoles et les institutions de l'éducation peuvent utilisé une imposition de la recherche sécurisée pour être certains que les moteurs de recherchent filtrent les contenus d'images et de vidéos pour adultes dans les résultats de recherche. Activation de la mise en œuvre de la recherche sécurisée transparente
- Configurez le pare-feu pour mettre en attente la requête web initiale pendant qu'il fait une recherche de catégorie d'URL avec PAN-DB

  Quand un utilisateur visite un site web, un pare-feu avec filtrage des URL activé vérifie son cache local de catégories des URLs pour catégoriser le site Si le pare-feu ne trouve pas la catégorie d'URL dans le cache, il effectue une interrogation avec PAN-DB, la base de données d'URLs de Palo Alto Networks. Par défaut, le pare-feu autorise la requête web de l'utilisateur pendant cette interrogation du cloud, et applique la politique quand le serveur répond.

  Mais si vous choisissez de mettre en attente les requêtes web, le pare-feu bloque la requête jusqu'à qu'il trouve la catégorie d'URL ou si elle expire. Si l'interrogation expire, le pare-feu choisit la catégorie URL non-résolu

  1. Dans **Device** > **Setup** > **Content-ID**, cocher la case pour

     **Garder en mémoire la demande du client pour la recherche de catégorie**.

# Activation de PAN-DB

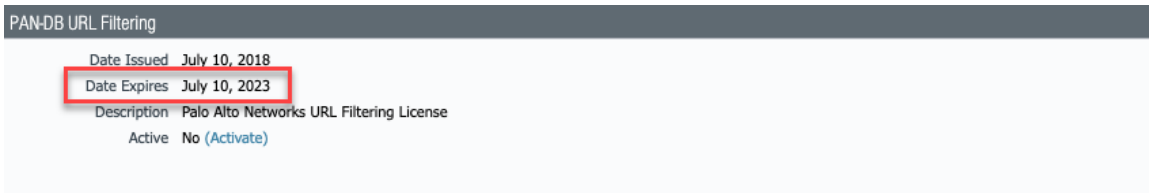
La base de données de filtrage des URL développée par Palo Alto Networks, PAN-DB, permet une mise en cache locale hautes performances pour des performances en ligne optimale lors de recherches d'URL, et protège contre les URL et adresses IP malveillantes. Lorsque WildFire identifie des logiciels malveillants inconnus, des utilisations du jour zéro et des advanced persistent threats (menaces persistantes avancées ; APT), la base de données PAN-DB est mise à jour avec des informations sur les URL malveillantes afin que vous puissiez bloquer les téléchargements de logiciels malveillants, et désactiver des communications Commande et contrôle (C2) pour protéger votre réseau contre les cyber-menaces. Les catégories d'URL qui identifient le contenu malveillant confirmé (logiciels malveillants, hameçonnage et C2) sont mises à jour toutes les cinq minutes, pour que vous puissiez gérer l'accès à ces sites dans les minutes qui suivent leur catégorisation.

*Si vous avez acheté une licence de filtrage d'URL avancé, qui permet également d'accéder à PAN-DB et au filtrage d'URL en ligne ML, il n'est pas nécessaire d'installer les licences supplémentaires séparément. L'installation de la licence de filtrage d'URL avancé active automatiquement le service pour tous les services d'abonnement contenus dans le package.*

**STEP 1 |** Procurez-vous et installez une licence de filtrage des URL PAN-DB et vérifiez qu'elle est installée.

*En cas d'expiration de la licence, le pare-feu cesse d'effectuer le filtrage des URL PAN-DB. L'application de la catégorie d'URL, les recherches d'URL dans le Cloud et les autres mises à jour basées sur le Cloud ne fonctionneront pas jusqu'à l'installation d'une licence valide.*

1. Sélectionnez **Device (Périphérique)** > **Licenses (Licences)**, puis, dans la section License Management (Gestion des licences), sélectionnez la méthode d'installation de la licence :
   - **Retrieve license keys from license server (Récupérer les clés de licence auprès du serveur de licences)**
   - **Activate feature using authorization code (Activer la fonction à l'aide du code d'autorisation)**
   - **Manually upload license key (Charger manuellement la clé de licence)**
2. Après avoir installé la licence, vérifiez, dans la section PAN-DB URL Filtering (Filtrage des URL PAN-DB), que le champ **Date Expires (Date d'expiration)** affiche une date valide.

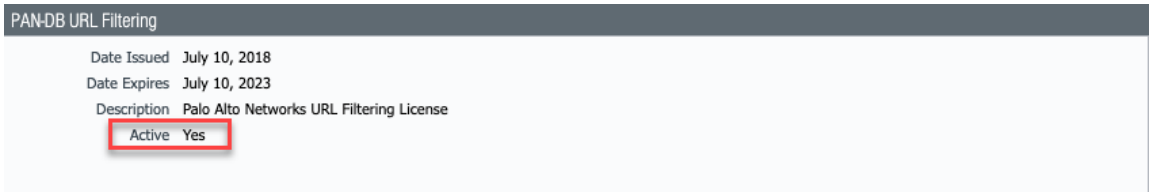


**STEP 2 |** Activez le filtrage des URL PAN-DB.

*PAN-OS 9.0 et les versions ultérieures ne téléchargent pas les bases de données PAN-DB initiales. Au lieu, lors de l'activation de la licence de filtrage des URL, le pare-feu remplit le cache au fur et à mesure que les requêtes d'URL sont transmises.*

1. Cliquez sur **Activate (Activer)**. La valeur qui s'affiche dans le champ Active (Actif) passe à Yes (Oui).




**STEP 3 |** Planifiez le pare-feu pour télécharger les mises à jour dynamiques des applications et des menaces.

*Une licence Threat Prevention est requise pour recevoir les mises à jour du contenu, notamment de l'antivirus, des applications et menaces.*

1. Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**.
2. Dans le champ Schedule (Programmer) de la section Applications and Threats (Applications et menaces), cliquez sur le lien **None (Aucune)** pour planifier des mises à jour périodiques.

   *Vous ne pouvez planifier des mises à jour dynamiques que si le pare-feu dispose d'un accès direct à Internet. Si des mises à jour sont déjà planifiées dans une section, le texte du lien affiche les paramètres de la planification.*

   Les mises à jour des applications et menaces contiennent parfois des mises à jour pour le filtrage des URL liées à la Mise en œuvre de la recherche sécurisée.

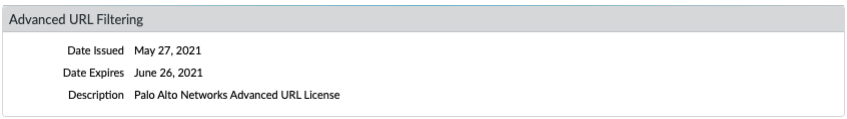
# Activer le filtrage d'URL avancé

L'abonnement de filtrage d'URL avancé de Palo Alto Networks fournit une analyse d'URL en temps réel et une prévention des logiciels malveillants, en plus des recherches d'URL PAN-DB locales, pour permettre une solution de protection multicouche. La configuration de Filtrage d'URL avancé est définie par votre profil de filtrage d'URL. L'installation de la licence de filtrage d'URL avancé active automatiquement le service pour tous les services d'abonnement contenus dans le package.

**STEP 1 |** Procurez-vous et installez une licence de filtrage des URL avancée et vérifiez qu'elle est installée.

*La licence Advanced URL Filtering inclut l'accès à PAN-DB ; si la licence expire, le pare-feu cesse d'effectuer toutes les fonctions de filtrage d'URL, d'application de catégorie d'URL et de recherche d'URL dans le cloud. De plus, toutes les autres mises à jour basées sur le cloud ne fonctionneront pas tant que vous n'aurez pas installé une licence valide.*

1. Sélectionnez **Device (Périphérique)** > **Licenses (Licences)**, puis, dans la section License Management (Gestion des licences), sélectionnez la méthode d'installation de la licence :
   - **Retrieve license keys from license server (Récupérer les clés de licence auprès du serveur de licences)**
   - **Activate feature using authorization code (Activer la fonction à l'aide du code d'autorisation)**
2. Après avoir installé la licence, vérifiez, dans la section Advanced URL Filtering (Filtrage des URL avancé), que le champ **Date Expires (Date d'expiration)** affiche une date valide.




*Lorsque vous activez la licence de filtrage d'URL avancé, vos droits de licence pour PAN-DB et le filtrage d'URL avancé peuvent ne pas s'afficher correctement sur le pare-feu - il s'agit d'une anomalie d'affichage, pas d'un problème de licence et n'affecte pas l'accès aux services. Vous pouvez mettre à jour les licences sur le pare-feu pour rectifier le problème d'affichage à l'aide de la commande CLI suivante :* ***`request license fetch`***.

**STEP 2 |** Download and install the latest PAN-OS content release (Téléchargez et installez la dernière version du contenu PAN-OS). La version de contenu PAN-OS Applications and Threats 8390-6607 et versions ultérieures permet aux pare-feu exécutant PAN-OS 9.x et versions ultérieures d'identifier les URL qui ont été catégorisées à l'aide de la nouvelle catégorie de détection en temps réel, en identifiant les URL classées par filtrage d'URL avancé. Pour plus d'informations sur la mise à jour, reportez-vous aux Notes de mise à jour des applications et du contenu de menace. Vous pouvez également lire la section Content Release Notes for apps and threats (Notes de version des signatures d'applications et de menaces) sur le portail d'assistance de Palo Alto Networks ou directement dans l'interface Web du pare-feu : sélectionnez **Device**

**(Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)** et ouvrez les Release Note (Notes de version) concernant une version de contenu donnée.

*Suivez les* Best Practices for Applications and Threats Content Updates (Meilleures pratiques pour les mises à jour du contenu de menace et des applications) *lors de la mise à jour vers la dernière version de contenu.*

**STEP 3 |** Planifiez le pare-feu pour télécharger les mises à jour dynamiques des applications et des menaces.

*Une licence Threat Prevention est requise pour recevoir les mises à jour du contenu, notamment de l'antivirus, des applications et menaces.*

1. Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**.
2. Dans le champ Schedule (Programmer) de la section Applications and Threats (Applications et menaces), cliquez sur le lien **None (Aucune)** pour planifier des mises à jour périodiques.

   *Vous ne pouvez planifier des mises à jour dynamiques que si le pare-feu dispose d'un accès direct à Internet. Si des mises à jour sont déjà planifiées dans une section, le texte du lien affiche les paramètres de la planification.*

   Les mises à jour des applications et menaces contiennent parfois des mises à jour pour le filtrage des URL liées à la Mise en œuvre de la recherche sécurisée.

**Étapes suivantes :**

1. Configure a URL filtering profile (Configurez un profil de filtrage d'URL) pour définir les politiques d'utilisation du Web de votre organisation.
2. Verify your advanced URL filtering configuration (Vérifiez votre configuration de filtrage d'URL avancé)

# Vérifier le filtrage d'URL avancé

Vérifiez que le filtrage d'URL avancé analyse les URL.

*Palo Alto Networks recommande de définir le paramètre d'action de détection en temps réel pour alerter de vos profils de filtrage d'URL actifs. Cela offre une visibilité sur les URL analysées en temps réel et bloque (ou autorise, en fonction de vos paramètres de stratégie) en fonction des paramètres de catégorie configurés pour des menaces Web spécifiques. L'action entreprise sur une URL est basée sur l'action la plus sévère pour une catégorie qui a été détectée pour une URL donnée. Par exemple, si example.com est classé comme détection en temps réel, commande et contrôle et achats ; et les actions configurées sont alerter, bloquer et autoriser, respectivement, l'URL sera bloquée car elle est considérée comme l'action la plus sévère parmi les catégories détectées.*

Vérifiez que les URL sont analysées et classées à l'aide du service avancé de filtrage d'URL.

1. Accédez à chacune des URL de test suivantes pour vérifier que le service de filtrage d'URL avancé catégorise correctement les URL :
   - **Malware (logiciel malveillant)**—urlfiltering.paloaltonetworks.com/test-real-time-detection-malware
   - **Phishing (Hameçonnage)**—urlfiltering.paloaltonetworks.com/test-real-time-detection-phishing
   - **C2**—urlfiltering.paloaltonetworks.com/test-real-time-detection-command-and-control
   - **Grayware**—urlfiltering.paloaltonetworks.com/test-real-time-detection-grayware
   - **Benign (unknown) (Bénigne (inconnu))**—urlfiltering.paloaltonetworks.com/test-real-time-detection
2. Surveillez l'activité sur le pare-feu pour vérifier que les URL ci-dessus ont été correctement classées comme détection en temps réel.
   1. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **URL Filtering (Filtrage des URL)**

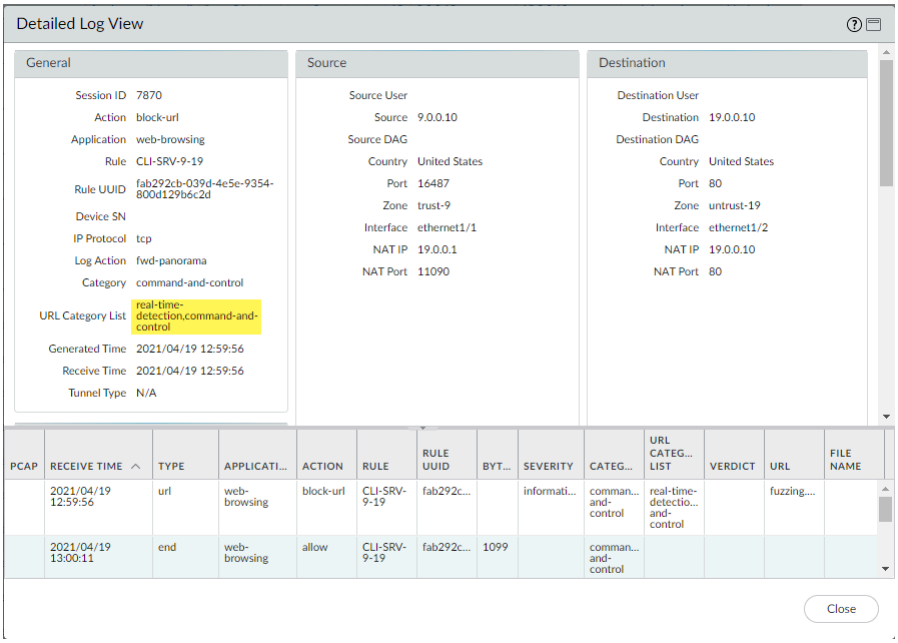
      ( url_category_list contains real-time-detection )

      | | RECEIVE TIME | CATEGORY | URL CATEGORY LIST | URL | FROM ZONE | TO ZONE | SOURCE | DESTINATION | APPLICATION | ACTION |
      |---|---|---|---|---|---|---|---|---|---|---|
      | | 04/19 13:00:08 | phishing | real-time-detection,phishing | fuzzing.me/fakeverdict/junophishing... | trust-9 | untrust-19 | 9.0.0.10 | 19.0.0.10 | web-browsing | block-url |
      | | 04/19 13:00:02 | malware | real-time-detection,malware | fuzzing.me/fakeverdict/junomalwar... | trust-9 | untrust-19 | 9.0.0.10 | 19.0.0.10 | web-browsing | block-url |
      | | 04/19 12:59:56 | command-and-control | real-time-detection,command-and-control | fuzzing.me/fakeverdict/junoc2/test | trust-9 | untrust-19 | 9.0.0.10 | 19.0.0.10 | web-browsing | block-url |
      | | 04/19 12:55:48 | command-and-control | real-time-detection,command-and-control | fuzzing.me/fakeverdict/junoc2 | trust-9 | untrust-19 | 9.0.0.10 | 19.0.0.10 | web-browsing | block-url |
      | | 04/19 12:55:46 | command-and-control | real-time-detection,command-and-control | fuzzing.me/fakeverdict/junoc2 | trust-9 | untrust-19 | 9.0.0.10 | 19.0.0.10 | web-browsing | block-url |

      et filtrez par `(url_category_list contains real-time-detection)` pour afficher les journaux qui ont été analysés à l'aide du filtrage d'URL avancé. Des correspondances de catégories de pages Web supplémentaires sont également affichées et correspondent aux catégories définies par PAN-DB.
   2. Examinez en détail les journaux pour vérifier que chaque type de menace Web est correctement analysé et catégorisé. Dans l'exemple ci-dessous, l'URL est classée comme ayant été analysée en temps réel et, en outre, comme possédant des qualités qui la définissent comme commande et contrôle. Parce que C&C a une action plus sévère par

rapport à la détection en temps réel (blocage par opposition à alerte), cette URL a été classée comme commande et contrôle et a été bloquée.



# Configuration du filtrage des URL

Après avoir determine URL Filtering policy requirements (Défini des exigences d'une politique de filtrage des URL), vous devriez être capable d'identifier sommairement les types et catégories de sites Web que consultent vos utilisateurs. Grâce à ces informations, vous êtes désormais prêt à créer des profils de Filtrage des URL personnalisés et à les associer à la ou aux règles de politique de sécurité qui autorisent l'accès au Web. En plus de gérer l'accès Web au moyen d'un profil de filtrage des URL, et si User-ID est configuré, vous pouvez également gérer les sites auxquels les utilisateurs peuvent transmettre les informations d'identification d'entreprise.

**STEP 1 |** Créez un profil de filtrage des URL.

***Configurez un** Profil de filtrage des URL suivant les meilleures pratiques **pour assurer une protection contre les URL qui ont été signalées comme hébergeant du contenu malveillant ou à risque.***

Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de Sécurité)** > **URL Filtering (Filtrage des URL)** et **Add (Ajouter)** ou modifiez un profil de filtrage des URL.

**STEP 2 |** Définir l'accès au site pour chaque catégorie d'URL.

Sélectionnez **Categories (Catégories)**, puis définissez l'accès aux sites pour chaque catégorie d'URL :

- **allow (autorise)** le trafic destiné pour cette catégorie d'URL, le trafic autorisé n'est pas journalisé
- Sélectionnez **alert (alerter)** afin d'avoir une visibilité des sites auxquels vos utilisateurs accèdent. Le trafic correspondant est autorisé, mais un journal de filtrage des URL est généré pour journaliser les situations où un utilisateur accède à un site appartenant à cette catégorie.
- Sélectionnez **block (bloquer)** pour refuser l'accès au trafic correspondant à la catégorie et pour activer la journalisation du trafic bloqué.
- Sélectionnez **continue (continuer)** et une page d'avertissement s'affichera et demandera aux utilisateurs de cliquer sur **Continue (Continuer)** pour accéder à un site appartenant à cette catégorie.
- Pour n'autoriser l'accès que si les utilisateurs fournissent un mot de passe configuré, sélectionnez **override (contrôle prioritaire)**. Pour obtenir de plus amples précisions sur ce paramètre, reportez-vous à la section Autoriser l'accès par mot de passe à certains sites.

**STEP 3 |** Configurez le profil de filtrage des URL afin qu'il détecte les saisies de noms d'utilisateurs d'entreprise valides sur des catégories d'URL autorisées.

*Le pare-feu saute automatiquement la vérification de l'envoi des informations d'identification pour les APP-ID associés à des sites qui n'ont jamais hébergé de contenu malveillant ou de hameçonnage afin d'assurer un rendement optimal et un faible taux de faux positifs, et ce, même si vous activez les vérifications dans la catégorie correspondante. La liste des sites que le pare-feu ignorera lors de ses contrôles d'informations d'identification est mise à jour de manière automatique à travers les mises à jour d'applications et de menaces.*

1. Sélectionnez **User Credential Detection (Détection des informations d'identification de l'utilisateur)**.
2. Sélectionnez l'une des methods to check for corporate credential submissions (Méthodes de vérification des saisies d'informations d'identification d'entreprise) sur les pages web dans la liste déroulante**User Credential Detection (Détection des informations d'identification de l'utilisateur)** :
   - **Use IP User Mapping (Utiliser le mappage des adresses IP aux utilisateurs)** : cherche des envois de noms d'utilisateur d'entreprise valides et vérifie que le nom d'utilisateur correspond à l'utilisateur connecté à l'adresse IP source de la session. Le pare-feu fait correspondre le nom d'utilisateur saisi à la table de mappage adresse IP / nom d'utilisateur. Vous pouvez utiliser n'importe laquelle des méthodes de mappage d'utilisateur décrites dans Map IP Addresses to Users (Mappage d'adresses IP à des utilisateurs).
   - **Use Domain Credential Filter (Utiliser le filtrage par informations de domaine)** : Contrôle les saisies de noms d'utilisateurs d'entreprise et mots de passe valides et vérifie que le nom d'utilisateur correspond à l'utilisateur connecté à l'adresse IP source de la session. Reportez-vous à la section Configuration du mappage d'utilisateur à l'aide de l'agent User-ID Windows pour obtenir les directives sur la configuration de User-ID afin de pouvoir utiliser cette méthode.
   - **Use Group Mapping (Utiliser le mappage de groupe)** : contrôle les saisies de nom d'utilisateur valide basé sur la table de mappage d'utilisateurs à des groupes renseignée quand vous configurez le pare-feu pour le map users to groups (Mappage d'utilisateurs à des groupes).

     Avec le mappage de groupe, vous pouvez appliquer la détection des informations d'identification à **any (toute)** partie du répertoire, ou à un groupe spécifique, comme le département informatique qui aura accès à vos applications les plus sensibles.

     *Cette méthode peut entrainer des faux positifs dans des environnements qui n'ont pas d'identifiants uniquement structurés, donc vous devriez n'utiliser cette méthode que pour protéger vos comptes utilisateurs les plus sensibles*
3. Sélectionnez le **Degré de gravité d'enregistrement des détections de nom d'utilisateur valide** que le pare-feu utilise pour consigner la détection des saisies d'informations d'identification d'entreprise.

**STEP 4 |** Configurez le profil de filtrage des URL pour détecter le phishing et les JavaScript malveillants en temps réel en utilisant Filtrage des URL Inline ML.

**STEP 5 |** Autorisez ou empêcher les utilisateurs de soumettre des informations d'identification d'entreprise à des sites, selon la catégorie d'URL afin d'prevent credential phishing (empêcher l'hameçonnage des informations d'identification).

> ***Le pare-feu saute automatiquement la vérification de l'envoi des informations d'identification pour les APP-ID associés à des sites qui n'ont jamais hébergé de contenu malveillant ou de hameçonnage afin d'assurer un rendement optimal et un faible taux de faux positifs, et ce, même si vous activez les vérifications dans la catégorie correspondante. La liste des sites que le pare-feu ignorera lors de ses contrôles d'informations d'identification est mise à jour de manière automatique à travers les mises à jour d'applications et de menaces.***

1. Pour chaque catégorie d'URL à laquelle le **Site Access (Accès au site)** est autorisé, sélectionnez l'option **User Credential Submissions (Envoi des informations d'identification de l'utilisateur)** à appliquer :
   - **alert (alerter)** : autorise les utilisateurs à saisir des informations d'identification sur le site Web, mais génère un journal d'alerte de Filtrage des URL chaque fois qu'un utilisateur saisit des informations d'identification sur les sites de cette catégorie d'URL.
   - **allow (autoriser)** (par défaut) – Autorise les utilisateurs à saisir des informations d'identification sur le site Web.
   - **block (bloquer)** : affiche la page de blocage anti-hameçonnage pour empêcher les utilisateurs de saisir des informations d'identification sur le site Web.
   - **continue (continuer)** : présente la Page de poursuite anti-hameçonnage pour demander aux utilisateurs de cliquer sur **Continuer** pour accéder au site.
2. Configurez le profil de filtrage des URL afin qu'il détecte les saisies de noms d'utilisateurs d'entreprise valides sur des catégories d'URL autorisées.

**STEP 6 |** Définissez des URL category exception lists (listes d'exceptions de catégories d'URL) pour préciser les sites Web qui doivent toujours être bloqué ou autorisé, quelle que soit leur catégorie d'URL.

Par exemple, pour réduire le nombre de journaux de filtrage URL, vous pouvez ajouter vos sites Internet à la liste d'autorisation, afin qu'aucun journal ne soit généré pour ces sites, ou s'il y a un site Internet qui est très utilisé et qui n'est pas en rapport avec le travail, vous pouvez ajouter ce site à la liste d'interdiction

Les actions de stratégie configurées pour les catégories d'URL personnalisées sont prioritaires sur les URL correspondantes dans les listes dynamiques externes.

Les éléments figurant dans la liste d'interdiction seront toujours bloqués, quelle que soit l'action attribuée à la catégorie associée, et les URL figurant dans la liste d'autorisation seront toujours autorisées.

Pour plus d'informations sur le format approprié et l'utilisation des caractères génériques, consultez les directives URL category exception list (Listes d'exceptions de catégories d'URL).

**STEP 7 |** Activer la mise en œuvre de la recherche sécurisée.

**STEP 8 |** Journalisez uniquement les Pages conteneur pour les événements de filtrage des URL.

1. Sélectionnez **URL Filtering Settings (Paramètres de filtrage des URL)**. L'option **Log container page only (Page conteneur de journaux uniquement)** est activée par défaut afin que seule la page principale correspondant à la catégorie soit consignée, mais pas les pages/catégories suivantes susceptibles d'être chargées dans la page conteneur.
2. Pour activer la journalisation de toutes les pages/catégories, décochez la case **Log container page only (Page conteneur de journaux uniquement)**.

**STEP 9 |** Activez la Journalisation de l'en-tête HTTP pour un ou plusieurs des champs d'en-tête HTTP pris en charge.

Sélectionnez **URL Filtering Settings (Paramètres de filtrage des URL)** et sélectionnez un ou plusieurs des champs suivants à journaliser :

- **User-Agent (Utilisateur-Agent)**
- **Referer (Référant)**
- **X-Forwarded-For**

**STEP 10 |** Enregistrez le profil de filtrage des URL et validez vos modifications.

1. Cliquez sur **OK**.
2. Cliquez sur **Commit (Valider)**.

**STEP 11 |** Testez la configuration de votre stratégie de Filtrage d'URL.

1. Accédez à un site Web dans la catégorie d'URL souhaitée et observez le comportement du pare-feu.

   Utilisez les URL Filtering Test Pages (pages de test de filtrage d'URL de Palo Alto Networks) (urlfiltering.paloaltonetworks.com/test-***<url-category>***) si vous souhaitez éviter d'accéder directement à un site. Palo Alto Networks propose des URL de test pour les catégories d'URL bénignes et malveillantes. Par exemple, pour tester votre politique de blocage des logiciels malveillants, visitez https://urlfiltering.paloaltonetworks.com/test-malware.
2. Consultez les journaux de trafic et de filtrage d'URL ( **(surveillance)** > **Logs (journaux)**) pour confirmer que la règle de politique correcte est consignée.

**STEP 12 |** Activer **Hold Client request for category lookup** pour bloquer les requêtes client quand le pare-feu effectue des recherches de catégorie URL

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Content ID**.
2. Sélectionnez **Garder en mémoire la demande du client pour la recherche de catégorie**.
3. Commit (Validez) vos modifications.

*Activez cette fonctionnalité comme une* bonne pratique de filtrage URL**.**

**STEP 13 |** Fixer le temps, en seconde, avant qu'une recherche de catégorie n'expire

1. Sélectionnez l'**icône de l'engrenage** > **Device (Périphérique)** > **Setup (Configuration)** > **Content ID (ID contenu)**.
2. Saisissez un numéro dans **Category lookup timeout (s) (Délai d'expiration pour le recherche de catégorie)**.
3. Cliquez sur **OK**.
4. Commit (Validez) vos modifications.

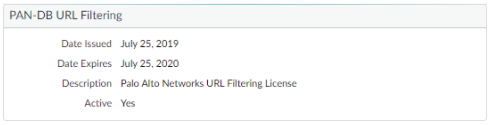
# Configuration du filtrage des URL Inline ML

Pour activer votre configuration de filtrage des URL Inline ML, attachez le profil de filtrage d'URL configuré avec les paramètres d'Inline ML à une règle de politique de sécurité (voir Configuration d'une politique de sécurité de base).

*Le filtrage des URL Inline ML n'est actuellement pas pris en charge sur l'appareil virtuel VM-50 ou VM50L.*

**STEP 1 |** Pour profiter du filtrage des URL Inline ML, vous devez avoir un abonnement actif au Filtrage des URL PAN-DB pour analyser les pages web à la recherche de menaces JavaScript et de phishing.

Vérifiez que vous disposez d'un abonnement au filtrage des URL PAN-DB. Pour vérifier les abonnements pour lesquels vous disposez de licences actuellement actives, sélectionnez **Device (Périphérique)** > **Licenses (Licences)** et vérifiez que les licences appropriées s'affichent et ne sont pas expirées.

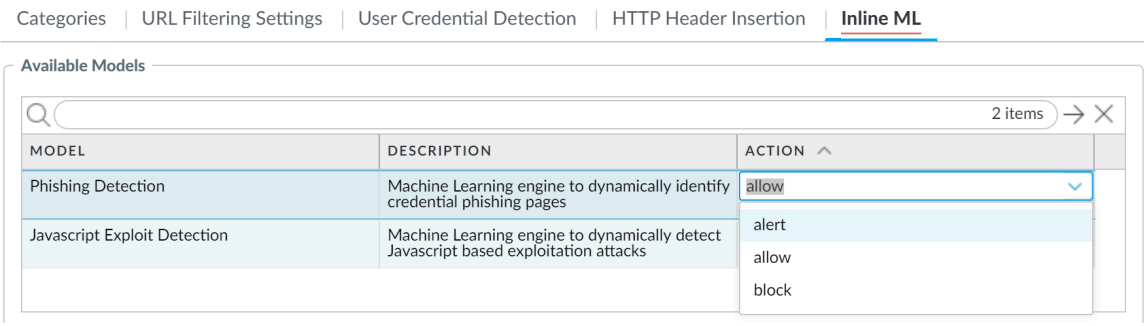



**STEP 2 |** Créez un nouveau profil de sécurité de Filtrage des URL ou mettez à jour vos profils existants pour utiliser le Filtrage des URL Inline ML.

1. Sélectionnez un **URL Filtering Profile (Profil de filtrage des URL)** existant ou **Add (Ajoutez)** un nouveau (**Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **URL Filtering (Filtrage des URL)**).
2. Sélectionnez **Inline ML** et définissez une **Action** de politique pour chaque modèle de filtrage des URL inline ML. Cela permet d'appliquer l'action de politique sélectionnée sur la base d'un modèle. Actuellement, il y a deux moteurs de classification disponibles : **Phishing** et **JavaScript Exploit (Exploitation de JavaScript)**, un pour chaque type de contenu de page web malveillante.
   - **Block (Blocage)** : lorsque le pare-feu détecte un site web avec un contenu de phishing, il génère une entrée de journal de filtrage des URL.
   - **Alert (Alerte)** : le pare-feu permet l'accès au site web mais génère également une entrée de journal de filtrage des URL.

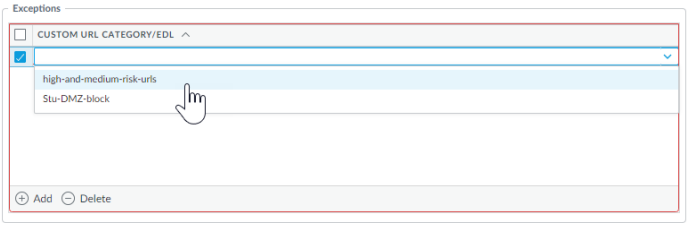
- **Allow (Autoriser)** : le pare-feu qui permet l'accès au site web ne génère pas d'entrée dans le journal du filtrage des URL.




3. Cliquez sur **OK** pour quitter la boîte de dialogue de configuration du profil de filtrage des URL et **Commit (Validez)** vos modifications.

**STEP 3 |** (Facultatif) Ajoutez des exceptions d'URL à votre profil de sécurité de filtrage des URL si vous rencontrez des faux positifs. Vous pouvez ajouter des exceptions en spécifiant une liste dynamique externe (EDL) à partir du profil de filtrage des URL ou en ajoutant une entrée de page web à partir des journaux de filtrage des URL.

- Ajoutez une liste dynamique externe d'exceptions d'URL.
  1. Sélectionnez **Objects (Objets) > Security Profiles (Profil de sécurité) > URL Filtering (Filtrage des URL)**.
  2. Sélectionnez un profil de filtrage des URL pour lequel vous souhaitez exclure des URL spécifiques, puis sélectionnez **Inline ML**.
  3. Cliquez sur **Add (Ajouter)** pour sélectionner une liste dynamique externe préexistante basée sur des URL. Si aucune n'est disponible, créez une nouvelle external dynamic list (liste dynamique externe).




  4. Cliquez sur **OK** pour enregistrer le profil de filtrage des URL et **Commit (Validez)** vos modifications.
- Ajout d'exceptions de fichier à partir des entrées de journal du filtrage des URL.
  1. Sélectionnez **Monitor (Moniteur) > Logs (Journaux) > URL Filtering (Filtrage des URL)** et filtrez les journaux pour les entrées d'URL avec un Verdict Inline ML **malicious-javascript (javascript malveillant)** ou **phishing**. Sélectionnez un journal de filtrage des URL pour une URL pour laquelle vous souhaitez créer une exception.

2. Accédez à **Detailed Log View (Vue détaillée du journal)** et faites défiler vers le bas jusqu'au volet **Details (Détails)** puis sélectionnez **Create Exception (Créer une exception)** situé à côté de **Inline ML Verdict (Verdict Inline ML**.


3. Sélectionnez une catégorie personnalisée pour l'exception d'URL et cliquez sur **OK**.
4. La nouvelle exception d'URL se trouve dans la liste à laquelle elle a été ajoutée, sous **Objects (Objets) > Custom Objects (Objets personnalisés) > URL Category (Catégorie d'URL)**.

**STEP 4 |** (Facultatif) Vérifiez l'état de la connectivité de votre pare-feu au service Inline ML dans le cloud.

Utilisez la commande CLI suivante sur le pare-feu pour afficher l'état de la connexion.

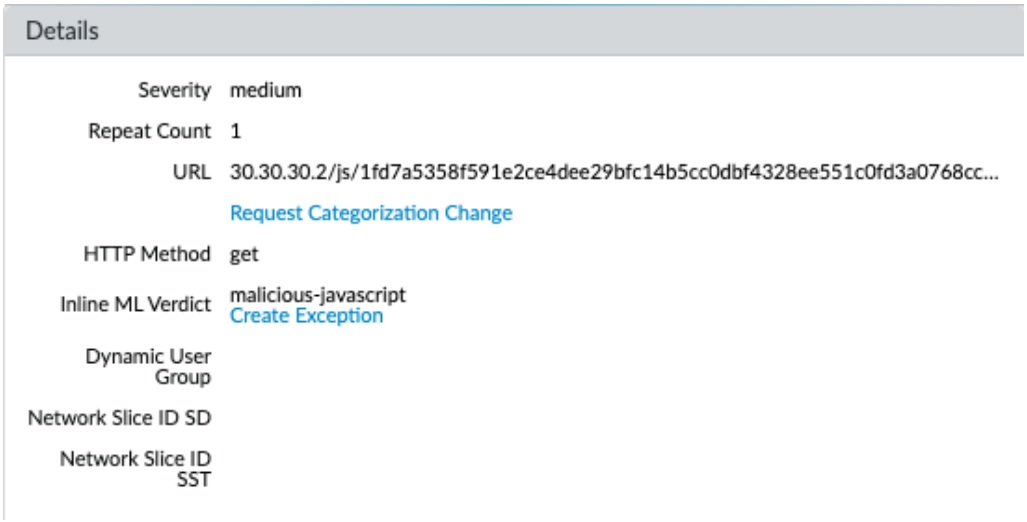
```
show mlav cloud-status
```

Par exemple :

```
show mlav cloud-status

MLAV cloud
Current cloud server:           ml.service.paloaltonetworks.com
Cloud connection:               connected
```

Si vous ne pouvez pas vous connecter au service cloud Inline ML, vérifiez que le domaine suivant n'est pas bloqué : ml.service.paloaltonetworks.com.

Pour afficher des informations sur les pages web qui ont été traitées à l'aide du filtrage des URL Inline ML, filtrez les journaux (**Monitor (Moniteur) > Logs (Journaux) > URL Filtering (Filtrage des URL)**) sur la base du **Inline ML Verdict (Verdict Inline ML)**. Les pages web dont il a été déterminé qu'elles contiennent des menaces sont classées par catégorie, avec des verdicts de **phishing** ou de **malicious-javascript (javascript malveillant)**. Par exemple :



# Tester la configuration du filtrage d'URL

Pour tester vos configurations de Filtrage d'URL et de Filtrage d'URL avancépolitique, utilisez les URL Filtering Test Pages (pages de test de filtrage d'URL) de Palo Alto Networks. Des pages de test ont été créées pour tester en toute sécurité toutes les predefined URL categories (catégories d'URL prédéfinies), y compris les catégories de détection en temps réel applicables uniquement aux pare-feu exécutant un filtrage d'URL avancé.

*Vous devez activer le déchiffrement SSL pour que les pages de test fonctionnent sur une connexion HTTPS.*

*Les pages de test de filtrage d'URL avancé contiennent une « détection en temps réel » dans l'URL et confirment que les pare-feu catégorisent et analysent correctement les URL malveillantes en temps réel. Ils ne vérifient pas le comportement du pare-feu pour toutes les autres catégories.*

*Vous pouvez vérifier la classification d'un site Web spécifique à l'aide de l'outil de recherche de catégorie d'URL de Palo Alto Networks,* Test A Site*.*

Suivez la procédure correspondant à votre abonnement au Filtrage d'URL :

- Verify URL Filtering (Vérifier le filtrage d'URL)
- Verify Advanced URL Filtering (Vérifier le filtrage d'URL avancé)

## Vérifier le filtrage d'URL

Si vous disposez d'un abonnement de filtrage d'URL de base, suivez les étapes ci-dessous pour tester et vérifier que le pare-feu catégorise, applique et enregistre correctement les URL dans les catégories auxquelles vous accédez.

**STEP 1 |** Accédez à un site Web dans la catégorie URL qui vous intéresse.

Envisagez de tester les sites dans les catégories d'URL bloquées. Vous pouvez utiliser une page de test (urlfiltering.paloaltonetworks.com/test-***<url-category>***) pour éviter d'accéder directement à un site. Par exemple, pour tester votre politique de blocage des logiciels malveillants, visitez https://urlfiltering.paloaltonetworks.com/test-malware.

**STEP 2 |** Vérifiez que votre pare-feu traite correctement le site.

Par exemple, si vous avez configuré une page de blocage à afficher lorsqu'une personne accède à un site qui enfreint la politique de votre organisation, vérifiez qu'elle s'affiche lorsque vous visitez le site de test.

1. Examinez les journaux de trafic et de filtrage d'URL (**Monitor (Surveiller)** > **Logs (Journaux)**) pour confirmer que les URL ont été correctement catégorisées et que la règle de politique est enregistrée.

# Verify Advanced URL Filtering (Vérifier le filtrage d'URL avancé)

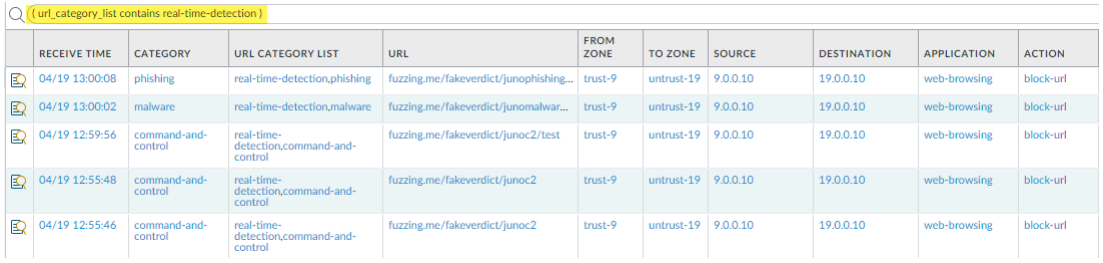
Si vous avez un Filtrage d'URL avancé abonnement, suivez les étapes ci-dessous pour tester et vérifier que l'analyse d'URL en temps réel est en cours.

*Palo Alto Networks recommande de définir le paramètre d'action de détection en temps réel pour alerter de vos profils de filtrage d'URL actifs. Cela offre une visibilité sur les URL analysées en temps réel et bloque (ou autorise, en fonction de vos paramètres de stratégie) en fonction des paramètres de catégorie configurés pour des menaces Web spécifiques.*

*Le pare-feu applique l'action la plus sévère des actions configurées pour les catégories d'URL détectées d'une URL donnée. Par exemple, supposons que example.com soit classé en tant que détection en temps réel, commande et contrôle et achats, des catégories avec une action d'alerte, de blocage et d'autorisation configurées, respectivement. Le pare-feu bloquera l'URL car le blocage est l'action la plus sévère parmi les catégories détectées.*

Vérifiez que les URL sont analysées et classées à l'aide du service avancé de filtrage d'URL.

1. Consultez chacune des URL de test suivantes pour vérifier que le service de filtrage d'URL avancé catégorise correctement les URL :
   - **Malware**—urlfiltering.paloaltonetworks.com/test-real-time-detection-malware
   - **Phishing (Hameçonnage)**—urlfiltering.paloaltonetworks.com/test-real-time-detection-phishing
   - **C2**—urlfiltering.paloaltonetworks.com/test-real-time-detection-command-and-control
   - **Grayware**—urlfiltering.paloaltonetworks.com/test-real-time-detection-grayware
   - **Benign (unknown) (Bénigne (inconnu))**—urlfiltering.paloaltonetworks.com/test-real-time-detection
2. Surveillez l'activité sur le pare-feu pour vérifier que les URL ci-dessus ont été correctement classées comme détection en temps réel.
   1. Sélectionnez **Monitor (Surveiller)** > **Logs (journaux)** > **URL Filtering (Filtrage des URL)** et filtrez par `(url_category_list contains real-time-detection)` pour afficher les journaux qui ont été analysés à l'aide du filtrage d'URL avancé. Des correspondances de catégories de pages Web supplémentaires sont également affichées et correspondent aux catégories définies par PAN-DB.

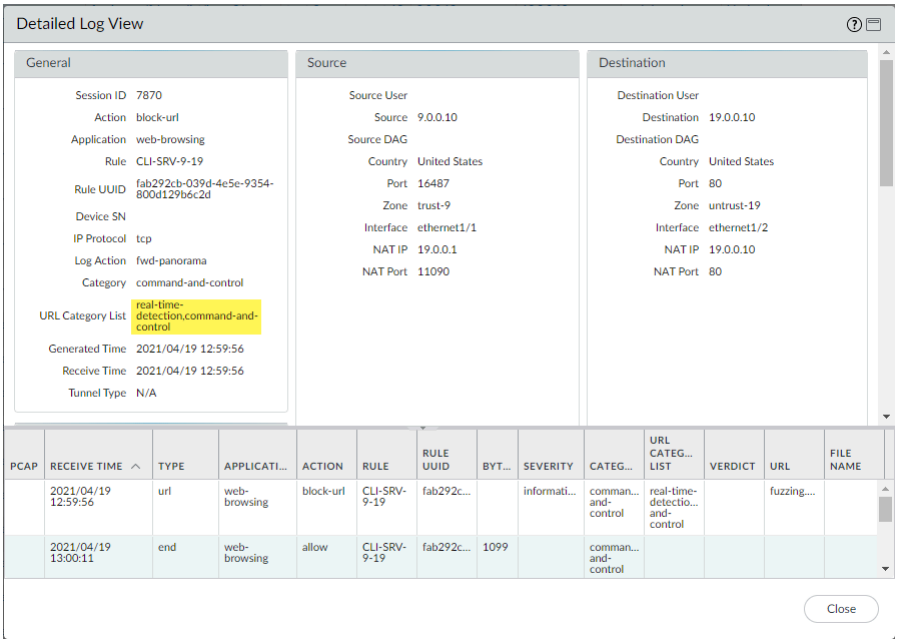



| RECEIVE TIME | CATEGORY | URL CATEGORY LIST | URL | FROM ZONE | TO ZONE | SOURCE | DESTINATION | APPLICATION | ACTION |
|---|---|---|---|---|---|---|---|---|---|
| 04/19 13:00:08 | phishing | real-time-detection,phishing | fuzzing.me/fakeverdict/junophishing... | trust-9 | untrust-19 | 9.0.0.10 | 19.0.0.10 | web-browsing | block-url |
| 04/19 13:00:02 | malware | real-time-detection,malware | fuzzing.me/fakeverdict/junomalwar... | trust-9 | untrust-19 | 9.0.0.10 | 19.0.0.10 | web-browsing | block-url |
| 04/19 12:59:56 | command-and-control | real-time-detection,command-and-control | fuzzing.me/fakeverdict/junoc2/test | trust-9 | untrust-19 | 9.0.0.10 | 19.0.0.10 | web-browsing | block-url |
| 04/19 12:55:48 | command-and-control | real-time-detection,command-and-control | fuzzing.me/fakeverdict/junoc2 | trust-9 | untrust-19 | 9.0.0.10 | 19.0.0.10 | web-browsing | block-url |
| 04/19 12:55:46 | command-and-control | real-time-detection,command-and-control | fuzzing.me/fakeverdict/junoc2 | trust-9 | untrust-19 | 9.0.0.10 | 19.0.0.10 | web-browsing | block-url |

   2. Examinez en détail les journaux pour vérifier que chaque type de menace Web est correctement analysé et catégorisé. Dans l'exemple ci-dessous, l'URL est classée comme ayant été analysée en temps réel et, en outre, comme possédant des qualités qui la définissent comme commande et contrôle. Parce que C&C a une action plus sévère par

rapport à la détection en temps réel (blocage par opposition à alerte), cette URL a été classée comme commande et contrôle et a été bloquée.



# Surveillance de l'activité Web

Dans l'ACC, les journaux et rapports de filtrage des URL consignent l'ensemble de l'activité Web des utilisateurs pour les catégories d'URL configurées sur **alert** (alerter), **block** (bloquer), **continue** (continuer) ou **override** (contrôle prioritaire). La surveillance des journaux vous permet de mieux comprendre l'activité Web de votre base de données d'utilisateurs afin de déterminer une politique d'accès Web.

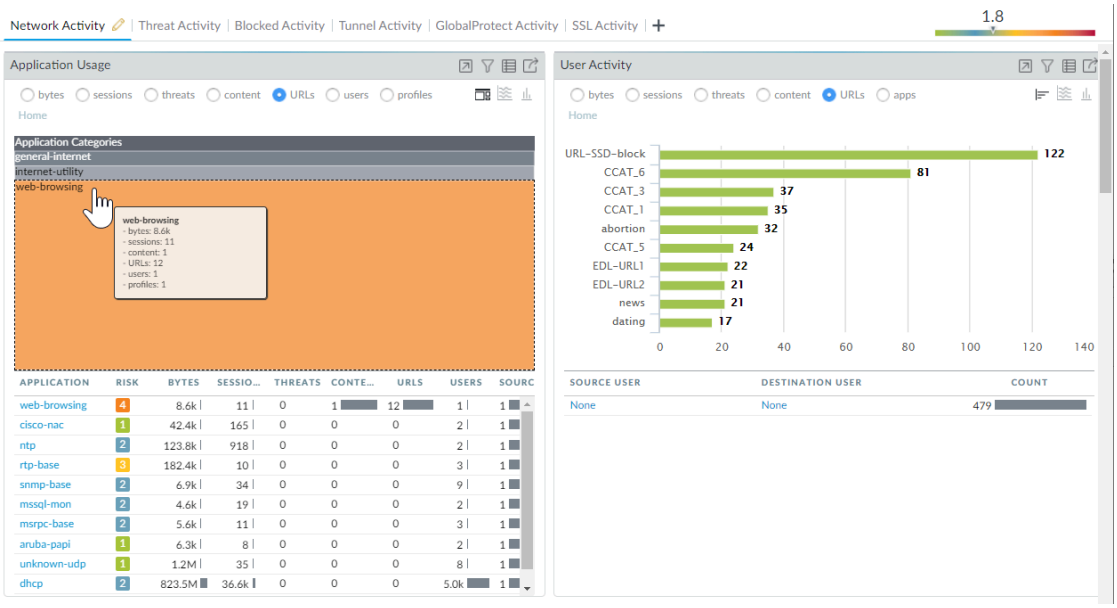
Les rubriques suivantes expliquent comment surveiller l'activité Web :

- Surveillance de l'activité Web des utilisateurs du réseau
- Affichage du rapport d'activités des utilisateurs
- Configuration de rapports personnalisés de filtrage des URL

## Surveillance de l'activité Web des utilisateurs du réseau

Vous pouvez utiliser le Centre re commande des applications (ACC), les rapports de filtrage des URL et les journaux générés sur le pare-feu pour suivre l'activité de l'utilisateur.

- Pour afficher rapidement les catégories les plus couramment consultées par les utilisateurs dans votre environnement, vérifiez les widgets **ACC**. La plupart des widgets de l'onglet **Network Activity (Activité réseau)** vous permettent de trier sur les URL. Par exemple, dans le widget Application Usage (Utilisation de l'application), vous pouvez voir que la catégorie de mise en réseau est la plus consultée, suivie du tunnel crypté et de SSL. Vous pouvez également consulter les listes **Threat Activity** (Activités des menaces) et **Blocked Activity** (Activités bloquées) triées sur les URL.




Afficher les journaux et configurer les options de journal :

- A partir de l'ACC, vous pouvez directement accéder aux journaux ( ) ou sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **URL Filtering (Filtrage des URL)**.

  L'action du journal pour chaque entrée dépend du paramètre Site Access (Accès au site) que vous avez défini pour la catégorie correspondante :

  - **Journal d'alerte** : Dans cet exemple, la catégorie computer-and-internet-info (infos sur l'ordinateur et internet) est définie sur alert (alerter).

    | RECEIVE TIME | CATEGORY | URL | FROM ZONE | TO ZONE | SOURCE | SOURCE USER | DESTINATION | APPLICATION | ACTION |
    |---|---|---|---|---|---|---|---|---|---|
    | 2020/04/16 14:10:53 | computer-and-internet-info | outlook.office36... | pm wifi | UNTRUST | [redacted] | [redacted] | [redacted] | outlook-web-online | alert |

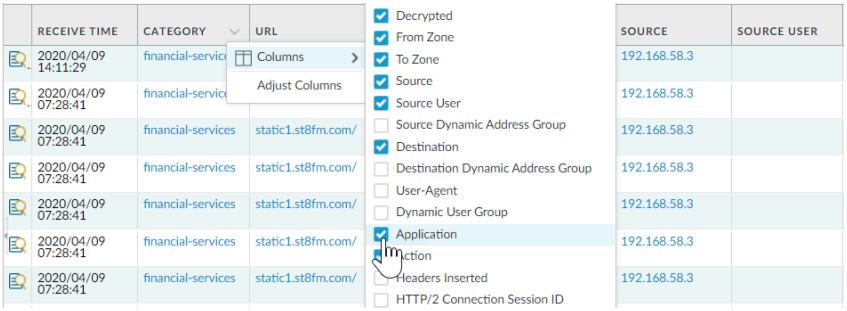
  - **Journal bloc** : dans cet exemple, la catégorie contenu-insuffisant est définie pour continuer. Si la catégorie avait été mise à block (bloc), le journal d'action serait à block-url.

    | RECEIVE TIME | CATEGORY | URL | FROM ZONE | TO ZONE | SOURCE | SOURCE USER | DESTINATION | APPLICATION | ACTION |
    |---|---|---|---|---|---|---|---|---|---|
    | 2020/04/08 18:47:49 | insufficient-content | munchkin.mark... | pm wifi | UNTRUST | [redacted] | [redacted] | [redacted] | ssl | block-continue |

  - **Journal d'alerte sur un site Web crypté** : Dans cet exemple, la catégorie est private-ip-addresses (addresses ip privées) et l'application est web-browsing (navigation sur le Web). Ce journal indique également que le pare-feu a décrypté ce trafic.

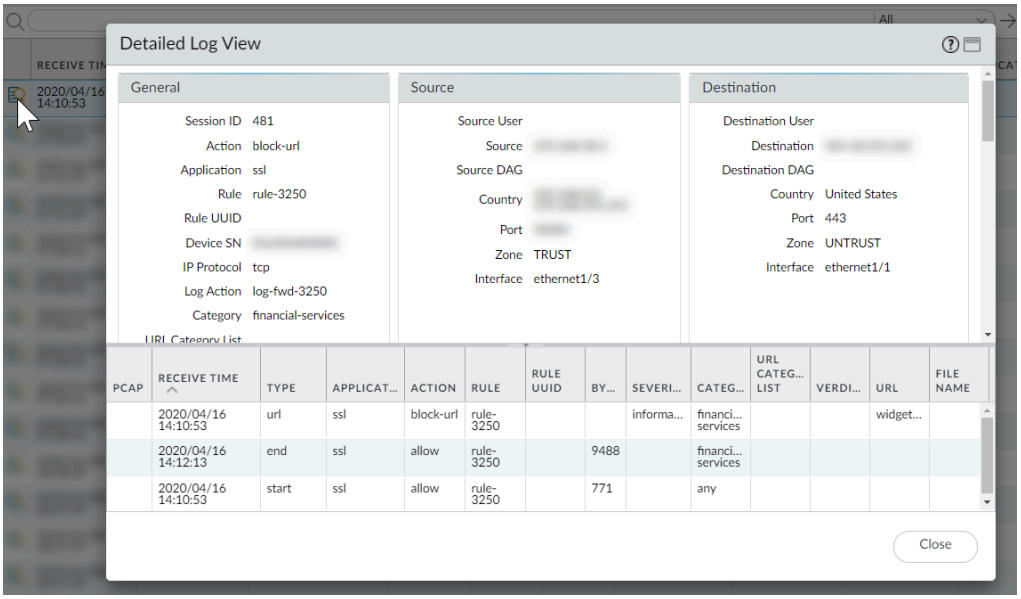
    | RECEIVE TIME | CATEGORY | URL | DECRYPTED | FROM ZONE | TO ZONE | SOURCE | SOURCE USER | DESTINATION | APPLICATION | ACTION |
    |---|---|---|---|---|---|---|---|---|---|---|
    | 2020/04/09 14:11:29 | private-ip-addresses | [redacted]/Updates/Updat... | yes | TRUST | UNTRUST | 192.168.58.3 | [redacted] | [redacted] | web-browsing | alert |

- Vous pouvez également ajouter plusieurs autres colonnes à votre vue de journal de filtrage des URL, comme : zone À et De, type de contenu et indiquer si des paquets ont été capturés ou non. Pour modifier les colonnes à afficher, cliquez sur la flèche vers le bas d'une colonne et sélectionnez l'attribut à afficher.



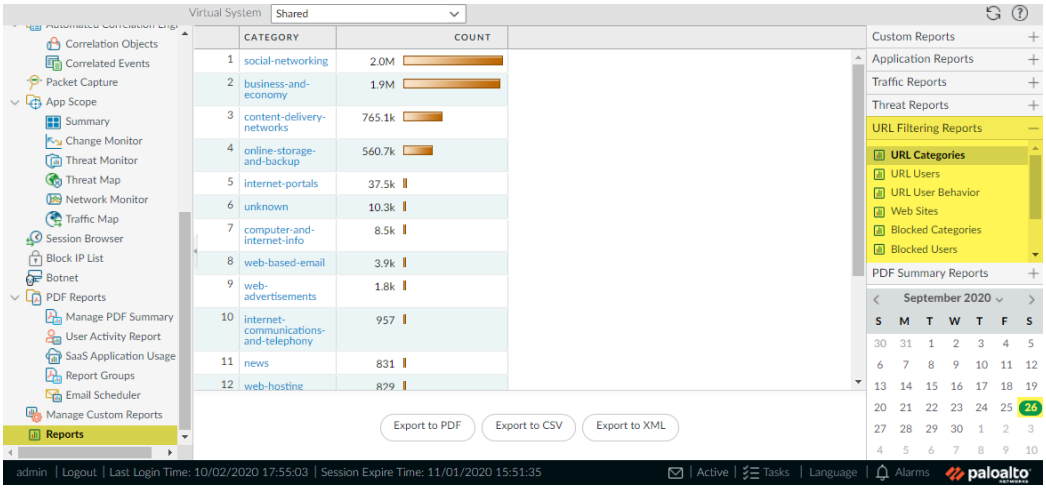

 

- Pour afficher l'ensemble des détails d'un journal et/ou demander la modification d'une catégorie pour une URL donnée ayant été consultée, cliquez sur l'icône Détails du journal qui se trouve dans la première colonne du journal.




- Générez des rapports de filtrage des URL prédéfinis sur les catégories d'URL, les utilisateurs des URL, les sites Web consultés, les catégories bloquées, etc.

  Sélectionnez **Monitor (Surveillance)** > **Reports (Rapports)**et dans la section **URL Filtering Reports (Rapports de filtrage d'URL)**, sélectionnez l'un des rapports. Les rapports couvrent la période de 24 heures de la date que vous sélectionnez dans le calendrier. Vous pouvez également exporter le rapport au format PDF, CSV ou XML.



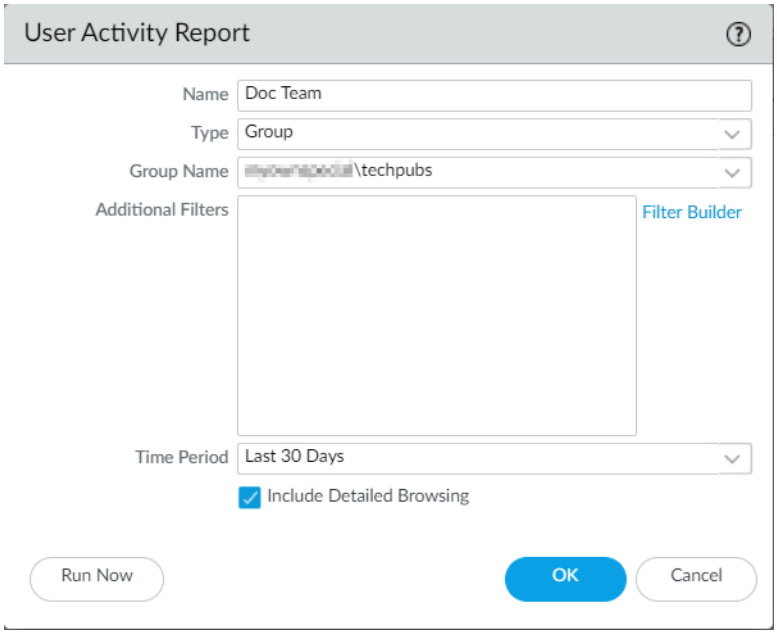

# Affichage du rapport d'activités des utilisateurs

Ce rapport permet de consulter rapidement l'activité des utilisateurs ou des groupes, mais aussi d'afficher la durée de navigation.

**STEP 1 |** Configurez un rapport d'activités des utilisateurs

1. Sélectionnez **Monitor (Surveillance)** > **PDF Reports (Rapports PDF)** > **User Activity Report (Rapport d'activité de l'utilisateur)**.
2. **Add (Ajoutez)** un rapport et donnez-lui un **Name (Nom)**.
3. Sélectionnez le **Type** de rapport :
   - Sélectionnez **User (Utilisateur)** pour générer un rapport pour une personne.
   - Sélectionnez **Group (Groupe)** pour un groupe d'utilisateurs.

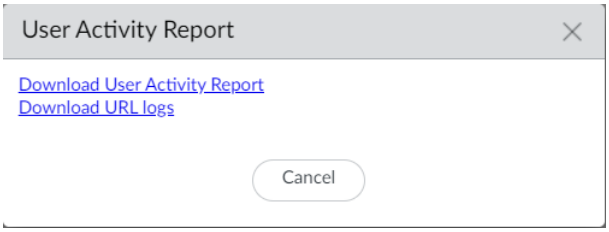
   *Vous devez enable User-ID (Activer l'User-ID) pour pouvoir sélectionner des noms d'utilisateurs ou de groupes. Si User-ID n'est pas configuré, vous pouvez sélectionner le type **User (Utilisateur)** et saisir l'adresse IP de l'ordinateur de l'utilisateur.*
4. Saisissez les valeurs pour **Username/IP Address (Nom d'utilisateur/adresse IP)** pour un rapport d'utilisateur ou le nom de groupe pour un rapport de groupe d'utilisateurs.
5. Sélectionnez la période. Vous pouvez sélectionner une période existante ou **Custom (Personnalisé)**.
6. Cochez la case **Include Detailed Browsing (Inclure la navigation détaillée)** afin d'inclure les informations de navigation dans le rapport.



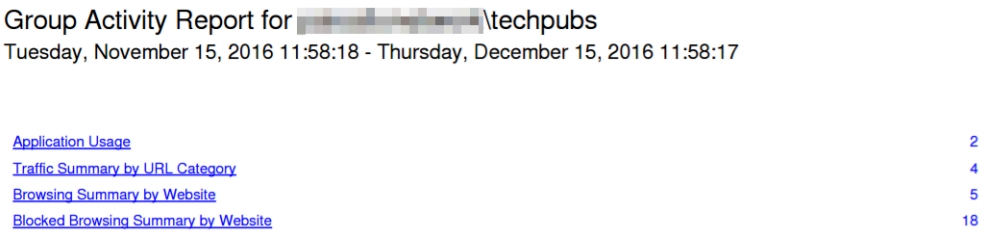
**STEP 2 |** Exécutez le rapport.

1. Cliquez sur **Run Now (Exécuter maintenant)**.
2. Lorsque le pare-feu finit de générer le rapport, cliquez sur un des liens pour le télécharger :
   - Cliquez sur **Download User Activity Report (Télécharger le rapport sur l'activité des utilisateurs)** pour télécharger une version PDF du rapport.
   - Cliquez sur **Download URL Logs (Télécharger les journaux d'URL)** pour télécharger un fichier CSV des entrées de journal correspondantes.

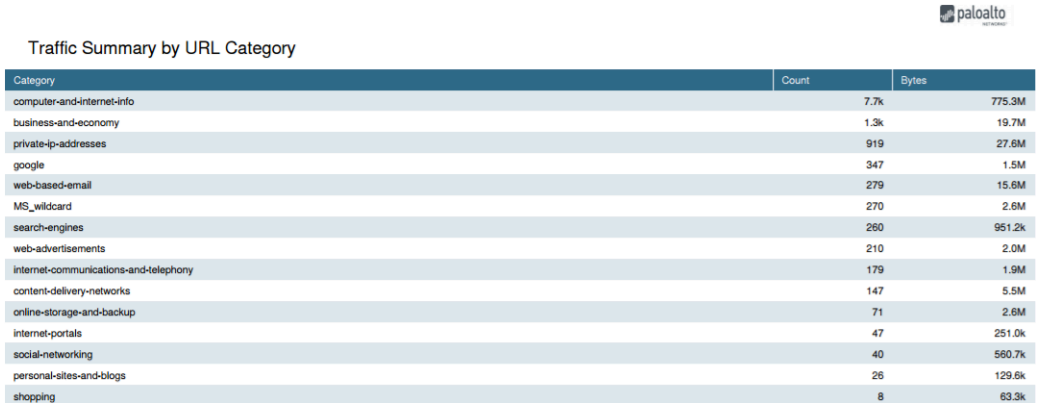



3. Après avoir téléchargé le rapport, cliquez sur **Cancel (Annuler)**.
4. Si vous souhaitez enregistrer les paramètres du rapport d'activité des utilisateurs pour pouvoir l'exécuter à nouveau plus tard, cliquez sur **OK (OK)** ; sinon, cliquez sur **Cancel (Annuler)**.

**STEP 3 |** Consultez le rapport d'activités de l'utilisateur en ouvrant le fichier que vous avez téléchargé. La version PDF du rapport montre l'utilisateur ou groupe sur lequel vous avez basé le rapport, la période du rapport et une table des matières :




**STEP 4 |** Cliquez sur un élément de la table des matières pour en afficher les détails du rapport. Par exemple, cliquez sur **Traffic Summary by URL Category (Récapitulatif du trafic par catégorie d'URL)** pour afficher les statistiques de l'utilisateur ou du groupe sélectionné.




| Category | Count | Bytes |
|---|---|---|
| computer-and-internet-info | 7.7k | 775.3M |
| business-and-economy | 1.3k | 19.7M |
| private-ip-addresses | 919 | 27.6M |
| google | 347 | 1.5M |
| web-based-email | 279 | 15.6M |
| MS_wildcard | 270 | 2.6M |
| search-engines | 260 | 951.2k |
| web-advertisements | 210 | 2.0M |
| internet-communications-and-telephony | 179 | 1.9M |
| content-delivery-networks | 147 | 5.5M |
| online-storage-and-backup | 71 | 2.6M |
| internet-portals | 47 | 251.0k |
| social-networking | 40 | 560.7k |
| personal-sites-and-blogs | 26 | 129.6k |
| shopping | 8 | 63.3k |

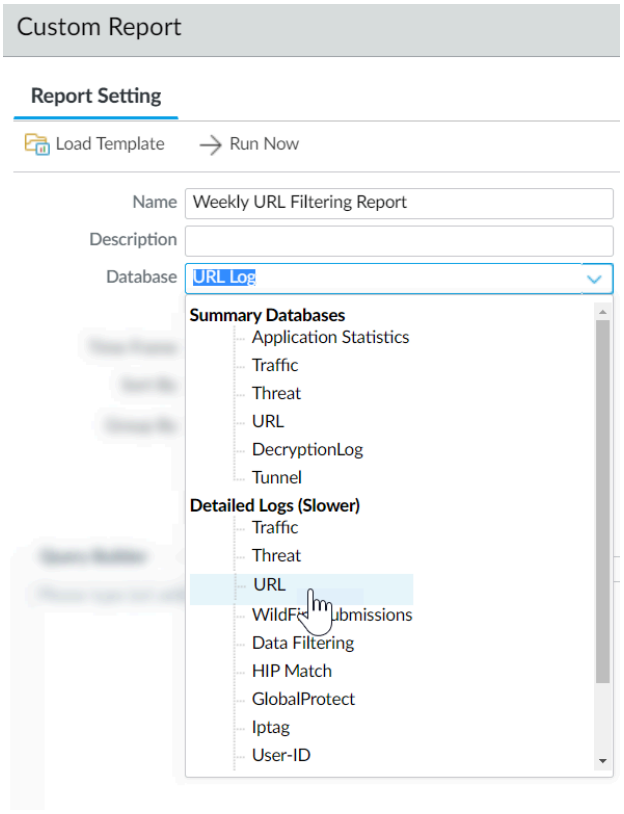
 

# Configuration de rapports personnalisés de filtrage des URL

Pour générer un rapport détaillé que vous pouvez également programmé pour être exécuté régulièrement, vous pouvez configurer un rapport personnalisé de filtrage des URL. Vous pouvez choisir n'importe quelle combinaison de champs des journaux de filtrage des URL sur lesquels reposera le rapport.

**STEP 1 |** Ajoutez un nouveau rapport personnalisé.

1. Sélectionnez **Monitor (Surveillance)** > **Manage Custom Reports (Gérer les rapports personnalisés)** et **Add (Ajoutez)** un rapport.
2. Donnez un **Name (Nom)** unique au rapport et, éventuellement, une **Description (Description)**.
3. Sélectionnez la **Database (Base de données)** à utiliser pour générer le rapport. Pour générer un rapport de filtrage des URL détaillé, sélectionnez **URL (URL)** à la section Detailed Logs (Journaux détaillés) :

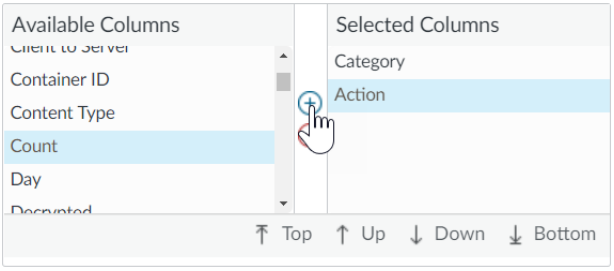



**STEP 2 |** Configurez les options du rapport.

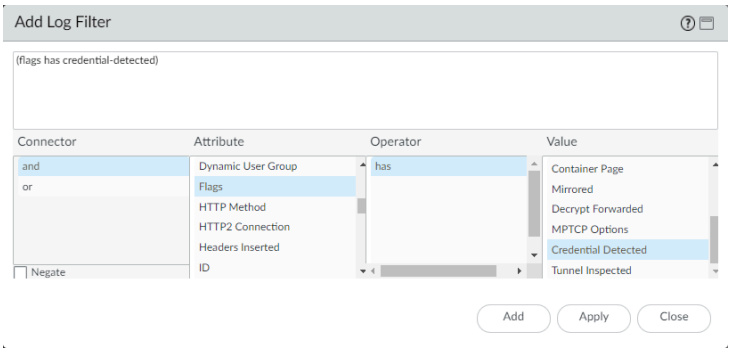
1. Sélectionnez un **Time Frame (Calendrier)** prédéfini ou sélectionnez **Custom (Personnalisé)**.
2. Sélectionnez les colonnes des journaux à inclure dans le rapport dans la liste Available Columns (Colonnes disponibles), puis ajoutez-les ( ⊞ ) aux Selected Columns (Colonnes sélectionnées). Par exemple, dans le cas d'un rapport de filtrage des URL, vous pourriez sélectionner les options suivantes :
   - Action (Action)
   - Catégorie d'applications

- Catégorie
- Pays de destination
- Source User (Utilisateur source)
- URL



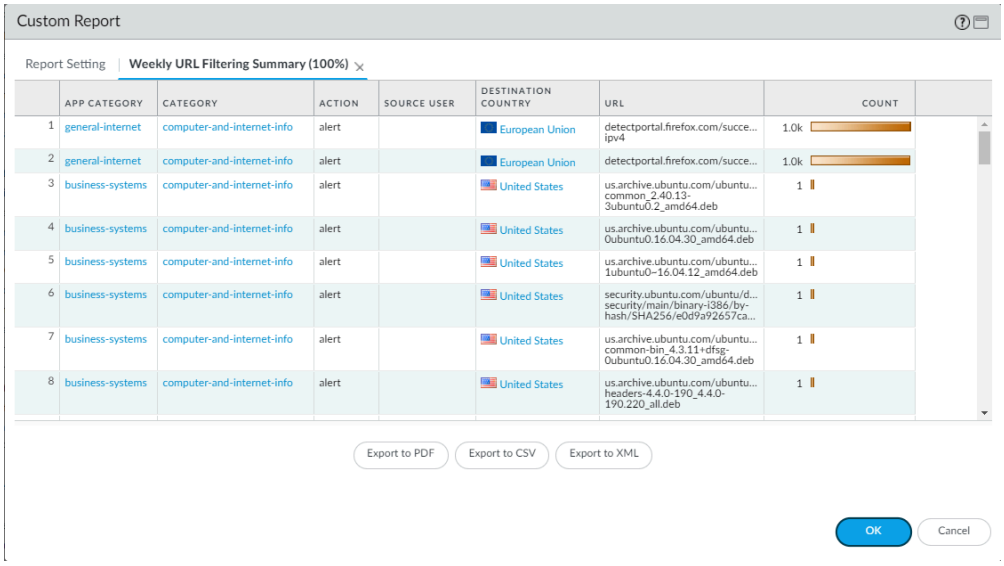

3. Si l'option prevent credential phishing (Empêcher l'hameçonnage des informations d'identification) est activée sur le pare-feu, sélectionnez les **Flags (Indicateurs)**, l'opérateur **has (a)** et la valeur **Credential Detected (Informations d'identification détectées)** pour également inclure les événements dans le rapport afin de consigner les situations où un utilisateur soumet des informations d'identification d'entreprise valide à un site.




4. (Facultatif) Sélectionnez une option **Sort By (Trier par)** pour définir l'attribut à utiliser pour agréger les détails du rapport. Si vous ne sélectionnez pas d'attribut pour le tri, le rapport renvoie les N premiers résultats sans agrégation. Sélectionnez un attribut **Group By (Regrouper par)** à utiliser comme ancrage pour regrouper des données. Voici un exemple d'un rapport dans lequel l'attribut **Group By (Regrouper par)** est défini sur **App Category**

**(Catégorie d'application)** et l'option **Sort By (Trier par)** est définie sur un **Count** (nombre) de **Top 5** (5 premières).




**STEP 3 |** Exécutez le rapport.

1. Cliquez sur l'icône **Run Now (Exécuter maintenant)** pour générer immédiatement le rapport, qui s'ouvre dans un nouvel onglet.
2. Lorsque vous avez terminé votre examen du rapport, retournez à l'onglet **Report Setting (Paramètres de rapport)**, puis précisez les paramètres et générez le rapport de nouveau ou passez à l'étape suivante pour planifier la génération du rapport.
3. Cochez la case **Schedule (Calendrier)** pour exécuter le rapport une fois par jour. Il sera généré quotidiennement et détaillera l'activité Web des 24 dernières heures.

**STEP 4 |** **Commit (Validez)** la configuration.

**STEP 5 |** Affichez le rapport personnalisé.

1. Sélectionnez **Monitor (Surveillance)** > **Reports (Rapports)**.
2. Développez le panneau **Custom Reports (Rapports personnalisés)** dans la colonne de droite et sélectionnez le rapport à afficher. Le rapport le plus récent s'affiche automatiquement.
3. Pour consulter le rapport d'une date antérieure, sélectionnez la date souhaitée dans le calendrier. Vous pouvez également exporter le rapport au format PDF, CSV ou XML.

# Journalisez uniquement la page visitée par un utilisateur

Une page conteneur est la page principale à laquelle accède un utilisateur lorsqu'il visite un site Web, mais d'autres pages peuvent être chargées en même temps que cette page principale. Si l'option **Log Container page only (Page conteneur de journaux uniquement)** est activée dans le profil de Filtrage des URL (**Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **URL Filtering (Filtrage des URL)**), seule la page conteneur principale sera journalisée, mais pas les pages suivantes susceptibles d'être chargées dans la page conteneur. Étant donné que le filtrage des URL peut potentiellement générer un grand nombre d'entrées de journal, vous pouvez activer cette option afin que les entrées de journal ne contiennent que les URL dont le nom de fichier de la page demandée correspond à des types MIME spécifiques. Les types MIME suivants sont fournis par défaut :

- application/pdf
- application/soap+xml
- application/xhtml+xml
- text/html
- text/plain
- text/xml

*Si vous activez l'option **Log container page only (Page conteneur de journaux uniquement)**, il est possible qu'une entrée corrélée du journal des URL n'existe pas pour identifier les menaces détectées par l'antivirus ou la protection contre les vulnérabilités.*

# Création d'une catégorie d'URL personnalisée

Vous pouvez créer un objet de filtrage des URL personnalisé pour spécifier les exceptions à l'application de la catégories d'URL et pour créer une catégorie d'URL personnalisée qui se fonde sur plusieurs catégories d'URL :

- **Define exceptions to URL category enforcement (Définir des exceptions à l'application de la catégorie d'URL)** : créez une liste personnalisée d'URL que vous souhaitez utiliser comme critères de correspondance dans une règle de politique de sécurité. C'est une bonne façon de spécifier des exceptions à des catégories d'URL, lorsque vous aimeriez appliquer des URL spécifiques différemment de la catégorie d'URL à laquelle elles appartiennent.
- **Définir une catégorie d'URL personnalisée en fonction de plusieurs catégories PAN-DB** : cette option vous permet de cibler l'application pour des sites Web qui correspondent à un ensemble de catégories. Le site Web ou la page doivent faire correspondre ***l'ensemble*** des catégories définies dans le cadre de la catégorie personnalisée.

Suivez ces étapes pour créer une catégorie d'URL personnalisée, et définir la façon dont vous souhaitez que le pare-feu applique la catégorie d'URL personnalisée :

**STEP 1 |** Sélectionnez **Objects (Objets)** > **Custom Objects (Objets personnalisés)** > **URL Category (Catégorie d'URL)**.

**STEP 2 |** **Add (Ajoutez)** ou modifier une catégorie d'URL personnalisée et donnez un **Name (Nom)** descriptif à la catégorie.

**STEP 3 |** Définissez le **Type** de catégorie sur **Category Match (Correspondance à la catégorie)** ou **URL List (Liste d'URL)** :

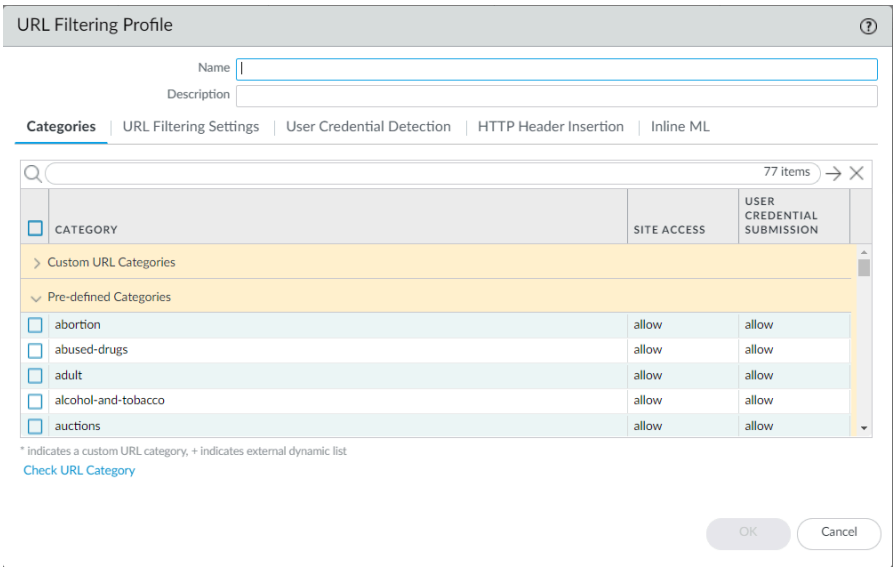
- **URL List (Liste d'URL)** : ajoutez les URL que vous souhaitez appliquer différemment de la catégorie d'URL à laquelle ils appartiennent. Utilisez ce type de liste pour définir des exceptions à l'application de la catégorie d'URL ou pour définir qu'une liste d'URL appartient à une catégorie personnalisée. Pour obtenir des détails sur la façon de générer cette liste, comme des lignes directrices sur l'utilisation des caractères génériques, reportez-vous à la rubrique Exceptions de catégories d'URL.
- **Category Match (Correspondance à la catégorie)** : fournir une application ciblée pour les sites Web qui correspondent à un ensemble de catégories. Le site Web ou la page doivent faire correspondre ***l'ensemble*** des catégories définies dans le cadre de la catégorie personnalisée.

**STEP 4 |** Sélectionnez **OK** pour enregistrer la catégorie d'URL personnalisée.

**STEP 5 |** Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de Sécurité)** > **URL Filtering (Filtrage des URL)** et **Add (Ajouter)** ou modifiez un profil de filtrage des URL.

Votre nouvelle catégorie personnalisée figurera dans la liste déroulante **Custom URL Categories (Catégories d'URL personnalisées)** :




**STEP 6 |** Décidez comment vous voulez appliquer le **Site Access (Accès au site)** et les **User Credential Submissions (Envois des informations d'identification de l'utilisateur** pour la catégorie d'URL personnalisée. (Pour contrôler les sites auxquels les utilisateurs peuvent soumettre leurs informations d'identification d'entreprise, reportez-vous à la section Empêcher le hameçonnage des informations d'identification).

**STEP 7 |** Associez le profil de Filtrage des URL à une Règle de politique de sécurité pour appliquer le trafic qui correspond à cette règle.

Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** > **Actions** et spécifiez que la Règle de politique applique le trafic en fonction du profil de Filtrage des URL que vous venez de mettre à jour. Assurez-vous de **Commit (Valider)** vos modifications.

*Vous pouvez également utiliser des catégories d'URL personnalisée en tant que critères de correspondance de la politique de sécurité. Dans ce cas, vous n'avez pas à définir la manière d'appliquer la catégorie dans le cadre d'un profil de filtrage des URL. Après avoir défini la catégorie personnalisée, allez directement à la règle de politique de sécurité à laquelle vous souhaitez ajouter la catégorie d'URL personnalisée (**Policies (Politiques)** > **Security (Sécurité)**). Sélectionnez **Service/URL Category (Catégorie de service/d'URL)** pour utiliser la catégorie d'URL personnalisée en tant que critère de correspondance pour la règle.*

# Exceptions de catégories d'URL

Vous pouvez exclure des sites Web spécifiques de l'application des catégories d'URL, ce qui garantit que ces sites Web sont bloqués ou autorisés, peu importe les catégories d'URL auxquelles ils sont associés. Par exemple, vous pouvez bloquer la catégorie d'URL de réseau social mais autoriser l'accès à LinkedIn. Pour créer des exceptions à l'application de la stratégie de catégorie d'URL :

- Ajoutez les adresses IP ou les URL des sites que vous souhaitez explicitement bloquer ou autoriser une custom URL category list (liste de catégories d'URL personnalisée) (**Objects (Objets)** > **Custom Objects (Objets personnalisés)** > **URL Category (Catégorie d'URL)**. Ensuite, définissez la manière dont vous souhaitez appliquer la catégorie dans un profil de filtrage d'URL. Enfin, attachez le profil à une règle de stratégie de sécurité. Vous pouvez également utiliser directement la liste d'URL personnalisée comme critères de correspondance dans une règle de Politique de sécurité.
- Use an external dynamic list in a URL Filtering profile (Utilisez une liste dynamique externe dans un profil de filtrage d'URL) ou comme match criteria in a Security policy rule (critères de correspondance dans une règle de politique de sécurité). L'avantage d'utiliser une liste dynamique externe est que vous pouvez mettre à jour la liste sans effectuer de modification de configuration ou de validation sur le pare-feu.
- Créez une règle de Politique de sécurité qui exclut le site ou l'application d'une catégorie d'URL particulière de l'application de la politique. Placez la règle d'exception au-dessus de la règle qui autorise ou bloque la catégorie d'URL à laquelle appartient l'exception d'URL.

Les lignes directrices suivantes décrivent la génération de listes d'interdiction et d'autorisation de catégories d'URL ou d'un fichier texte que vous utilisez en tant que source d'une liste dynamique externe des URL :

- Directives de base pour les listes d'exceptions de catégories d'URL
- Directives sur les caractères génériques pour les listes d'exceptions de catégories d'URL
- Listes d'exceptions de catégories d'URL : exemples de caractères génériques

## Directives de base pour les listes d'exceptions de catégories d'URL

- Saisissez les adresses IP ou les URL des sites Web que vous souhaitez appliquer distinctement de la catégorie d'URL à laquelle elles sont associées.
- Les entrées de la liste doivent être exactes et sont sensibles à la casse.
- Entrez une chaîne qui est une correspondance exacte au site Web (et, éventuellement, un sous-domaine spécifique) auquel vous souhaitez contrôler l'accès ou utilisez des caractères génériques pour permettre à une entrée de correspondre à plusieurs sous-domaines d'un site Web. Pour plus de précisions sur l'utilisation des caractères génériques, passez en revue la section Directives sur les caractères génériques pour les listes d'exceptions de catégories d'URL.
- Omettez `http` et `https` des entrées d'URL.
- Chaque entrée d'URL peut contenir un maximum de 255 caractères.

# Directives sur les caractères génériques pour les listes d'exceptions de catégories d'URL

Vous pouvez utiliser des caractères génériques dans les listes d'exceptions de catégories d'URL afin de facilement configurer une seule entrée qui doit correspondre à plusieurs sous-domaines de site Web et de pages, sans avoir à spécifier des sous-domaines et des pages exacts.

Suivez les directives suivantes lorsque vous créez des entrées qui possèdent des caractères génériques :

- Les caractères suivants sont considérés comme des séparateurs de jetons : . / ? & = ; +

  Chaque chaîne séparée par un ou deux de ces caractères est un jeton. Utilisez les caractères génériques en tant que marque substitutive d'un jeton, laquelle indique qu'un jeton spécifique peut contenir une valeur.
- À la place d'un jeton, vous pouvez soit utiliser un astérisque (*) ou un caret (^) pour indiquer une valeur d'un caractère générique.
- Les caractères génériques sont les seuls caractères autorisés au sein d'un jeton ; cependant, une entrée peut contenir plusieurs caractères génériques.

**Utilisation des astérisques (*) et des carets (^)**

| | |
|---|---|
| * | À utiliser pour indiquer un ou plusieurs sous-domaines variables. Si vous utilisez *****, l'entrée sera mise en correspondance avec les sous-domaines supplémentaires, qu'ils se trouvent au début ou à la fin de l'URL. Utilisez une barre oblique avant à la fin de l'entrée si vous ne voulez plus mettre en correspondance les sous-domaines supplémentaires au-delà de ce point.<br>Exemple :<br>• ***.paloaltonetworks.com** correspond à www.paloaltonetworks.com et à www.paloaltonetworks.com.uk.<br>• ***.paloaltonetworks.com** correspond à www.paloaltonetworks.com et à www.paloaltonetworks.com.uk. |
| ^ | À utiliser pour indiquer un sous-domaine variable.<br>Exemple :<br>**mail.^.com** correspond à mail.company.com, mais pas à mail.company.sso.com. |

***Ne créez pas d'entrée comportant des astérisques (*) consécutifs ou plus de neuf carets (^) consécutifs. De telles entrées peuvent compromettre la performance du pare-feu.***

*Par exemple, n'ajoutez pas d'entrée comme* ***mail.*.*.com*** *; selon la plage de sites Web auxquels vous souhaitez contrôler l'accès, entrez plutôt* ***mail.*.com*** *ou* ***mail.^.^.com****. Une entrée comme* ***mail.*.com*** *correspond à un plus grand nombre de sites que* ***mail.^.^.com*** *;* ***mail.*.com*** *correspond à des sites qui comprennent un nombre indéfini de sous-domaines, tandis que* ***mail.^.^.com*** *correspond à des sites qui contiennent exactement deux sous-domaines.*

## Listes d'exceptions de catégories d'URL : exemples de caractères génériques

Le tableau suivant présente des exemples d'entrées de listes d'exception d'URL qui utilisent des caractères génériques de même que des exemples de sites auxquels ces entrées correspondent.

| Entrée de la liste d'exceptions d'URL | Sites correspondants |
|---|---|
| **Ensemble d'exemples 1** | |
| *.company.com | eng.tools.company.com<br>support.tools.company.com<br>tools.company.com<br>docs.company.com |
| ^.company.com | tools.company.com<br>docs.company.com |
| ^.^.company.com | eng.tools.company.com<br>support.tools.company.com |
| **Ensemble d'exemples 2** | |
| mail.google.* | mail.google.com<br>mail.google.co.uk |
| mail.google.^ | mail.google.com |
| mail.google.^.^ | mail.google.co.uk |
| **Example Set 3 (Ensemble d'exemples 3)** | |
| site.*.com | site.a.com<br>site.a.b.com |

| Entrée de la liste d'exceptions d'URL | Sites correspondants |
|---|---|
| | site.a.b.c.com |
| site.^.com | mail.a.com |
| site.^.^.com | mail.a.b.com |
| site.com/* | site.com/photos<br>site.com/blog/2019<br>tout sous-répertoire site.com |

# Utilisation d'une liste dynamique externe dans un profil de filtrage des URL

Pour protéger votre réseau des menaces et des fichiers malveillants nouvellement découverts, vous pouvez utiliser des external dynamic lists (listes dynamiques externes) dans les profils de filtrage des URL. Les listes dynamiques externes vous offrent la possibilité de mettre à jour la liste sans effectuer de changement de configuration ou de validation sur le pare-feu. Une liste dynamique externe est un fichier texte qui est hébergé sur un serveur Web externe. Vous pouvez vous servir de cette liste pour importer des URL et appliquer une politique à ces URL. Lorsque la liste est mise à jour sur le serveur Web, le pare-feu récupère les modifications apportées et applique la politique à la liste modifiée sans qu'aucune validation n'ait lieu sur le pare-feu.

Le pare-feu importe la liste de manière dynamique à l'intervalle configuré et applique la politique aux URL (les adresses IP ou les domaines sont ignorés) qui figurent dans la liste. Pour obtenir des directives de mise en forme des URL, reportez-vous à la section Exceptions de catégories d'URL.

Pour plus d'informations, consultez Liste dynamique externe.

**STEP 1 |** Configure the firewall to access an external dynamic list (Configuration du pare-feu pour qu'il accède à la liste dynamique externe).

- Assurez-vous que la liste ne comprenne aucune adresse IP ou aucun nom de domaine ; le pare-feu ignore toutes les entrées qui ne sont pas des URL.
- Utilisez les custom URL list guidelines (directives de liste d'URL personnalisées) pour vérifier la mise en forme de la liste.
- Sélectionnez **URL List (Liste des URL)** dans la liste déroulante Type.

**STEP 2 |** Utilisez la liste dynamique externe dans un profil de filtrage des URL.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **URL Filtering (Filtrage des URL)**.
2. **Add (Ajoutez)** ou modifiez un profil de filtrage des URL existant.
3. Donnez un **Name (Nom)** au profil et, dans l'onglet **Categories (Catégories)**, sélectionnez la liste dynamique externe dans la liste Category (Catégorie).
4. Cliquez sur Action (Action) pour sélectionner une action plus granulaire pour les URL figurant dans la liste dynamique externe.

   *Si une URL qui figure dans une liste dynamique externe figure également dans une catégorie d'URL personnalisée, ou dans les block and allow list (Listes d'interdiction et d'autorisation), l'action précisée dans la catégorie personnalisée ou dans la liste d'interdiction et d'autorisation est prioritaire par rapport à la liste dynamique externe.*
5. Cliquez sur **OK**.
6. Associez le profil de filtrage des URL à une règle de politique de sécurité.
   1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
   2. Sélectionnez l'onglet **Actions (Actions)** puis, dans la section Profile Setting (Paramètre de profil), sélectionnez le nouveau profil dans la liste déroulante **URL Filtering (Filtrage des URL)**.
   3. Cliquez sur **OK**, puis sur **Commit (Valider)**.

**STEP 3 |** Vérifiez que l'action de politique est appliquée.

1. View the external dynamic list entries (Affichez les entrées de la liste dynamique externe) et essayez d'accéder à une URL de la liste.
2. Vérifiez que l'action que vous avez définie est appliquée dans le navigateur.
3. Pour surveiller l'activité sur le pare-feu :
   1. Sélectionnez **ACC (ACC)** et ajoutez un domaine d'URL en tant que filtre général pour afficher l'activité sur le réseau et l'activité bloquée pour l'URL à laquelle vous avez accédé.
   2. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **URL Filtering (Filtrage des URL)** pour accéder à la vue détaillée du journal.

**STEP 4 |** Vérifiez si les entrées de la liste dynamique externe ont été ignorées ou sautées.

Dans une liste d'URL, le pare-feu saute toutes les entrées qui ne sont pas des URL et les considère comme non valables ; il ignore également les entrées qui dépassent le nombre maximum d'entrées permises sur le modèle de pare-feu.

*Pour vérifier si vous avez atteint la limite pour un type de liste dynamique externe, sélectionnez* ***Objects (Objets)*** *>* ***External Dynamic Lists (Listes dynamiques externes)*** *et cliquez sur* ***List Capacities (Capacités de liste)****.*

Pour revoir les détails d'une liste, servez-vous de la commande CLI suivante sur un pare-feu :

```
request system external-list show type url name <list_name>
```

Par exemple :

```
request system external-list show type url name My_URL_List
vsys5/My_URL_List:
Next update at: Tue Jan 3 14:00:00 2017
Source: http://example.com/My_URL_List.txt
Referenced: Yes
Valid: Yes
Auth-Valid: Yes

Total valid entries: 3
Total invalid entries: 0
Valid urls:
www.URL1.com
www.URL2.com
www.URL3.com
```

# Autoriser l'accès par mot de passe à certains sites

Dans certains cas, vous souhaiterez peut-être bloquer des catégories d'URL mais en autoriser occasionnellement l'accès à certaines personnes. Dans ce cas, vous devez définir l'action de la catégorie sur **override (contrôle prioritaire)** et définir un mot de passe de forçage de l'URL par l'administrateur dans la configuration Content-ID du pare-feu. Les utilisateurs devront fournir le mot de passe de contrôle prioritaire avant de pouvoir accéder aux sites de ces catégories. Suivez la procédure ci-dessous pour configurer le contrôle prioritaire de l'URL par l'administrateur :

**STEP 1 |** Définissez le mot de passe de contrôle prioritaire de l'URL par l'administrateur.

1. Sélectionnez **Device (Périphérique)** > **Setup( Configuration)** > **Content ID**.
2. Dans la section **URL Admin Override (Forçage de l'URL par l'administrateur)**, cliquez sur **Add (Ajouter)**.
3. Dans le champ **Location (Emplacement)**, sélectionnez le système virtuel auquel le mot de passe s'applique.
4. Saisissez le **Password (Mot de passe)** et **Confirm Password (Confirmez le mot de passe)**.
5. Sélectionnez un **SSL/TLS Service Profile (profil de service SSL/TLS)**. Le profil spécifie le certificat que le pare-feu présente à l'utilisateur si le site contenant le contrôle prioritaire est un site HTTPS. Pour plus d'informations, voir Configuration d'un profil de service SSL/TLS.
6. Sélectionnez le **Mode (Mode)** de demande du mot de passe à l'utilisateur:
   - **Transparent (Transparent)** : le pare-feu intercepte le trafic du navigateur destiné au site d'une catégorie d'URL que vous avez définie pour forcer et remplacer l'URL de destination d'origine en générant une requête HTTP 302 de demande de mot de passe, qui s'applique au niveau du système virtuel.

     *Le navigateur client affichera des erreurs de certificat s'il ne reconnaît pas le certificat.*
   - **Redirect (Rediriger)** : le pare-feu intercepte le trafic HTTP ou HTTPS vers une catégorie d'URL définie pour le forçage et redirige la requête vers une interface de Couche 3 du pare-feu à l'aide d'une redirection HTTP 302 de demande de mot de passe de forçage. Si vous sélectionnez cette option, vous devez fournir l'**Address (Adresse)** (adresse IP ou nom d'hôte DNS) vers laquelle rediriger le trafic.
7. Cliquez sur **OK**.

**STEP 2 |** (Facultatif) Définissez une période de contrôle prioritaire personnalisée.

1. Modifiez la section URL Filtering (Filtrage des URL).
2. Pour modifier la durée pendant laquelle les utilisateurs peuvent consulter un site d'une catégorie pour laquelle ils ont fourni le mot de passe de contrôle prioritaire, saisissez une nouvelle valeur dans le champ **URL Admin Override Timeout (Délai de contrôle prioritaire de l'URL par l'administrateur)**. Par défaut, les utilisateurs peuvent accéder aux sites de la catégorie pendant 15 minutes sans saisir à nouveau le mot de passe.
3. Pour modifier la durée pendant laquelle les utilisateurs ne peuvent pas accéder à un site défini sur un contrôle prioritaire après trois échecs de saisie du mot de passe de forçage, saisissez une nouvelle valeur dans le champ **URL Admin Lockout Timeout (Délai de**

**contrôle prioritaire sur l'URL par l'administrateur)**. Par défaut, les utilisateurs sont bloqués pendant 30 minutes.

4. Cliquez sur **OK**.

**STEP 3 |** (Mode Rediriger uniquement) Créez une interface de Couche 3 vers laquelle rediriger les requêtes Web vers des sites d'une catégorie configurée pour le contrôle prioritaire.

1. Créez un profil de gestion pour permettre à l'interface d'afficher la page de réponse Continuer et Contrôle prioritaire du filtrage des URL :
   1. Sélectionnez **Network (Réseau)** > **Interface Mgmt (Gestion de l'interface)**, puis cliquez sur **Add (Ajouter)**.
   2. Donnez un **Name (Nom)** au profil, sélectionnez **Response Pages (Pages de réponse)**, puis cliquez sur **OK (OK)**.
2. Créez l'interface de couche 3. Veillez à associer le profil de gestion que vous venez de créer (dans l'onglet **Advanced (Avancé)** > **Other Info (Autres informations)** de la boîte de dialogue Ethernet Interface (Interface Ethernet)).

**STEP 4 |** (Mode Rediriger uniquement) Pour rediriger en toute transparence les utilisateurs sans afficher d'erreur de certificat, installez un certificat correspondant à l'adresse IP de l'interface vers laquelle vous redirigez les requêtes Web vers un site d'une catégorie d'URL configurée pour le contrôle prioritaire. Vous pouvez générer un certificat auto-signé ou importer un certificat signé par une CA externe.

Pour utiliser un certificat auto-signé, vous devez tout d'abord créer un certificat CA racine puis utiliser cette CA pour signer le certificat que vous utiliserez pour le contrôle prioritaire de l'URL par l'administrateur comme suit :

1. Pour créer un certificat d'autorité de certification racine, sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion de certificat)** > **Certificates (Certificats)** > **Device Certificates (certificats de périphérique)**, puis cliquez sur **Generate (Générer)**. Saisissez un **nom de certificat**, RootCA par exemple. Ne sélectionnez pas de valeur dans le champ **Signed By (Signé par)** (ceci indique qu'il est auto-signé). Veillez à bien cocher la case **Certificate Authority (Autorité de certification)**, puis cliquez sur **Generate (Générer)** le certificat.
2. Pour créer le certificat à utiliser pour le forçage de l'URL par l'administrateur, cliquez sur **Generate (Générer)**. Saisissez le **Certificate Name (Nom du certificat)**, puis le nom DNS de l'hôte ou l'adresse IP de l'interface en tant que **Common Name (Nom commun)**. Dans le champ **Signed By (Signé par)**, sélectionnez l'AC créée à l'étape précédente. Ajoutez un attribut d'adresse IP, puis précisez l'adresse IP de l'interface de Couche 3 vers laquelle les requêtes Web seront redirigées vers des catégories d'URL comprenant l'action de contrôle prioritaire.
3. **Generate (Générez)** le certificat.
4. Pour configurer des clients autorisant le certificat, sélectionnez le certificat AC dans l'onglet **Device Certificates (Certificats de périphérique)**, puis cliquez sur **Export (Exporter)**. Vous devez ensuite importer le certificat en tant que CA racine de confiance dans tous les navigateurs clients, en configurant manuellement le navigateur ou en ajoutant le certificat aux racines de confiance d'un objet GPO (Group Policy Object) d'Active Directory.

**STEP 5 |** Spécifiez les catégories d'URL qui requièrent un mot de passe de contrôle prioritaire pour en autoriser l'accès.

1. Sélectionnez **Objects (Objets)** > **URL Filtering (Filtrage des URL)**, puis sélectionnez un profil de Filtrage des URL existant ou cliquez sur **Add (Ajouter)** pour en créer un nouveau.
2. Dans l'onglet **Categories (Catégories)**, définissez l'action sur **override (contrôle prioritaire)** pour chaque catégorie demandant un mot de passe.
3. Renseignez les sections restantes du profil de Filtrage des URL, puis cliquez sur **OK (OK)** pour enregistrer le profil.

**STEP 6 |** Appliquez le profil de filtrage des URL à la ou aux règles de politique de Sécurité qui autorisent l'accès aux sites demandant un mot de passe de contrôle prioritaire pour l'accès.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et sélectionnez la politique de Sécurité adéquate pour la modifier.
2. Cliquez sur l'onglet **Actions** puis, dans la section **Profile Setting (Paramètre de profil)**, cliquez sur la liste déroulante **URL Filtering (Filtrage des URL)** et sélectionnez le profil.
3. Cliquez sur **OK (OK)** pour enregistrer les paramètres.

**STEP 7 |** Enregistrer la configuration.

Cliquez sur **Commit (Valider)**.

# Empêcher le hameçonnage des informations d'identification

Les sites d'hameçonnage sont des sites auxquels les pirates donnent une apparence légitime dans le but de voler les informations des utilisateurs, particulièrement les informations d'identification d'entreprise qui procurent l'accès à votre réseau. Lorsqu'un e-mail de hameçonnage pénètre dans un réseau, il suffit qu'un seul utilisateur clique sur le lien et saisisse ses informations d'identification pour mettre une violation en branle. Vous pouvez détecter et détecter les attaques par hameçonnage en cours et ainsi empêcher le vol de vos informations d'identification, en contrôlant les sites sur lesquels les utilisateurs peuvent transmettre leurs informations d'identification d'entreprise selon la catégorie d'URL du site. Vous pouvez ainsi empêcher les utilisateurs de transmettre leurs informations d'identifications à des sites non approuvés, tout en leur permettant de continuer de les transmettre aux sites de l'entreprise ou aux sites approuvés.

La prévention du hameçonnage des informations d'identification passe par l'analyse des noms d'utilisateur et des mots de passe transmis aux sites Web et leur comparaison aux informations d'identification d'entreprise valides. Vous pouvez choisir les sites Web auxquels vous souhaitez autoriser ou bloquer l'envoi des informations d'identification d'entreprise selon la catégorie d'URL du site Web. Lorsque le pare-feu détecte qu'un utilisateur tente de soumettre des informations d'identification à un site d'une catégorie faisant l'objet d'une restriction, il affiche une page de réponse d'interdiction qui empêche l'utilisateur de transmettre ces informations d'identification ou présente une page permettant de continuer qui avertit l'utilisateur de ne pas soumettre ses informations d'identification à des sites appartenant à certaines catégories d'URL, tout en lui permettant tout de même de poursuivre la transmission de ses informations d'identification. Vous pouvez customize these block pages (personnaliser ces pages de blocage) pour qu'elles informent les utilisateurs qu'ils ne doivent pas réutiliser leurs informations d'identification d'entreprise, même sur des sites légitimes absents de hameçonnage.

Pour activer la prévention de l'hameçonnage des informations d'identification, vous devez configurer à la fois User-ID (ID utilisateur) pour détecter lorsque les utilisateurs soumettent des informations d'identification de l'entreprise valides à un site (par opposition aux informations d'identification personnelles) et le URL Filtering (Filtrage d'URL) pour spécifier les catégories d'URL dans lesquelles vous souhaitez empêcher les utilisateurs d'entrer leurs informations d'identification de l'entreprise. Les rubriques suivantes décrivent les différentes méthodes que vous pouvez utiliser pour détecter les soumissions d'informations d'identification et fournissent des instructions pour la configuration de la protection contre le hameçonnage des informations d'identification.

- Méthodes de vérification des soumissions d'informations d'identification de l'entreprise
- Configurer la détection des informations d'identification avec l'agent User-ID de Windows
- Configurer la prévention contre le hameçonnage des informations d'identification

## Méthodes de vérification des soumissions d'informations d'identification de l'entreprise

Avant de set up credential phishing prevention (Configurer la prévention de l'hameçonnage des informations d'identification), décidez quelle méthode vous souhaitez que le pare-feu utilise pour vérifier si des informations d'identification de l'entreprise valides ont été envoyées à une page web.

| Méthode de vérification des informations d'identification envoyées | Configuration requise pour la configuration de l'User-ID | Comment cette méthode détecte-t-elle les noms d'utilisateur et/ou les mots de passe des entreprises que les utilisateurs soumettent à des sites Web ? |
|---|---|---|
| mappage de groupe | Configuration du Mappage de groupe sur le pare-feu | Le pare-feu vérifie si le nom d'utilisateur qu'un utilisateur saisit sur un site restreint correspond à un nom d'utilisateur d'entreprise valide.<br><br>Pour ce faire, le pare-feu fait correspondre le nom d'utilisateur saisi à la liste des noms d'utilisateur dans sa table de mappage utilisateur / groupe pour détecter quand les utilisateurs saisissent un nom d'utilisateur sur des sites d'une catégorie restreinte.<br><br>Cette méthode ne vérifie que les envois de noms d'utilisateur d'entreprise en fonction de l'appartenance à un groupe LDAP, ce qui simplifie la configuration, mais l'expose davantage aux faux positifs. |
| Mappage des adresses IP aux utilisateurs | Mappages des adresses IP aux noms d'utilisateurs identifiés via le Mappage des utilisateurs, GlobalProtect, ou la Politique d'authentification et le portail d'authentification. | Le pare-feu vérifie si le nom d'utilisateur saisi par un utilisateur sur un site restreint correspond à l'adresse IP du nom d'utilisateur utilisé pour la connexion.<br><br>Pour ce faire, le pare-feu fait correspondre l'adresse IP du nom d'utilisateur utilisé pour la connexion et le nom d'utilisateur soumis à un site Web à sa table de mappage des adresses IP aux utilisateurs pour détecter le moment où les utilisateurs soumettent leurs noms d'utilisateur d'entreprise à des sites d'une catégorie restreinte.<br><br>Comme cette méthode correspond à l'adresse IP du nom d'utilisateur utilisé pour la connexion à la session par rapport à la table de mappage adresse IP-nom d'utilisateur, elle constitue une méthode efficace pour détecter les soumissions de noms d'utilisateur d'entreprise, mais pas la soumission de mots de passe d'entreprise. Si vous souhaitez détecter la soumission d'un nom d'utilisateur et d'un mot de passe d'entreprise, vous devez utiliser la méthode de filtrage des informations d'identification de domaine. |
| Filtre d'informations d'identification de domaine | Agent User-ID Windows configuré avec le module complémentaire de service d'informations | Le pare-feu vérifie si le nom d'utilisateur et le mot de passe soumis par un utilisateur correspondent au nom d'utilisateur et au mot de passe d'entreprise de ce même utilisateur.<br><br>Pour ce faire, le pare-feu doit être capable de faire correspondre les soumissions d'informations d'identification à des noms d'utilisateur et des mots de passe d'entreprise valides et de vérifier que le nom |

| Méthode de vérification des informations d'identification envoyées | Configuration requise pour la configuration de l'User-ID | Comment cette méthode détecte-t-elle les noms d'utilisateur et/ou les mots de passe des entreprises que les utilisateurs soumettent à des sites Web ? |
|---|---|---|
| | d'identification User-ID<br>- ET -<br>Mappages des adresses IP aux noms d'utilisateurs identifiés via le Mappage des utilisateurs, GlobalProtect, ou la Politique d'authentification et le portail d'authentification. | d'utilisateur soumis correspond à l'adresse IP du nom d'utilisateur utilisé pour la connexion comme suit :<br>• **Pour détecter les noms d'utilisateur et les mots de passe d'entreprise** : le pare-feu récupère un masque de bits sécurisé, appelé ***filtre bloom***, à partir d'un agent User-ID Windows équipé du module d'extension de service d'identification utilisateur. Ce service complémentaire analyse votre répertoire pour y trouver des hachages de noms d'utilisateur et de mots de passe et les déconstruit en un masque de bits sécurisé (le filtre bloom) et le délivre à l'agent User-ID Windows. Le pare-feu extrait le filtre bloom de l'agent User-ID Windows à intervalles réguliers. Chaque fois qu'il détecte la soumission, par un utilisateur, d'informations d'identification à une catégorie restreinte, il reconstruit le filtre bloom et recherche un hachage de nom d'utilisateur et de mot de passe correspondant. Le pare-feu peut uniquement se connecter à un agent User-ID Windows qui exécute le module complémentaire des informations d'identification User-ID.<br>• **Pour vérifier que les informations d'identification appartiennent au nom d'utilisateur utilisé pour la connexion** : Le pare-feu recherche un mappage entre l'adresse IP du nom d'utilisateur utilisé pour la connexion et le nom d'utilisateur détecté dans sa table de mappage des adresses IP aux noms d'utilisateur.<br>Pour en savoir plus sur le fonctionnement de la méthode d'identification de domaine et sur les conditions requises pour activer ce type de détection, reportez-vous à la section Configurer la détection des informations d'identification avec l'agent User-ID Windows. |

## Configurer la détection des identifiants avec l'agent User-ID de Windows

La détection du filtre d'informations d'identification de domaine permet au pare-feu de détecter les mots de passe qui ont été soumis à des pages Web. Cette méthode de détection des identifiants exige que l'agent User-ID Windows et le service d'informations d'identification User-ID, un module

d'extension de l'agent User-ID, soient installés sur un ***Read-Only Domain Controller (contrôleur de domaine en lecture seule ; RODC)***.

***La méthode de détection des identifiants de domaine est prise en charge avec l'agent User-ID Windows uniquement. Vous ne pouvez pas utiliser l'agent User-ID intégré à PAN-OS pour configurer cette méthode de détection des informations d'identification.***

Un RODC est un serveur Microsoft Windows qui conserve une copie en lecture seule d'une base de données Active Directory qu'un contrôleur de domaine héberge. Lorsque le contrôleur de domaine se trouve au siège social d'une entreprise, les RODC peuvent être déployés à des emplacements réseau distants pour fournir les services d'authentification locale. Il peut être utile d'installer l'agent User-ID sur un RODC pour diverses raisons : l'accès à l'annuaire du contrôleur de domaine n'est pas requis pour activer la détection des informations d'identification et vous pouvez prendre en charge la détection des informations d'identification pour un ensemble d'utilisateurs restreint ou cible. Étant donné que l'annuaire qu'héberge le RODC est en lecture seule, son contenu est protégé sur le contrôleur de domaine.

***Comme vous devez installer l'agent User-ID Windows sur le RODC pour utiliser la détection des identifiants, il est recommandé de déployer un agent distinct à cette fin. N'utilisez pas l'agent User-ID qui est installé sur le RODC pour mapper les adresses IP à des utilisateurs.***

Après avoir installé l'agent User-ID sur un RODC, le service d'informations d'identification User-ID s'exécute en arrière-plan et analyse l'annuaire afin d'y repérer le hachage des noms d'utilisateur et des mots de passe des membres des groupes qui figurent dans la Password Replication Policy (Stratégie de réplication de mot de passe ; PRP) du RODC. Vous pouvez définir les membres que vous souhaitez voir sur la liste. Le service d'informations d'identification User-ID prend ensuite les hachages de mots de passe et les noms d'utilisateur recueillis et déconstruit les données dans un type de masque de bits que l'on appelle un ***filtre de Bloom***. Les filtres de Bloom sont des structures de données compactes qui procurent un moyen sécuritaire de vérifier si un élément (un hachage de mot de passe ou un nom d'utilisateur) fait partie d'un ensemble d'éléments (l'ensemble des informations d'identification que vous avez approuvées aux fins de réplication dans le RODC). Le service d'identifiants User-ID transfère le filtre de Bloom à l'agent User-ID Windows ; le pare-feu récupère le dernier filtre de Bloom auprès de l'agent User-UD à des intervalles réguliers et l'utilise pour détecter tout envoi du hachage d'un mot de passe ou d'un nom d'utilisateur. Selon vos paramètres, le pare-feu bloque, alerte ou autorise l'envoi de mots de passe valides aux pages Web ou présente aux utilisateurs une page de réponse les avertissant des risques d'hameçonnage, tout en les laissant continuer l'envoi.

Tout au long de ce processus, l'agent User-ID ne consigne ni expose aucun hachage de mot de passe et ne transmet aucun hachage de mot de passe au pare-feu. Une fois les hachages de mot de passe déconstruits en un filtre de Bloom, il n'est plus possible de les récupérer.

**STEP 1 |** Configure user mapping using the Windows User-ID agent (Configuration du mappage d'utilisateur à l'aide de l'agent User-ID Windows)

> ***Pour activer la détection des identifiants, vous devez installer l'agent User-ID Windows sur un RODC. Consultez la** grille de compatibilité **pour obtenir une liste des serveurs pris en charge. Installez un agent User-ID distinct à cette fin.***

Points importants à ne pas oublier lors de la configuration de User-ID dans le but d'activer la détection du filtre d'informations d'identification de domaine :

- Étant donné que l'efficacité de la détection de l'hameçonnage des informations d'identification dépend de la configuration de votre RODC, assurez-vous de toujours passer en revue les pratiques exemplaires et les recommandations relatives à l'administration des RODC.
- Téléchargez les mises à jour logicielles de User-ID :
  - Programme d'installation de l'agent User-ID Windows : UaInstall-x.x.x-x.msi.
  - Programme d'installation du service d'informations d'identification de l'agent User-ID Windows : UaCredInstall64-x.x.x-x.msi.
- Installez l'agent User-ID et le service d'informations d'identification de l'agent User-ID sur un RODC en utilisant un compte qui dispose des autorisations nécessaires pour lire Active Directory via LDAP (l'agent User-ID doit également détenir cette autorisation).
  - Le service d'informations d'identification de l'agent User-ID exige la permission d'ouvrir une session au compte de système local. Pour obtenir de plus amples informations, consultez créer un compte de service dédié pour l'agent User-ID.
  - Le compte de service doit être membre du groupe d'administrateurs local sur le RODC. Pour plus d'informations, reportez-vous au lien suivant.

**STEP 2 |** Activez l'option de partages des informations sur l'agent User-ID et le service d'informations d'identification de l'agent User-ID (qui s'exécute en arrière-plan pour analyser les informations d'identification autorisées).

1. Sur le serveur RODC, lancez l'agent User-ID.
2. Sélectionnez **Setup (Configuration)** et modifiez la section Setup (Paramétrage).
3. Sélectionnez l'onglet **Credentials (Informations d'identification)**. Cet onglet n'apparaît que si vous avez déjà installé le service d'informations d'identification de l'agent User-ID.
4. Sélectionnez **Import from User-ID Credential Agent (Importer à partir de l'agent d'informations d'identification User-ID)**. Cette sélection permet à l'agent User-ID d'importer le filtre de Bloom que l'agent d'informations d'identification crée pour représenter les utilisateurs et les hachages de mot de passe correspondants.
5. Cliquez sur **OK (OK)**, **Save (Enregistrez)** vos paramètres et **Commit (Validez)**.

**STEP 3 |** Dans l'annuaire RODC, définissez le groupe d'utilisateurs pour lequel vous souhaitez prendre en charge la détection de l'envoi des informations d'identification.

- Confirmez que les groupes pour lesquels l'envoi des informations d'identification doit faire l'objet d'un contrôle ont été ajoutés au groupe Réplication de mot de passe sur un RODC autorisée.
- Vérifiez qu'aucun des groupes du groupe Réplication de mot de passe sur un RODC autorisée ne se trouve également dans le groupe Réplication de mot de passe sur un RODC refusée par défaut. Les groupes qui se trouvent dans les deux groupes ne seront pas soumis au contrôle contre l'hameçonnage des informations d'identification.

**STEP 4 |** Passez à la tâche suivante.

Set up credential phishing prevention Paramétrage de la protection contre l'hameçonnage des informations d'identification) sur le pare-feu.

## Configurer la prévention contre le hameçonnage des informations d'identification

Après avoir choisi la methods to detect corporate credential submissions (méthodes de détection des saisies d'informations d'identification d'entreprise) que vous voulez utiliser, suivez les instructions suivantes pour autoriser le pare-feu à détecter les envois d'identifications d'entreprise effectués par des utilisateurs sur des pages web et à apporter une réponse, soit en sensibilisant les utilisateurs sur les dangers de cette action, soit en bloquant l'envoi de l'identification entreprise ou soit en demandant à l'utilisateur de reconnaître les dangers du hameçonnage avant de valider la saisie.

***Avant d'activer la prévention du phishing des informations d'identification, vérifiez que le** Primary Username (nom d'utilisateur principal) **que vous configurez sur le pare-feu utilise l'attribut sAMAccountName. La prévention de l'hameçonnage des informations d'identification ne prend pas en charge d'autres attributs.***

**STEP 1 |** Si vous ne l'avez pas déjà fait, enable User-ID (Activez User-ID).

Chacune des methods to check for corporate credential submissions (méthodes de vérification des envois d'informations d'identification d'entreprise) nécessite une configuration d'ID utilisateur différente :

- Si vous comptez utiliser la méthode de mappage de groupe, qui détecte quand un utilisateur saisit un nom d'utilisateur d'entreprise valide, map users to groups (Mappage d'utilisateurs à des groupes).
- Si vous comptez utiliser une méthode de Mappage d'IP à des utilisateurs, qui détecte quand un utilisateur saisit un nom d'utilisateur d'entreprise valide et que le nom d'utilisateur correspond à l'utilisateur connecté, map IP addresses to users (Mappage des adresses IP à des utilisateurs).
- Si vous comptez utilisez la méthode de filtrage d'informations d'identification du domaine, qui détecte quand un utilisateur saisit un nom d'utilisateur d'entreprise valide et un mot de passe et que le nom d'utilisateur correspond à l'utilisateur connecté, configure credential detection with the Windows-based User-ID agent (Configuration de la Détection des informations d'identification avec l'agent User-ID Windows), map IP addresses to users (Mappage des adresses IP à des utilisateurs).

**STEP 2 |** Si vous ne l'avez pas déjà fait, Configurez un profil de filtrage des URL exemplaire pour assurer une protection contre des URL qui ont été identifiés comme hébergeant des logiciels malveillants ou du contenu dangereux.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de Sécurité)** > **URL Filtering (Filtrage des URL)** et **Add (Ajouter)** ou modifiez un profil de filtrage des URL.
2. Bloquez l'accès aux catégories d'URL suivantes : logiciels malveillants, phishing, DNS dynamiques, commandes et contrôles, extrémisme,violation des droits d'auteur, contournement des proxy et des anonymiseurs, domaine nouvellement enregistré, logiciel indésirable et URL en parking.

**STEP 3 |** Add (Ajoutez) une politique de déchiffrement pour déchiffrer le trafic que vous souhaitez surveiller pour les soumissions d'identifiants d'utilisateurs

**STEP 4 |** Configurez le profil de filtrage des URL afin qu'il détecte les saisies de noms d'utilisateurs d'entreprise valides sur des catégories d'URL autorisées.

*Le pare-feu ne vérifie pas les soumissions d'identifiants pour les sites de confiance, même si vous activez la vérification pour les catégories d'URL pour ces sites, pour fournir les meilleurs performances. Les sites de confiance représente les sites pour lesquels Palo Alto Networks n'a pas observé d'activités malicieuses ou d'attaques d'hameçonnage Les mises à jour pour cette liste de sites de confiance sont délivrées au travers des mises à jour d'Applications et de Contenu des menaces Pour obtenir une liste des App-IDs qui sont approuvés pour la détection des informations d'identification, reportez-vous à la section* App-IDs de confiance qui sautent la détection de l'envoi des informations d'identification *sur* live.paloaltonetworks.com**.**

1. Sélectionnez **User Credential Detection (Détection des informations d'identification de l'utilisateur)**.
2. Sélectionnez l'une des user credential detection methods (méthodes de détection des informations d'identification de l'utilisateur) sur les pages Web dans la liste déroulante **User Credential Detection (Détection des informations d'identification de l'utilisateur)** :

   *Confirmez que le format du nom d'utilisateur principal est identique au forme du nom d'utilisateur que la source User-ID fournit.*

   - **Use IP User Mapping (Utiliser le mappage d'utilisateur IP)** : Contrôle les saisies de noms d'utilisateurs d'entreprise valides et vérifie que le nom d'utilisateur correspond à l'utilisateur connecté à l'adresse IP source de la session. Pour cela, le pare-feu fait correspondre le nom d'utilisateur saisi et l'adresse IP source à la table de mappage adresse IP/nom d'utilisateur. Pour utiliser cette méthode, vous pouvez utiliser n'importe laquelle des méthodes de mappage d'utilisateur décrites dans map IP addresses to users (Mappaged'adresses IP à des utilisateurs).
   - **Use Domain Credential Filter (Utiliser le filtrage par informations de domaine)** : Contrôle les saisies de noms d'utilisateurs d'entreprise et mots de passe valides et vérifie que le nom d'utilisateur correspond à l'utilisateur connecté à l'adresse IP source de la session. Pour obtenir des instructions sur la configuration d'un User-ID pour activer cette méthode, reportez-vous à la section Configuration de la Détection des informations d'identification avec l'agent User-ID Windows.

- **Use Group Mapping (Utiliser le mappage de groupe)** : contrôle les saisies de nom d'utilisateur valide basé sur la table de mappage d'utilisateurs à des groupes renseignée quand vous configurez le pare-feu pour le map users to groups (Mappage d'utilisateurs à des groupes).

  Avec le mappage de groupe, vous pouvez appliquer la détection des informations d'identification à toute partie du répertoire, ou à un groupe spécifique, comme le département informatique qui aura accès à vos applications les plus sensibles.

  *Cette méthode est susceptible de générer des faux positifs dans des environnements où les noms d'utilisateurs ne sont pas structurés de manière unique. Pour cette raison, vous devriez utiliser cette méthode dans le seul but de protéger les comptes utilisateurs de haute valeur.*

3. Sélectionnez le **Degré de gravité d'enregistrement des détections de nom d'utilisateur valide** que le pare-feu utilise pour consigner la détection des saisies d'informations d'identification d'entreprise. Par défaut, le pare-feu consigne ces événements en tant que gravité moyenne.

**STEP 5 |** Bloquez (ou signalez) les tentatives de saisies d'informations d'identification sur des sites autorisés.

1. Sélectionnez **Categories (Catégories)**.
2. Pour chaque catégorie pour laquelle l'**Site Access (Accès au site)** est autorisé, choisissez le comportement que vous voulez adopter pour les **User Credential Submissions (saisies d'informations d'identification entreprise)** :
   - **alert (alerter)** - Autorise les utilisateurs à saisir des informations d'identification sur le site Web, mais génère un journal de Filtrage des URL chaque fois qu'un utilisateur saisit des informations d'identification sur les sites de cette catégorie.
   - **allow (autoriser)** (par défaut) – Autorise les utilisateurs à saisir des informations d'identification sur le site Web.
   - **block (bloquer)** - Empêche les utilisateurs de saisir des informations d'identification sur le site Web. Quand un utilisateur essaie de saisir des informations d'identification, le pare-feu affiche la Page de Blocage Anti-Hameçonnage, empêchant la saisie d'informations d'identification.
   - **continue (continuer)** - Affiche la Page de réponse Invitant à Continuer Anti-Hameçonnage aux utilisateurs essayant de saisir des informations d'identification. Les utilisateurs doivent sélectionner Continuer sur la page de réponse pour poursuivre leur saisie.
3. Sélectionnez **OK** pour enregistrer le profil de filtrage des URL.

**STEP 6 |** Appliquez le profil de filtrage des URL avec les réglages de détection des informations d'identification à vos règles de politiques de sécurité.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et **Add (ajoutez)** ou modifiez une règle de politique de sécurité.
2. Dans l'onglet **Actions**, définissez le **Profile Type (Type de profil)** sur **Profiles (Profils)**.
3. Sélectionnez le nouveau profil de **URL Filtering (Filtrage des URL)** ou celui mis à jour à associer à votre règle de politique de sécurité.
4. Cliquez sur **OK** pour enregistrer la règle de politique de sécurité.

**STEP 7 |** **Commit (Validez)** la configuration.

**STEP 8 |** Surveillez les saisies des informations d'identification que le pare-feu détecte.

*Select **ACC > Hosts Visiting Malicious URLs (hôtes visitant des URLS malveillantes)** afin d'afficher la quantité d'utilisateurs ayant visité des sites malveillants ou d'hameçonnage.*

Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **URL Filtering (Filtrage des URL)**.

La nouvelle colonne **Credential Detected (Informations d'identification détectées)** indique les événements où le pare-feu a détecté un requête HTTP Post incluant des informations d'identifications valides.

Pour afficher cette colonne, placez la souris sur n'importe quelle colonne et cliquez sur la flèche pour sélectionner les colonnes à afficher).

Les détails des entrées du journal indiquent également les saisies d'informations d'identification.

**STEP 9 |** Confirmation et dépannage des détections de saisies d'informations d'identification.

- Servez-vous de la commande CLI suivante pour voir les statistiques des détections de saisies d'informations d'identification :

```
> show user credential-filter statistics
```

La sortie pour cette commande varie selon la méthode configurée de détection par le pare-feu des saisies d'informations d'identification. Par exemple, si la méthode de Filtrage par Informations de Domaine est configurée pour tout profil de filtrage des URL, une liste d'agents User-ID ayant transféré un filtre de Bloom vers le pare-feu est affichée, ainsi que le nombre d'informations d'identification contenue dans ce filtre de Bloom.

- (Uniquement pour la méthode de Mappage de Groupe) - Servez-vous de la commande CLI suivante pour voir les informations de mappage de groupe, dont le nombre de profils de filtrage d'URL avec la détection d'informations d'identification de mappage de groupe activée,

ainsi que les noms d'utilisateurs des membres du groupe ayant tenté de saisir des informations d'identification sur des sites restreints :

```
> show user group-mapping statistics
```

- (Uniquement pour la méthode de Filtrage par Informations de Domaine) - Servez-vous de la commande CLI suivante pour voir tous les agents User-ID Windows qui envoient des mappages au pare-feu :

  ```
  > show user user-id-agent state all
  ```

  La sortie pour cette commande affiche maintenant la quantité de filtre de Bloom incluant le nombre de mises à jour de filtre de Bloom que le pare-feu a reçu de chaque agent, la notification d'échecs de mises à jour de filtre de Bloom le cas échéant, et le nombre de secondes écoulées depuis la dernière mise à jour de filtre de Bloom.
- (Uniquement pour la méthode de Filtrage par Informations de Domaine) - L'agent User-ID Windows affiche des messages de journal mentionnant des transmissions de filtre de Bloom vers le pare-feu. Dans l'interface agent de User-ID, sélectionnez **Monitoring (Surveillance)** > **Logs (Journaux)**.

# Mise en œuvre de la recherche sécurisée

De nombreux moteurs de recherche incluent un paramètre de recherche sécurisée qui filtre les images et vidéos réservées aux adultes dans le trafic renvoyé d'une recherche. Vous pouvez autoriser le pare-feu à bloquer des résultats de la recherche si l'utilisateur final n'utilise pas les paramètres de recherche sécurisée les plus stricts dans sa recherche, et vous pouvez également mettre en œuvre la recherche sécurisée transparente pour vos utilisateurs. Le pare-feu peut appliquer la recherche sécurisée pour les moteurs de recherche suivants : Google, Yahoo, Bing, Yandex et YouTube. Veuillez prendre en considération qu'il s'agit d'un paramètre visant à fournir le meilleur résultat possible et les fournisseurs de services ne garantissent nullement que son fonctionnement soit compatible avec tous les sites Web et que les moteurs de recherche classifient les sites comme sécurisés ou non sécurisés (non Palo Alto Networks).

Pour utiliser cette fonctionnalité, vous devez activer l'option **Safe Search Enforcement (Application de la recherche sécurisée)** dans un profil de Filtrage d'URL et l'attacher à une règle de politique de sécurité. Le pare-feu bloque alors tout trafic renvoyé d'une recherche correspondant qui n'utilise pas les paramètres de recherche sécurisée les plus stricts. Deux méthodes de blocage des résultats de la recherche sont possibles :

- Block Search Results when Strict Safe Search is not Enabled (Blocage des résultats de la recherche n'utilisant pas des paramètres de recherche sécurisée stricts) : lorsqu'un utilisateur final tente d'effectuer une recherche sans activer au préalable les paramètres de recherche sécurisée les plus stricts, le pare-feu bloque les résultats de la recherche et affiche la page de blocage de la recherche sécurisée du filtrage des URL. Par défaut, cette page inclut une URL vers les paramètres du moteur de recherche afin de configurer la recherche sécurisée.
- Transparently Enable Safe Search for Users (Activation de la mise en œuvre de la recherche sécurisée transparente) : lorsqu'un utilisateur final tente d'effectuer une recherche sans activer au préalable les paramètres de recherche sécurisée les plus stricts, le pare-feu bloque les résultats de la recherche avec un code d'état HTTP 503 et redirige la recherche vers une URL incluant les paramètres de recherche sécurisée. Vous activez cette fonctionnalité en important une nouvelle page de blocage de la recherche sécurisée du filtrage des URL contenant le Javascript de réécriture de l'URL de recherche afin qu'elle inclue les paramètres de recherche sécurisée stricts. Dans cette configuration, les utilisateurs ne voient pas la page de blocage mais sont automatiquement redirigés vers une recherche qui applique les options de recherche sécurisée les plus strictes. Cette mise en œuvre de la recherche sécurisée est prise en charge pour les recherches Google, Yahoo et Bing.

Comme les recherches sécurisées varient selon les moteurs de recherche, commencez par examiner les différentes méthodes de mise en œuvre de la recherche sécurisée. Ensuite, appliquez la recherche sécurisée de l'une des deux manières suivantes : bloquez les résultats de la recherche lorsque la recherche sécurisée est désactivée ou activer de manière transparente la recherche sécurisée pour vos utilisateurs.

- Réglages de la recherche sécurisée pour les moteurs de recherche
- Blocage des résultats de la recherche n'utilisant pas des paramètres de recherche sécurisée stricts
- Activation de la mise en œuvre de la recherche sécurisée transparente

# Réglages de la recherche sécurisée pour les moteurs de recherche

Les réglages de la recherche sécurisée varient selon les moteurs de recherche—examinez les réglages suivants pour en savoir plus.

| Moteur de recherche | Description du paramètre de recherche sécurisée |
|---|---|
| Google/YouTube | Permet une recherche sécurisée sur un ordinateur ou un réseau via une adresse IP de recherche sécurisée de Google :<br><br>**Mise en œuvre de la recherche sécurisée pour des recherches Google sur un ordinateur**<br><br>Dans les Paramètres de recherche Google, le paramètre **Filter explicit results (Filtrer les résultats explicites)** active la fonctionnalité de recherche sécurisée. Lorsqu'elle est activée, le paramètre est enregistré dans un cookie de navigateur sous la forme **FF=** et est transmis au serveur chaque fois que l'utilisateur effectue une recherche Google.<br><br>L'ajout de **`safe=active`** à une URL de recherche Google permet également d'activer les paramètres de recherche sécurisée les plus stricts.<br><br>**Mise en œuvre de la recherche sécurisée pour des recherches Google et YouTube à l'aide d'une adresse IP virtuelle**<br><br>Google fournit des serveurs qui verrouillent les paramètres SafeSearch (forcesafesearch.google.com) dans chaque recherche Google et YouTube. En ajoutant une entrée DNS pour **`www.google.com`** et **`www.youtube.com`** (et d'autres sous-domaines nationaux Google et YouTube) qui contient un enregistrement CNAME pointant sur **`forcesafesearch.google.com`** à la configuration de votre serveur DNS, vous êtes assuré que tous les utilisateurs de votre réseau utilisent des paramètres de recherche sécurisée stricts chaque fois qu'ils effectuent une recherche Google ou YouTube. N'oubliez toutefois pas que cette solution n'est pas compatible avec la mise en œuvre de la recherche sécurisée sur le pare-feu. Par conséquent, si vous utilisez cette option pour forcer la recherche sécurisée sur Google, la meilleure pratique consiste à bloquer l'accès aux autres moteurs de recherche sur le pare-feu en créant des catégories d'URL personnalisées et en les ajoutant à la liste d'interdiction du profil de filtrage des URL. |

| Moteur de recherche | Description du paramètre de recherche sécurisée |
| --- | --- |
| |  <br>• *PAN-OS prend en charge l'application de la recherche sécurisée pour YouTube par l'insertion d'en-têtes HTTP. L'insertion d'en-tête HTTP n'est actuellement pas prise en charge pour HTTP/2. Pour appliquer la recherche sécurisée sur YouTube,* Inspection d'App-ID et HTTP/2 *il faut déclasser les connexions HTTP/2 en HTTP/1.1 en utilisant la fonction* ***Strip ALPN (Enlever l'ALPN)*** *dans le profil de décryptage approprié.*<br>• *Si vous envisagez d'utiliser la solution Google Lock SafeSearch, pensez à configurer un proxy DNS (****Network (Réseau)*** *>* ***DNS Proxy (Proxy DNS)****) et à définir la source d'héritage sur l'interface de Couche 3 sur laquelle le pare-feu reçoit des paramètres DNS du fournisseur de services via DHCP. Vous devez configurer le proxy DNS avec des* ***Static Entries (Entrées statiques)*** *pour www.google.com et www.youtube.com, en utilisant l'adresse IP locale du serveur forcesafesearch.google.com.* |
| Yahoo | Permet une recherche sécurisée sur un ordinateur uniquement. Les Préférences de recherche Yahoo incluent trois paramètres SafeSearch : **Strict**, **Moderate (Modéré)** ou **Off (Désactivé)**. Lorsqu'elle est activée, le paramètre est enregistré dans un cookie de navigateur sous la forme `vm=` et est transmis au serveur chaque fois que l'utilisateur effectue une recherche Yahoo. |

| Moteur de recherche | Description du paramètre de recherche sécurisée |
|---|---|
| | L'ajout de `vm=r` à une URL de recherche Yahoo permet également d'activer les paramètres de recherche sécurisée les plus stricts.<br><br>*Lorsque vous effectuez une recherche sur Yahoo Japan (**`yahoo.co.jp`**) alors que vous êtes connecté à un compte Yahoo, les utilisateurs finaux doivent également activer l'option **Lock (Verrouiller) SafeSearch**.* |
| Bing | Permet une recherche sécurisée sur un ordinateur ou via leur programme Bing in the Classroom. Les Paramètres Bing incluent trois paramètres SafeSearch : **Strict**, **Moderate (Modéré)** ou **Off (Désactivé)**. Lorsqu'elle est activée, le paramètre est enregistré dans un cookie de navigateur sous la forme **`adlt=`** et est transmis au serveur chaque fois que l'utilisateur effectue une recherche Bing.<br><br>L'ajout de **`adlt=strict`** à une URL de recherche Bing permet également d'activer les paramètres de recherche sécurisée les plus stricts.<br><br>Le moteur de recherche SSL Bing n'applique pas les paramètres d'URL de recherche sécurisée et vous devez donc prendre en compte le blocage de Bing sur SSL pour une mise en œuvre complète de la recherche sécurisée. |

## Blocage des résultats de la recherche n'utilisant pas des paramètres de recherche sécurisée stricts

Par défaut, si vous activez la mise en œuvre de la recherche sécurisée, lorsqu'un utilisateur final effectue une recherche sans utiliser les paramètres de recherche sécurisée les plus stricts, le pare-feu bloque les résultats de la recherche et affiche la page de blocage de la recherche sécurisée du filtrage des URL. Cette page inclut un lien vers la page des paramètres de recherche du moteur de recherche concerné afin que l'utilisateur final puisse activer les paramètres de recherche sécurisée. Si vous envisagez d'utiliser cette méthode de mise en œuvre de la recherche sécurisée par défaut, vous devez transmettre la politique aux utilisateurs finaux avant de l'appliquer. Reportez-vous à la section Réglages de la recherche sécurisée pour les moteurs de recherche pour plus de détails sur la mise en œuvre de la recherche sécurisée de chaque moteur de recherche. Vous pouvez éventuellement procéder à la customize the URL Filtering response pages (Personnalisation des pages de réponse de filtrage des URL).

Alternativement, vous pouvez transparently enable safe search for users (activer de manière transparente la recherche sécurisée pour les utilisateurs) afin qu'ils n'aient pas à configurer manuellement les paramètres.

**STEP 1 |** Activez la mise en œuvre de la recherche sécurisée dans le profil Filtrage des URL.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **URL Filtering (Filtrage des URL)**.
2. Sélectionnez un profil existant pour le modifier ou clonez le profil par défaut pour en créer un nouveau.
3. Dans l'onglet **Settings (Paramètres)**, cochez la case **Safe Search Enforcement (Mise en œuvre de la recherche sécurisée)** pour l'activer.
4. (Facultatif) Limitez les utilisateurs à des moteurs de recherche spécifiques :
   1. Dans l'onglet **Categories (Catégories)**, définissez la catégorie **search-engines** sur **block (bloquer)**.
   2. Pour chaque moteur de recherche dont vous souhaitez autoriser l'accès aux utilisateurs finaux, saisissez l'adresse Web dans la zone de texte **Allow List (Liste d'autorisation)**. Par exemple, pour autoriser les utilisateurs à accéder aux recherches Google et Bing uniquement, saisissez ce qui suit :

      **`www.google.com`**

      **`www.bing.com`**
5. Si nécessaire, configurez d'autres paramètres pour :
   - Définir l'accès au site pour chaque catégorie d'URL.
   - Définir les listes d'autorisation et de blocage pour spécifier les sites Web qui doivent toujours être bloqués ou autorisés, quelle que soit la catégorie d'URL.
6. Cliquez sur **OK** pour enregistrer le profil.

**STEP 2 |** Ajoutez le profil de filtrage des URL à la règle de Politique de sécurité qui autorise le trafic de clients de la zone approuvée vers Internet.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et sélectionnez une règle à laquelle appliquer le profil de Filtrage des URL que vous venez d'activer pour la mise en œuvre de la recherche sécurisée.
2. Dans l'onglet **Actions**, sélectionnez le profil **URL Filtering (Filtrage des URL)**.
3. Cliquez sur **OK (OK)** pour enregistrer la Règle de politique de sécurité.

**STEP 3 |** Activez le décryptage du proxy de transfert SSL.

Étant donné que la plupart des moteurs de recherche cryptent leurs résultats de recherche, vous devez activer le Décryptage du proxy de transfert SSL afin que le pare-feu puisse inspecter le trafic et détecter les paramètres de recherche sécurisée.

1. Ajoutez une catégorie d'URL personnalisée pour les sites de recherche :
   1. Sélectionnez **Objects (Objets)** > **Custom Objects (Objets personnalisés)** > **URL Category (Catégorie d'URL)** et cliquez sur **Add (Ajouter)** pour ajouter une catégorie personnalisée.
   2. Saisissez un **Name (Nom)** pour la catégorie, par exemple DécryptageMoteurRecherche.
   3. **Add (Ajoutez)** les sites suivants à la liste Sites :

      **`www.bing.*`**

      **`www.google.*`**

      **`search.yahoo.*`**
   4. Cliquez sur **OK (OK)** pour enregistrer l'objet de catégorie d'URL personnalisée.
2. Suivez les étapes pour configure SSL Forward Proxy (Configurer le proxy de transfert SSL).
3. Dans l'onglet **Service/URL Category (Catégorie de service/d'URL)** de la règle de politique de décryptage, cliquez sur **Add (Ajouter)** pour ajouter la catégorie d'URL personnalisée que vous venez de créer, puis cliquez sur **OK (OK)**.

**STEP 4 |** (Recommandé) Bloquez le trafic de recherche Bing exécuté sur SSL.

Le moteur de recherche SSL Bing n'appliquant pas les paramètres de recherche sécurisée, vous devez refuser toutes les sessions Bing exécutées sur SSL pour obtenir une mise en œuvre de la recherche sécurisée complète.

1. Ajoutez une catégorie d'URL personnalisée pour Bing :
   1. Sélectionnez **Objects (Objets)** > **Custom Objects (Objets personnalisés)** > **URL Category (Catégorie d'URL)** et cliquez sur **Add (Ajouter)** pour ajouter une catégorie personnalisée.
   2. Saisissez un **Name (Nom)** pour la catégorie, par exemple ActiverRechercheSécuriséeBing.
   3. **Add (Ajoutez)** les sites suivants à la liste Sites :

      **`www.bing.com/images/*`**

      **`www.bing.com/videos/*`**
   4. Cliquez sur **OK (OK)** pour enregistrer l'objet de catégorie d'URL personnalisée.
2. Créez un autre profil de Filtrage des URL afin qu'il bloque la catégorie personnalisée que vous venez de créer :
   1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **URL Filtering (Filtrage des URL)**.
   2. **Add (Ajoutez)** un nouveau profil et donnez-lui un **Name (Nom)** descriptif.
   3. Recherchez la catégorie personnalisée dans la liste des catégories et définissez-la sur **block (bloquer)**.
   4. Cliquez sur **OK (OK)** pour enregistrer le profil de Filtrage des URL
3. Ajoutez) une Règle de politique de sécurité pour bloquer le trafic SSL Bing :
   1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et cliquez sur **Add (Ajouter)** pour ajouter une règle de politique qui autorise le trafic de votre zone approuvée vers Internet.
   2. Dans l'onglet **Actions (Actions)**, associez le profil de Filtrage des URL que vous venez de créer pour bloquer la catégorie Bing personnalisée.
   3. Dans l'onglet **Service/URL Category (Catégorie de service/d'URL)**, **Add (ajoutez)** un **New Service (Nouveau service)** et donnez-lui un **Name (Nom)** descriptif, bingssl par exemple.
   4. Sélectionnez **TCP (TCP)** comme **Protocol (Protocole)** et définissez le **Destination Port (Port de destination)** sur 443.
   5. Cliquez sur **OK** pour enregistrer la règle.
   6. Utilisez les options **Move (Déplacer)** pour vous assurer que cette règle se situe sous la règle contenant le profil de Filtrage des URL avec la mise en œuvre de la recherche sécurisée activée.

**STEP 5 |** Enregistrer la configuration.

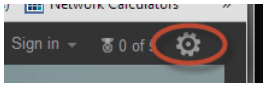
Cliquez sur **Commit (Valider)**.

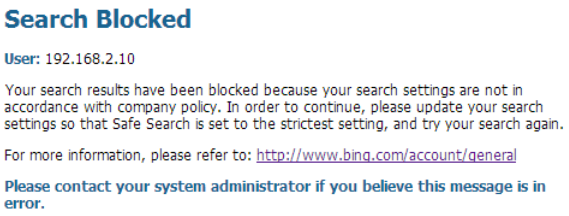
**STEP 6 |** Vérifiez la configuration de la mise en œuvre de la recherche sécurisée.

Cette étape de vérification ne s'applique que si vous utilisez des pages de blocage pour mettre en œuvre la recherche sécurisée. Si vous utilisez la mise en œuvre de la recherche sécurisée transparente, la page de blocage du pare-feu demandera la réécriture de l'URL avec les paramètres de recherche sécurisée dans la chaîne de la requête.

1. Sur un ordinateur situé derrière le pare-feu, désactivez les paramètres de recherche stricts pour l'un des moteurs de recherche pris en charge. Par exemple, sur bing.com, cliquez sur l'icône **Preferences (Préférences)** dans la barre de menus Bing.




2. Définissez l'option **SafeSearch (Recherche sécurisée)** sur **Moderate (Modérée)** ou sur **Off (Désactivée)**, puis cliquez sur **Save (Enregistrer)**.
3. Effectuez une recherche Bing et vérifiez que la page de blocage de recherche sécurisée du filtrage des URL s'affiche à la place des résultats de la recherche :




4. Utilisez le lien indiqué dans la page de blocage pour accéder aux paramètres de recherche du moteur de recherche, rétablissez la recherche sécurisée sur le paramètre le plus strict (**Strict (Strict)** pour Bing), puis cliquez sur **Save (Enregistrer)**.
5. Effectuez une nouvelle recherche dans Bing et vérifiez que les résultats de la recherche filtrés s'affichent à la place de la page de blocage.

## Activation de la mise en œuvre de la recherche sécurisée transparente

Si vous souhaitez mettre en œuvre le filtrage des résultats de la recherche avec les filtres de recherche sécurisée les plus stricts mais que vous ne souhaitez pas que vos utilisateurs finaux configurent manuellement les paramètres, vous pouvez activer une mise en œuvre de la recherche sécurisée transparente comme suit. Cette fonctionnalité est prise en charge sur les moteurs de recherche Google, Yahoo et Bing uniquement et requiert la version de contenu 475 ou ultérieure.

**STEP 1 |** Vérifiez que le pare-feu exécute la version de contenu 475 ou ultérieure.

1. Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**.
2. Consultez la section **Applications and Threats (Applications et menaces)** pour connaître la mise à jour actuelle.
3. Si le pare-feu n'exécute pas la mise à jour requise ou une mise à jour ultérieure, cliquez sur **Check Now (Vérifier maintenant)** pour récupérer la liste des mises à jour disponibles.
4. Localisez la mise à jour requise, puis cliquez sur **Download (Télécharger)**.
5. Une fois le téléchargement terminé, cliquez sur **Install (Installer)**.

**STEP 2 |** Activez la mise en œuvre de la recherche sécurisée dans le profil Filtrage des URL.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **URL Filtering (Filtrage des URL)**.
2. Sélectionnez un profil existant pour le modifier ou clonez le profil par défaut pour en créer un nouveau.
3. Dans l'onglet **Settings (Paramètres)**, cochez la case **Safe Search Enforcement (Mise en œuvre de la recherche sécurisée)** pour l'activer.
4. (Facultatif) Autorisez l'accès à des moteurs de recherche spécifiques uniquement :
   1. Dans l'onglet **Categories (Catégories)**, définissez la catégorie **search-engines** sur **block (bloquer)**.
   2. Pour chaque moteur de recherche dont vous souhaitez autoriser l'accès aux utilisateurs finaux, saisissez l'adresse Web dans la zone de texte **Allow List (Liste d'autorisation)**. Par exemple, pour autoriser les utilisateurs à accéder aux recherches Google et Bing uniquement, saisissez ce qui suit :

      **`www.google.com`**

      **`www.bing.com`**
5. Si nécessaire, configurez d'autres paramètres pour :
   - Définir l'accès au site pour chaque catégorie d'URL.
   - Define block and allow lists to specify websites that should always be blocked or allowed, regardless of URL category. (Définir les listes d'autorisation et de blocage pour spécifier les sites Web qui doivent toujours être bloqués ou autorisés, quelle que soit la catégorie d'URL.)
6. Cliquez sur **OK** pour enregistrer le profil.

**STEP 3 |** Ajoutez le profil de filtrage des URL à la règle de Politique de sécurité qui autorise le trafic de clients de la zone approuvée vers Internet.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et sélectionnez une règle à laquelle appliquer le profil de Filtrage des URL que vous venez d'activer pour la mise en œuvre de la recherche sécurisée.
2. Dans l'onglet **Actions**, sélectionnez le profil **URL Filtering (Filtrage des URL)**.
3. Cliquez sur **OK (OK)** pour enregistrer la Règle de politique de sécurité.

**STEP 4 |** (Recommandé) Bloquez le trafic de recherche Bing exécuté sur SSL.

Le moteur de recherche SSL Bing n'appliquant pas les paramètres de recherche sécurisée, vous devez refuser toutes les sessions Bing exécutées sur SSL pour obtenir une mise en œuvre de la recherche sécurisée complète.

1. Ajoutez une catégorie d'URL personnalisée pour Bing :
   1. Sélectionnez **Objects (Objets)** > **Custom Objects (Objets personnalisés)** > **URL Category (Catégorie d'URL)** et cliquez sur **Add (Ajouter)** pour ajouter une catégorie personnalisée.
   2. Saisissez un **Name (Nom)** pour la catégorie, par exemple ActiverRechercheSécuriséeBing.
   3. **Add (Ajoutez)** les sites suivants à la liste Sites :

      **`www.bing.com/images/*`**

      **`www.bing.com/videos/*`**
   4. Cliquez sur **OK (OK)** pour enregistrer l'objet de catégorie d'URL personnalisée.
2. Créez un autre profil de Filtrage des URL afin qu'il bloque la catégorie personnalisée que vous venez de créer :
   1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **URL Filtering (Filtrage des URL)**.
   2. **Add (Ajoutez)** un nouveau profil et donnez-lui un **Name (Nom)** descriptif.
   3. Recherchez la catégorie personnalisée que vous venez de créer dans la liste de catégories et définissez-la sur **block (bloquer)**.
   4. Cliquez sur **OK (OK)** pour enregistrer le profil de Filtrage des URL
3. **Add (Ajoutez)** une règle de politique de sécurité pour bloquer le trafic SSL Bing :
   1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et cliquez sur **Add (Ajouter)** pour ajouter une règle de politique qui autorise le trafic de votre zone approuvée vers Internet.
   2. Dans l'onglet **Actions (Actions)**, associez le profil de Filtrage des URL que vous venez de créer pour bloquer la catégorie Bing personnalisée.
   3. Dans l'onglet **Service/URL Category (Catégorie de service/d'URL)**, **Add (ajoutez)** un **New Service (Nouveau service)** et donnez-lui un **Name (Nom)** descriptif, bingssl par exemple.
   4. Sélectionnez **TCP** comme **Protocol (Protocole)** et définissez le **Destination Port (Port de destination)** sur **443**.
   5. Cliquez sur **OK** pour enregistrer la règle.
   6. Utilisez les options **Move (Déplacer)** pour vous assurer que cette règle se situe sous la règle contenant le profil de Filtrage des URL avec la mise en œuvre de la recherche sécurisée activée.

**STEP 5 |** Saisissez l'URL de la page de blocage de la recherche sécurisée du filtrage des URL, en remplaçant le code existant par le Javascript de réécriture des URL de recherche pour mettre en œuvre la recherche sécurisée de manière transparente.

1. Sélectionnez **Device (Équipement)** > **Response Pages (Pages de réponse)** > **URL Filtering Safe Search Block Page (Page de blocage de la recherche sécurisée du filtrage des URL)**.
2. Sélectionnez **Predefined (Prédéfinie)**, puis cliquez sur **Export (Exporter)** pour enregistrer le fichier localement.
3. Dans un éditeur HTML, remplacez l'ensemble du texte de page de blocage existant par le texte ci-dessous, puis enregistrez le fichier.

```
<html>
  <head>
    <title>Search Blocked</title>
    <meta http-equiv="Content-Type" content="text/html;
 charset=utf-8">
    <meta http-equiv="pragma" content="no-cache">
    <meta name="viewport" content="initial-scale=1.0">
    <style>
      #content {
      border:3px solid#aaa;
      background-color:#fff;
      margin:1.5em;
      padding:1.5em;
      font-family:Tahoma,Helvetica,Arial,sans-serif;
      font-size:1em;
      }
      h1 {
      font-size:1.3em;
      font-weight:bold;
      color:#196390;
      }
      b {
      font-weight:normal;
      color:#196390;
      }
    </style>
  </head>
  <body bgcolor="#e7e8e9">
    <div id="content">
      <h1>Search Blocked</h1>
      <p>
        <b>User:</b>
        <user/>
      </p>
      <p>Your search results have been blocked because your
search settings are not in accordance with company policy.
In order to continue, please update your search settings so
that Safe Search is set to the strictest setting. If you are
currently logged into your account, please also lock Safe
Search and try your search again.</p>
      <p>
        For more information, please refer to:
        <a href="<ssurl/>">
          <ssurl/>
```

```
        </a>
      </p>
      <p id="java_off"> Please enable JavaScript in your
 browser.<br></p>
      <p><b>Please contact your system administrator if you
 believe this message is in error.</b></p>
    </div>
  </body>
  <script>
    // Grab the URL that's in the browser.
    var s_u = location.href;
    //bing
    // Matches the forward slashes in the beginning, anything,
 then ".bing." then anything followed by a non greedy slash.
 Hopefully the first forward slash.
    var b_a = /^.*\/\/(.+\.bing\..+?)\//.exec(s_u);
    if (b_a) {
       s_u = s_u + "&adlt=strict";
        window.location.replace(s_u);
        document.getElementById("java_off").innerHTML = 'You
 are being redirected to a safer search!';
    }
    //google
    // Matches the forward slashes in the beginning, anything,
 then ".google." then anything followed by a non greedy slash.
 Hopefully the first forward slash.
    var g_a = /^.*\/\/(.+\.google\..+?)\//.exec(s_u);
    if (g_a) {
        s_u = s_u.replace(/&safe=off/ig,"");
        s_u = s_u + "&safe=active";
        window.location.replace(s_u);
        document.getElementById("java_off").innerHTML = 'You
 are being redirected to a safer search!';    }
    //yahoo
    // Matches the forward slashes in the beginning, anything,
 then ".yahoo."" then anything followed by a non greedy slash.
 Hopefully the first forward slash.
    var y_a = /^.*\/\/(.+\.yahoo\..+?)\//.exec(s_u);
    if (y_a) {
        s_u = s_u.replace(/&vm=p/ig,"");
        s_u = s_u + "&vm=r";
        window.location.replace(s_u);
        document.getElementById("java_off").innerHTML = 'You
 are being redirected to a safer search!';
    }
    document.getElementById("java_off").innerHTML = ' ';
  </script>
</html>
```

**STEP 6 |** Importez la page modifiée de blocage de la recherche sécurisée du filtrage des URL sur le pare-feu.

1. Pour importer la page de blocage modifiée, sélectionnez **Device (Équipement)** > **Response Pages (Pages de réponse)** > **URL Filtering Safe Search Block Page (Page de blocage de la recherche sécurisée du filtrage des URL)**.
2. Cliquez sur **Import (Importer)** puis saisissez le chemin et le nom de fichier dans le champ **Import File (Importer le fichier)** ou **Browse (Naviguez)** pour trouver le fichier.
3. (Facultatif) Sélectionnez le système virtuel sur lequel cette page d'ouverture de session sera utilisée dans la liste déroulante **Destination** ou sélectionnez **shared (Partagée)** pour la rendre disponible pour tous les systèmes virtuels.
4. Cliquez sur **OK** pour importer le fichier.

**STEP 7 |** Activez le décryptage du proxy de transfert SSL.

Étant donné que la plupart des moteurs de recherche cryptent leurs résultats de recherche, vous devez activer le décryptage du proxy de transfert SSL afin que le pare-feu puisse inspecter le trafic et détecter les paramètres de recherche sécurisée.

1. Ajoutez une catégorie d'URL personnalisée pour les sites de recherche :
   1. Sélectionnez **Objects (Objets)** > **Custom Objects (Objets personnalisés)** > **URL Category (Catégorie d'URL)** et cliquez sur **Add (Ajouter)** pour ajouter une catégorie personnalisée.
   2. Saisissez un **Name (Nom)** pour la catégorie, par exemple DécryptageMoteurRecherche.
   3. **Add (Ajoutez)** les sites suivants à la liste Sites :

      **`www.bing.*`**

      **`www.google.*`**

      **`search.yahoo.*`**
   4. Cliquez sur **OK (OK)** pour enregistrer l'objet de catégorie d'URL personnalisée.
2. Suivez les étapes pour configure SSL Forward Proxy (Configurer le proxy de transfert SSL).
3. Dans l'onglet **Service/URL Category (Catégorie de service/d'URL)** de la règle de politique de décryptage, cliquez sur **Add (Ajouter)** pour ajouter la catégorie d'URL personnalisée que vous venez de créer, puis cliquez sur **OK (OK)**.

**STEP 8 |** Enregistrer la configuration.

Cliquez sur **Commit (Valider)**.

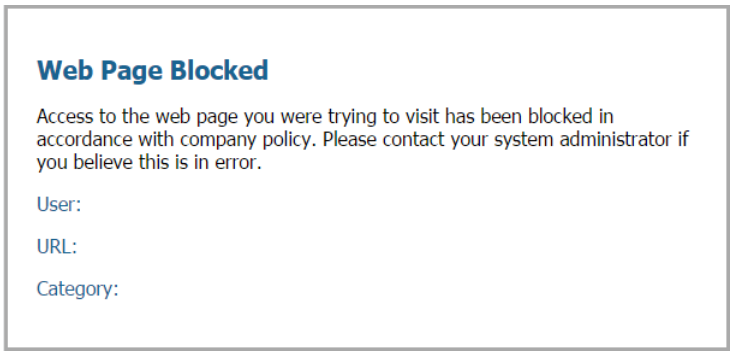
 

# Pages de réponse de filtrage des URL

Le pare-feu propose trois pages de réponse prédéfinies qui s'affichent par défaut lorsqu'un utilisateur tente d'accéder à un site appartenant à une catégorie configurée avec l'une des actions de blocage dans le profil de filtrage des URL (bloquer, continuer ou contrôle prioritaire) ou lorsque les Pages de conteneur sont activées :

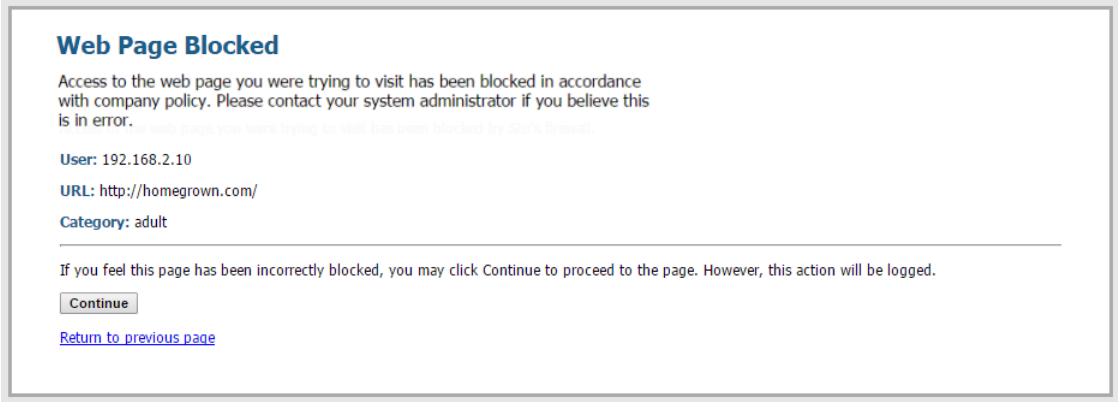
- **Page de blocage du filtrage et des correspondances de catégories des URL**

  Accès bloqué par un profil de filtrage des URL ou parce que la catégorie d'URL est bloquée par une règle de politique de Sécurité.




- **Page de maintien et de contrôle prioritaire du filtrage des URL**

  Page incluant la politique de blocage initiale permettant aux utilisateurs d'ignorer le blocage en cliquant sur **Continue (Continuer)**. Lorsque le contrôle prioritaire de l'URL par l'administrateur est activé (Allow Password Access to Certain Sites (Autoriser l'accès par mot de passe à certains sites), après avoir cliqué sur **Continue (Continuer)**, l'utilisateur doit fournir un mot de passe pour forcer la politique bloquant cette URL.

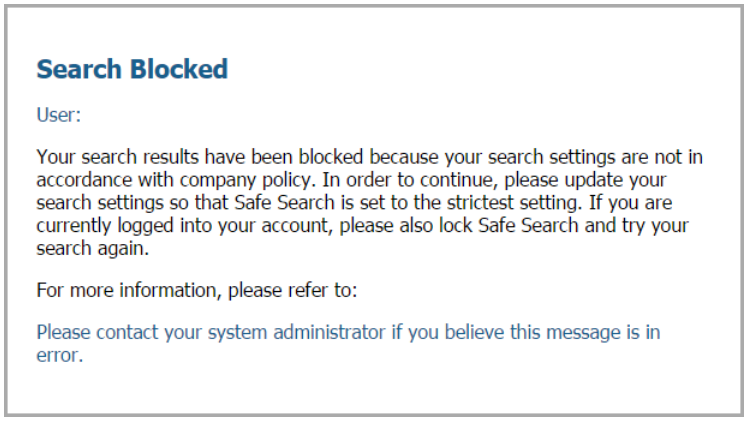



- **Page de blocage de la recherche sécurisée du filtrage d'URL**

  Accès bloqué par une règle de politique de Sécurité dotée d'un profil de filtrage des URL pour lequel l'option Mise en œuvre de la recherche sécurisée est activée (voir la section Mise en œuvre de la recherche sécurisée). Cette page est présentée à l'utilisateur si une recherche est effectuée

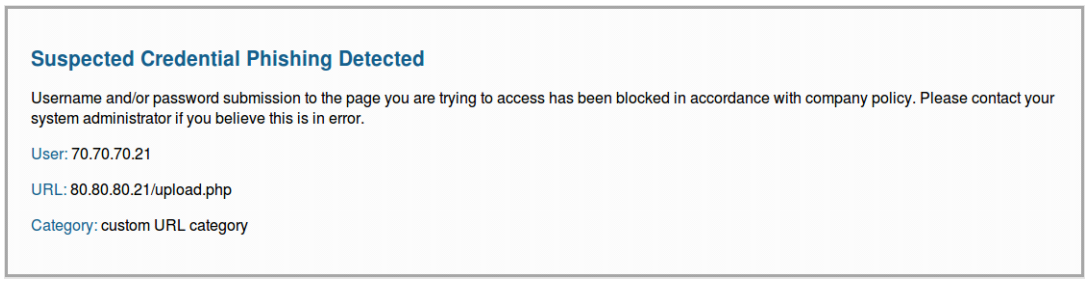
 

à l'aide de Google, Bing, Yahoo ou Yandex et que le paramètre de recherche sécurisée de son compte de moteur de recherche ou de navigateur n'est pas défini sur Strict.




- **Page de blocage anti-hameçonnage**

  Cette page s'affiche aux utilisateurs lorsqu'ils tentent de saisir des informations d'identification d'entreprise (noms d'utilisateur ou mots de passe) sur une page Web dans une catégorie sur laquelle l'envoi des informations d'identification est bloqué. L'utilisateur peut accéder au site, mais il ne peut toujours pas saisir des informations d'identification d'entreprise valides pour tous les formulaires Web associés. Pour contrôler les sites auxquels les utilisateurs envoient des informations d'identification, le pare-feu doit être configuré avec l'User-ID et être activé pour prevent credential phishing (Empêcher le hameçonnage des informations d'identification) en fonction de la catégorie d'URL.

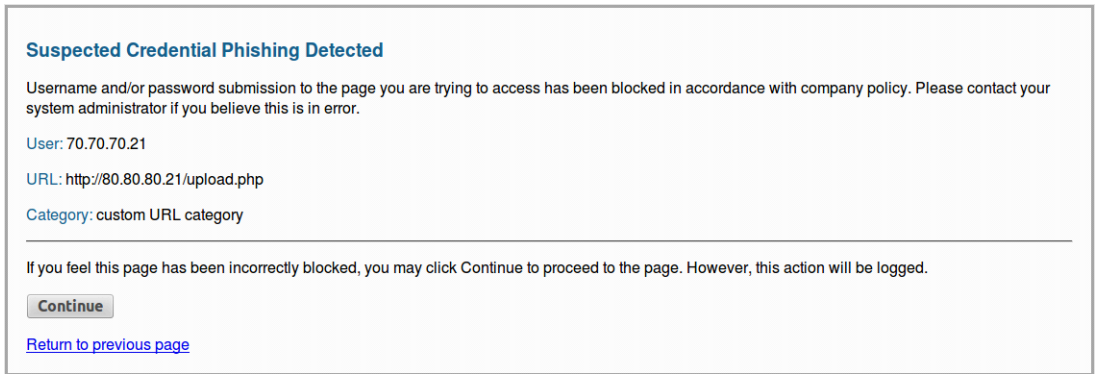



- **Page de poursuite anti-hameçonnage**

  Cette page met en garde les utilisateurs contre la transmission des informations d'identification (noms d'utilisateur et mots de passe) vers un site Web. La mise en garde des utilisateurs contre la transmission des informations d'identification peut les décourager de réutiliser les informations d'identification de l'entreprise et les informer sur les éventuelles tentatives d'hameçonnage. Ils doivent sélectionner Continuer pour saisir les informations d'identification sur le site. Pour contrôler les sites auxquels les utilisateurs envoient des informations d'identification, le pare-feu

doit être configuré avec l'User-ID et être activé pour prevent credential phishing (Empêcher le hameçonnage des informations d'identification) en fonction de la catégorie d'URL.




Vous pouvez utiliser les pages prédéfinies ou customize the URL Filtering response pages (Personnaliser des pages de réponse de filtrage des URL) pour indiquer vos politiques d'utilisation acceptables et/ou votre marque d'entreprise. Vous pouvez également utiliser les URL Filtering response page variables (Variables de page de réponse de filtrage des URL) remplacées lors de l'événement de blocage ou ajouter l'une des response page references (Références de page de réponse) prises en charge aux images, sons ou feuilles de styles externes.

*Le navigateur n'affichera pas les pages de réponse si vous avez activé votre pare-feu pour inspect SSL/TLS handshakes (inspecter les compromis SSL/TLS).*

**Table 2: Variables de page de réponse de filtrage des URL**

| Variable | Usage |
|---|---|
| <user/> | Le pare-feu remplace la variable par le nom d'utilisateur (si disponible via User-ID) ou l'adresse IP de l'utilisateur lors de l'affichage de la page de réponse. |
| <url/> | Le pare-feu remplace la variable par l'URL demandée lors de l'affichage de la page de réponse. |
| <category/> | Le pare-feu remplace la variable par la catégorie de filtrage des URL de la demande bloquée. |
| <pan_form/> | Le code HTML pour l'affichage du bouton **Continue (Continuer)** sur la page Continuer et Contrôle prioritaire du filtrage des URL. |

Vous pouvez également ajouter un code demandant au pare-feu d'afficher différents messages en fonction de la catégorie d'URL à laquelle l'utilisateur tente d'accéder. Par exemple, l'extrait de code suivant d'une page de réponse demande l'affichage du Message 1 si la catégorie d'URL est « jeux », le Message 2 si la catégorie est « voyages » ou le Message 3 si la catégorie est « enfants » :

```
var cat = "<category/>";
switch(cat)
```

```
{
 case 'games':
 document.getElementById("warningText").innerHTML = "Message 1";
 break;
 case 'travel':
 document.getElementById("warningText").innerHTML = "Message 2";
 break;
 case 'kids':
 document.getElementById("warningText").innerHTML = "Message 3";
 break;
}
```

Une seule page HTML peut être chargée sur chaque système virtuel pour chaque type de page de blocage. D'autres ressources comme des images, des sons et des feuilles de styles au format CSS, peuvent toutefois être chargées d'autres serveurs lorsque la page de réponse s'affiche dans le navigateur. Toutes les références doivent contenir une URL complète.

**Table 3: Références de page de réponse**

| Type de référence | Exemple de code HTML |
|---|---|
| Image | `<img src="http://virginiadot.org/images/Stop-Sign-gif.gif">` |
| Son | `<embed src="http://simplythebest.net/sounds/WAV/WAV_files/ movie_WAV_files/ do_not_go.wav" volume="100" hidden="true" autostart="true">` |
| Feuille de styles | `<link href="http://example.com/style.css" rel="stylesheet" type="text/css" />` |
| Lien hypertexte | `<a href="http://en.wikipedia.org/wiki/Acceptable_use_policy">View Corporate Policy</a>` |

# Personnalisation des pages de réponse de filtrage des URL

Le pare-feu fournit des URL Filtering response pages (pages de réponse de filtrage d'URL) prédéfinies qui s'affichent par défaut lorsque :

- Un utilisateur tente d'accéder à un site qui se trouve dans une catégorie dont l'accès est limité.
- Un utilisateur soumet des informations d'identification d'entreprise valides pour accéder à un site pour lequel la détection des informations d'identification est activée (Empêcher le hameçonnage des informations d'identification en fonction de la catégorie d'URL).
- Journalisez uniquement la page visitée par un utilisateur bloque une tentative de recherche.

Toutefois, vous pouvez créer vos propres pages de réponse personnalisées avec votre marque d'entreprise, les politiques d'utilisation acceptables, et les liens vers vos ressources internes.

***Les pages de réponse personnalisées qui dépassent la taille maximale prise en charge ne sont pas déchiffrées ou affichées aux utilisateurs. Dans la version 8.1.2 de PAN-OS et les versions de PAN-OS 8.1 antérieures, les pages de réponse personnalisées sur un site déchiffré ne peuvent dépasser 8 191 octets ; la taille maximale est passée à 17 999 octets dans PAN-OS 8.1.3 et les versions ultérieures.***

**STEP 1 |** Exportez la ou les pages de réponse par défaut.

1. Sélectionnez **Device (Périphérique)** > **Response Pages (Pages de réponse)**.
2. Sélectionnez le lien de la page de réponse de filtrage des URL que vous souhaitez modifier.
3. Cliquez sur la page de réponse (prédéfinie ou partagée), puis sur le lien **Export (Exporter)** et enregistrez le fichier sur votre bureau.

**STEP 2 |** Modifiez la page exportée.

1. À l'aide de l'éditeur de texte HTML de votre choix, modifiez la page :
   - Si vous souhaitez que la page de réponse fournisse des informations personnalisées sur l'utilisateur, l'URL ou la catégorie qui a été bloqué, ajoutez une ou plusieurs des response page variables (variables de la page de réponse) prises en charge.
   - Si vous souhaitez insérer des images personnalisées (comme le logo de votre entreprise), un son, une feuille de styles ou un lien vers une autre URL, par exemple vers un document décrivant votre politique d'utilisation Web acceptable, insérez une ou plusieurs des response page references (références de page de réponse) prises en charge.
2. Enregistrez la page modifiée avec un nouveau nom de fichier. Veillez à ce que la page conserve son codage UTF-8. Par exemple, dans Notepad, vous sélectionnez **UTF-8 (UTF-8)** dans la liste déroulante **Encoding (Codage)** de la boîte de dialogue Save As (Enregistrer sous).

**STEP 3 |** Importez la page de réponse personnalisée.

1. Sélectionnez **Device (Périphérique)** > **Response Pages (Pages de réponse)**.
2. Sélectionnez le lien correspondant à la page de réponse de filtrage des URL que vous avez modifiée.
3. Cliquez sur **Import (Importer)** puis saisissez le chemin et le nom de fichier dans le champ **Import File (Importer le fichier)** ou **Browse (Naviguez)** pour trouver le fichier.
4. (Facultatif) Sélectionnez le système virtuel sur lequel cette page d'ouverture de session sera utilisée dans la liste déroulante **Destination** ou sélectionnez **shared (Partagée)** pour la rendre disponible pour tous les systèmes virtuels.
5. Cliquez sur **OK** pour importer le fichier.

**STEP 4 |** Enregistrez la ou les nouvelles pages de réponse.

**Commit (Validez)** les modifications.

**STEP 5 |** Vérifiez que la nouvelle page de réponse s'affiche.

Dans un navigateur, accédez à l'URL qui déclenchera la page de réponse. Par exemple, pour afficher une page de réponse Filtrage des URL et correspondance de catégorie modifiée, accédez à l'URL pour laquelle votre politique de Filtrage des URL est définie sur bloquer.

Le pare-feu utilise les ports suivants pour afficher les pages de réponse du Filtrage des URL :

- **HTTP** : 6080
- **TLS par défaut avec certificat de pare-feu** : 6081
- **Profil SSL/TLS personnalisé** : 6082

# Journalisation de l'en-tête HTTP

Le filtrage des URL permet la visibilité et le contrôle du trafic Web sur votre réseau. Pour une meilleure visibilité sur le contenu Web, vous pouvez configurer le profil de filtrage des URL pour consigner les attributs d'en-tête HTTP inclus dans une requête Web. Lorsqu'un client demande une page Web, l'en-tête HTTP inclut les champs Utilisateur-Agent, Référant et X-Forwarded-For sous forme de paire attribut/valeur et les transmet au serveur Web. Lorsque cette option est activée pour consigner les en-têtes HTTP, le pare-feu consigne les paires attributs/valeurs suivantes dans les journaux de filtrage des URL.

*Vous pouvez utiliser les en-têtes HTTP pour gérer l'accès aux applications SaaS. Pour ce faire, vous n'avez pas besoin d'un abonnement de filtrage des URL, mais vous devez utiliser un profil de filtrage des URL pour activer cette fonction.*

| Attribut | Description |
|---|---|
| User-Agent (Utilisateur-Agent) | Le navigateur Web utilisé par l'utilisateur pour accéder à l'URL, Internet Explorer par exemple. Ces informations sont incluses dans la demande HTTP envoyée au serveur. |
| Referer (Référant) | L'URL de la page Web associée qui relie l'utilisateur à une autre page Web ; il s'agit de la source qui a redirigé (référé) l'utilisateur vers (à) la page Web demandée. |
| X-Forwarded-For (XFF) | L'option du champ d'en-tête de requête HTTP qui conserve l'adresse IP de l'utilisateur qui a demandé la page Web. Si votre réseau comporte un serveur proxy, XFF vous permet d'identifier l'adresse IP de l'utilisateur qui a demandé le contenu au lieu d'enregistrer uniquement l'adresse IP du serveur proxy en tant qu'adresse IP de l'utilisateur qui a demandé la page Web. |
| Insertion d'en-têtes | Le type d'en-tête et le texte de l'en-tête que le pare-feu insère. |

# Demande de changement de la catégorie d'une URL

Si vous croyez qu'une URL n'est pas bien catégorisée, vous pouvez nous demander de la catégoriser différemment. Soumettez une demande de changement directement dans le pare-feu ou utilisez le site d'essai A. Une demande de changement entraîne une analyse immédiate de l'URL faisant l'objet d'une demande de catégorie par PAN-DB, le cloud de filtrage des URL. Si PAN-DB valide que la proposition est justifiée, la demande de changement est alors approuvée. Si PAN-DB ne trouve pas la suggestion de la nouvelle catégorie pertinente, la requête de changement est ensuite examinée par des membres de l'équipe de recherche et de l'équipe de science de données de Palo Alto Networks.

Après avoir soumis une requête de changement, vous recevrez un email de notre part vous confirmant que nous avons bien reçu votre requête. Après avoir complété notre investigation, vous recevrez un second email vous confirmant les résultats

Vous ne pouvez pas demander de changer la catégorie de risque qu'une URL reçoit (**high risk (risque élevé)**, **medium risk (risque moyen)**, ou **low risk (faible risque)**), ou vers les URLs catégorisées dans **insufficient content (contenu insuffisant)** ou **newly-registered domains (domaines nouvellement enregistrés)**.

- Faire une demande de changement en ligne
- Faire une demande de changement en masse
- Faire une demande de changement depuis le pare-feu

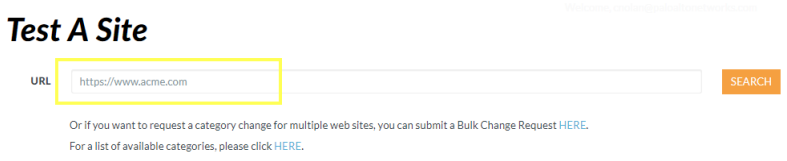
## Faire une demande de changement en ligne

Visitez le Test A Site filtrage des URL Palo Alto Networks pour faire une demande de changement en ligne

**STEP 1 |** Allez à Test A Site.

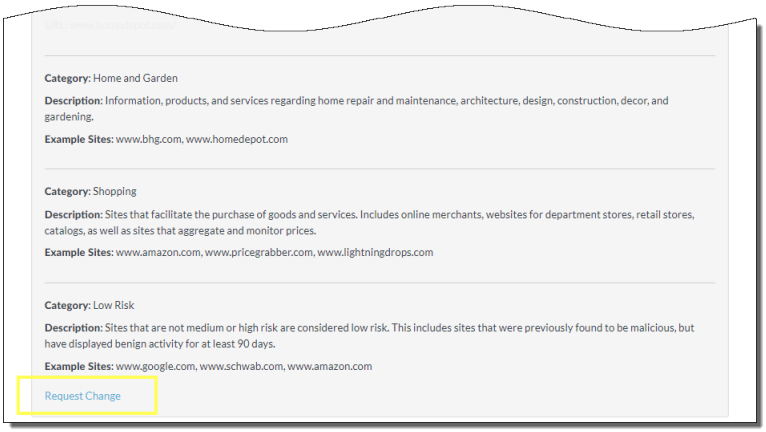
Vous n'avez pas besoin de vous authentifier pour soumettre une requête de changement, bien que vous deviez fournir votre email dans le formulaire de demande de changement. Si vous décidez de ne pas vous authentifier, vous aurez besoin de passer un test CAPTCHA pour confirmer que vous n'êtes pas un robot (authentifiez vous pour éviter le test CAPTCHA)

**STEP 2 |** Entrez une URL pour vérifier ses catégories :



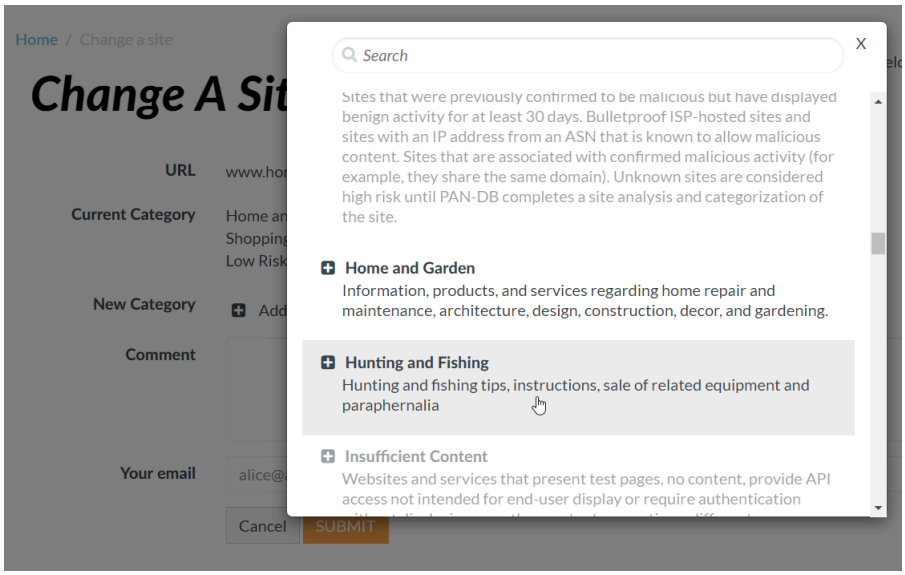

 

**STEP 3 |** Examinez les catégories URLs, et si vous pensez qu'elles ne sont pas pertinentes, sélectionnez **Demande de changement**.




**STEP 4 |** Continuez à remplir le formulaire et soumettez la demande de changement

Incluez au moins une (et jusqu'à deux) nouvelles suggestions de catégories, et laissez un commentaire (optionnel) pour nous en dire davantage sur votre suggestion.




## Faire une demande de changement en masse

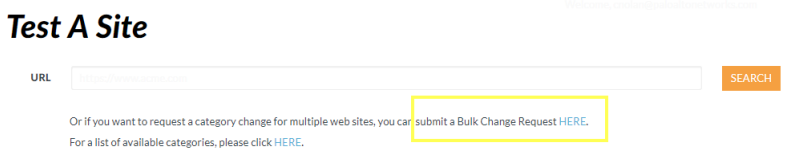
Vous pouvez aussi utiliser Test A Site pour faire une demande de changement en masse, où vous pourrez soumettre des demandes de changement pour de multiples URLs en une seule fois.

**STEP 1 |** Allez à Test A Site.

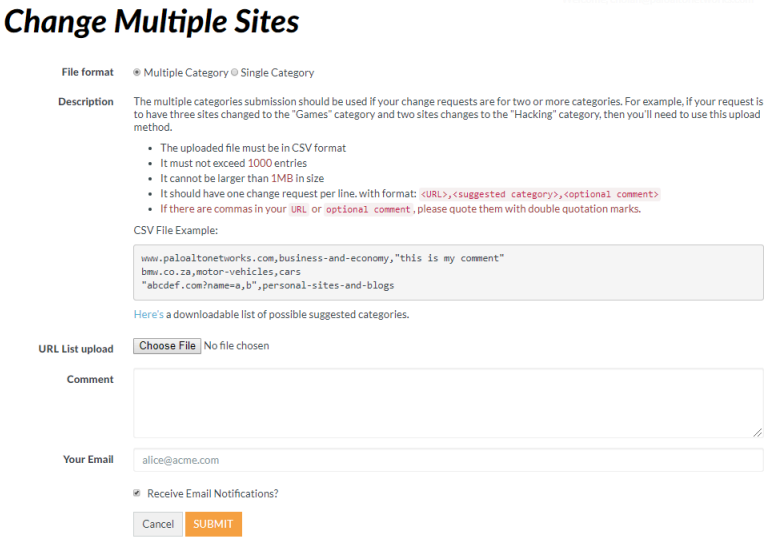
Vous n'avez pas besoin de vous authentifier pour soumettre une requête de changement, bien que vous deviez fournir votre email dans le formulaire de demande de changement. Si vous décidez de ne pas vous authentifier, vous aurez besoin de passer un test CAPTCHA pour confirmer que vous n'êtes pas un robot (authentifiez vous pour éviter le test CAPTCHA)

**STEP 2 |** Choisissez une option pour soumettre une demande de changement en masse :

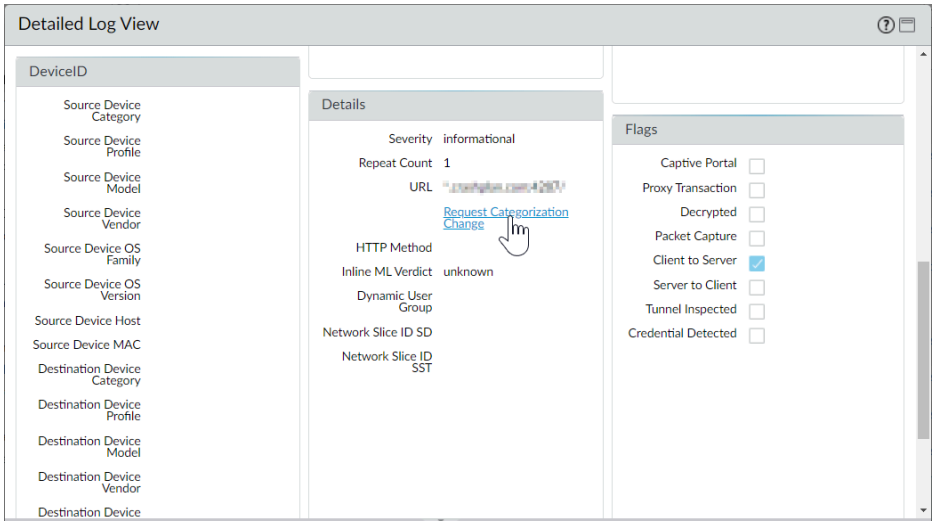



**STEP 3 |** Compléter et soumettez le formulaire de demande de changement en masse.



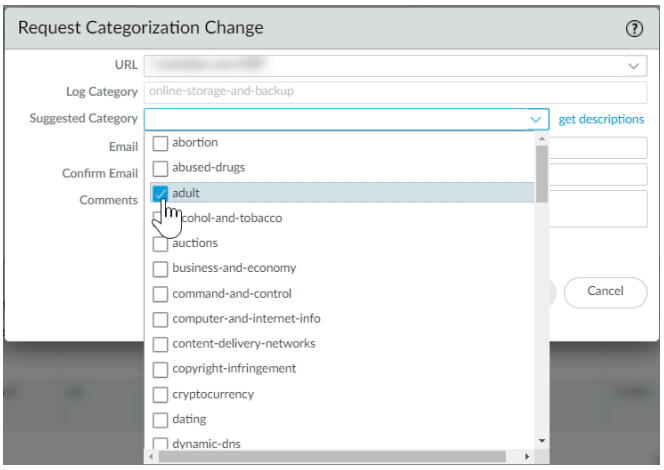

# Faire une demande de changement depuis le pare-feu

Vous pouvez aussi soumettre une demande de changement de catégorie d'URL directement depuis le pare-feu. Dans les journaux de Filtrage des URL, les détails de chaque entrée du journal incluent une option pour **Request Categorization Change (Demander une modification de catégorisation)**(**Monitor (Surveiller)** > **Logs (journaux)** > **URL Filtering (Filtrage d'URL)**).




De là, vous pouvez compléter le formulaire de demande, et le soumettre.



# Dépannage du filtrage des URL

Les rubriques suivantes fournissent des instructions de dépannage pour diagnostiquer et résoudre les problèmes couramment liés au filtrage des URL.

- Problèmes d'activation de PAN-DB
- Problèmes de connectivité au cloud PAN-DB
- URL classées comme étant non résolues
- Catégorisation incorrecte

## Problèmes d'activation de PAN-DB

Utilisez le flux de travail suivant pour résoudre les problèmes d'activation de PAN-DB.

**STEP 1 |** Accès à la CLI PAN-OS.

**STEP 2 |** Vérifiez si PAN-DB a été activé en exécutant la commande suivante :

```
show system setting url-database
```

Si la réponse est **paloaltonetworks**, alors PAN-DB est le fournisseur actif.

**STEP 3 |** Vérifiez que le pare-feu dispose d'une licence PAN-DB valide en exécutant la commande suivante :

```
request license info
```

L'entrée de licence **Feature: Filtrage des données PAN-DB**. Si la licence n'est pas installée, vous devrez vous procurer et installer une licence. Consultez Configuration du filtrage des URL.

**STEP 4 |** Vérifiez l'état de la connexion au cloud PAN-DB.

## Problèmes de connectivité au cloud PAN-DB

Pour vérifier la connectivité entre le pare-feu et le cloud PAN-DB :

```
show url-cloud status
```

Si le Cloud est accessible, la réponse attendue doit être semblable à la suivante :

```
show url-cloud status
PAN-DB URL Filtering
License :                          valid
Current cloud server :
 serverlist.urlcloud.paloaltonetworks.com
Cloud connection :                 connected
Cloud mode :                       public
URL database version - device :    20200624.20296
URL database version - cloud :     20200624.20296  ( last update time
 2020/06/24 12:39:19 )
```

```
URL database status :                good
URL protocol version - device :      pan/2.0.0
URL protocol version - cloud :       pan/2.0.0
Protocol compatibility status :      compatible
```

Si le cloud est inaccessible, la réponse attendue doit être semblable à la suivante :

```
show url-cloud status
PAN-DB URL Filtering
License :                            valid
Cloud connection :                   not connected
URL database version - device :      0000.00.00.000
URL protocol version - device :      pan/0.0.2
```

Utilisez la liste de vérification suivante pour identifier et résoudre les problèmes de connectivité :

- Le champ de la licence de filtrage des données PAN-DB affiche-t-il invalid (non valide) ? Obtenez et installez une licence PAN-DB valide.
- La version du protocole d'URL affiche-t-elle not compatible (non compatible) ? Passez à la dernière version de PAN-OS.
- Pouvez-vous envoyer une requête ping au serveur cloud PAN-DB à partir du pare-feu ? Exécutez la commande suivante pour vérifier :

  ```
  ping source <ip-address> host
   serverlist.urlcloud.paloaltonetworks.com <
  ```

  Par exemple, si l'adresse IP de votre interface de gestion est 10.1.1.5, exécutez la commande suivante :

  ```
  ping source 10.1.1.5 host serverlist.urlcloud.paloaltonetworks.com
  ```

- Le pare-feu est-il dans une configuration HA ? Vérifiez que l'état HA des pare-feu est à l'état actif, actif-principal ou actif-secondaire. L'accès au cloud PAN-DB sera bloqué si l'état du pare-feu est autre. Exécutez la commande suivante sur chaque pare-feu de la paire pour voir l'état :

  ```
  show high-availability state
  ```

Si vous avez toujours des problèmes de connectivité entre le pare-feu et le cloud PAN-DB, contactez le support Palo Alto Networks.

## URL classées comme étant non résolues

Les URL sont classées comme non résolues lorsque votre connexion au service cloud de filtrage d'URL PAN-DB est interrompue, ce qui entraîne l'échec des recherches d'URL. L'état de la connexion au cloud et la classification des URL ne s'appliquent pas aux licences d'abonnement expirées ou aux utilisateurs sans licence.

Utilisez le flux de travail suivant lorsque certaines ou toutes les URL identifiées par PAN-DB sont classées comme étant Not-resolved (non résolues) :

**STEP 1 |** Vérifiez la connexion au Cloud PAN-DB en exécutant la commande suivante :

```
show url-cloud status
```

Le champ Cloud connection: doit indiquer `connected`. Si une valeur autre que `connected` s'affiche, toutes les URL qui ne figurent pas dans le cache du plan de gestion seront classées comme étant `non résolues`. Pour résoudre ce problème, consultez Problèmes de connectivité Cloud PAN-DB.

**STEP 2 |** Si le statut de connexion au cloud indique `connected`, vérifiez l'utilisation actuelle du pare-feu. Si l'utilisation du pare-feu monte en flèche, les requêtes d'URL peuvent être abandonnées (et éventuellement ne pas atteindre le plan de gestion) et seront classées comme étant `not-resolved`.

Pour afficher les ressources système, exécutez la commande suivante et consultez les colonnes `%CPU` et `%MEM` :

```
show system resources
```

Vous pouvez également visualiser les ressources du système sur le widget System Resources (Ressources système) dans le **Dashboard (Tableau de bord)** de l'interface Web.

**STEP 3 |** Si le problème persiste, contactez le support de Palo Alto Networks.

## Catégorisation incorrecte

Il se peut parfois que vous tombiez sur une URL qui, selon vous, est mal catégorisée. Servez-vous du flux de travail suivant pour déterminer la catégorisation de l'URL d'un site et pour demander que la catégorie soit modifiée, si nécessaire.

**STEP 1 |** Vérifiez la catégorie dans le plan de données en exécutant la commande suivante :

```
show running url <URL>
```

Par exemple, pour afficher la catégorie du site Web de Palo Alto Networks, exécutez la commande suivante :

```
show running url paloaltonetworks.com
```

Si l'URL stockée dans le cache du plan de données affiche la catégorie correcte (computer-and-internet-info dans cet exemple), alors la catégorisation est correcte et aucune autre action n'est requise. Si la catégorie est incorrecte, passez à l'étape suivante.

**STEP 2 |** Vérifiez si la catégorie figure dans le plan de gestion en exécutant la commande suivante :

```
test url-info-host <URL>
```

Par exemple :

```
test url-info-host paloaltonetworks.com
```

Si l'URL stockée dans le cache du plan de gestion affiche la catégorie correcte, supprimez l'URL du cache du plan de gestion en exécutant la commande suivante :

```
clear url-cache url <URL>
```

La prochaine fois que le pare-feu demandera la catégorie de cette URL, la requête sera transférée au plan de gestion. Ceci va résoudre le problème et aucune autre action ne sera requise. Si le problème n'est toujours pas résolu, passez à l'étape suivante pour vérifier la catégorie d'URL sur les systèmes Cloud.

**STEP 3 |** Vérifiez la catégorie dans le Cloud en exécutant la commande suivante :

```
test url-info-cloud <URL>
```

**STEP 4 |** Si l'URL stockée dans le cloud affiche la catégorie correcte, supprimez l'URL des caches des plans de données et de gestion.

Exécutez la commande suivante pour supprimer une URL du cache du plan de données :

```
clear url-cache url <URL>
```

Exécutez la commande suivante pour supprimer une URL du cache du plan de gestion :

```
delete url-database url <URL>
```

La prochaine fois que le pare-feu demandera la catégorie de l'URL donné, la requête sera transférée au plan de gestion, puis au cloud. Ceci devrait résoudre le problème de recherche de catégorie. Si le problème persiste, passez à l'étape suivante pour soumettre une requête de modification de catégorisation.

**STEP 5 |** Pour soumettre une requête de modification depuis l'interface Web, accédez au journal des URL et sélectionnez l'entrée de journal de l'URL que vous souhaitez modifier.

**STEP 6 |** Cliquez sur lien **Request Categorization (Demander un changement de catégorisation)** et suivez les instructions. Vous pouvez également demander un changement de catégorie sur le site Web Test A Site de Palo Alto Networks en recherchant l'URL et en cliquant sur l'icône **Request Change (Demander un changement)**. Pour voir une liste de toutes les catégories

disponibles avec une description de chaque catégorie, reportez-vous à l'adresse https://urlfiltering.paloaltonetworks.com/CategoryList.aspx.

Vous recevez une notification par courrier électronique si votre requête de modification est approuvée. Deux options pour vérifier que la catégorie d'URL est mise à jour sur le pare-feu sont possibles :

- Patientez jusqu'à ce que l'URL dans le cache arrive à expiration et la prochaine fois qu'un utilisateur accède à l'URL, la nouvelle mise à jour de catégorisation sera mise dans le cache.
- Exécutez la commande suivante pour forcer une mise à jour dans le cache :

```
request url-filtering update url <URL>
```

# Cloud privé PAN-DB

Le cloud privé PAN-DB est une solution sur site adaptée aux organisations limitant l'utilisation des services de cloud. Grâce à cette solution sur site, vous pouvez déployer un ou plusieurs périphériques M-600 en tant que serveurs PAN-DB dans votre réseau ou centre de données. Les pare-feu interrogent le cloud privé PAN-DB pour rechercher des URL plutôt que d'accéder au cloud public PAN-DB.

Le processus de recherche d'URL, que ce soit dans le cloud privé ou public, est identique pour les pare-feu du réseau. Par défaut, le pare-feu est configuré pour accéder au cloud PAN-DB public. Si vous déployez un cloud privé PAN-DB, vous devez configurer les pare-feu avec une liste d'adresses IP ou de FQDN pour accéder au ou aux serveurs du cloud privé.

***Les pare-feu exécutant PAN-OS 5.0 ou une version ultérieure peuvent communiquer avec le cloud privé PAN-DB.***

Lorsque vous set up the PAN-DB private cloud (configurez le cloud privé PAN-DB), vous pouvez soit configurer les périphériques M-600 pour qu'ils disposent d'un accès direct à Internet ou les maintenir hors ligne. L'appareil M-600 nécessitant des mises à jour de la base de données et du contenu pour rechercher des URL, si le périphérique ne dispose pas d'une connexion à Internet, vous devez télécharger manuellement les mises à jour sur un serveur de votre réseau, puis importer les mises à jour à l'aide de SCP dans chaque appareil M-600 du cloud privé PAN-DB. De plus, les périphériques doivent être en mesure d'accéder à la base de données initiale et à toute autre mise à jour du contenu périodique ou critique pour les pare-feu qu'ils desservent.

Pour authentifier les pare-feu qui se connectent au cloud privé PAN-DB, un jeu de certificats du serveur par défaut est fourni avec le périphérique ; vous ne pouvez pas importer ou utiliser un autre certificat du serveur pour authentifier les pare-feu. Si vous modifiez le nom d'hôte sur le périphérique M-600, ce dernier génère automatique un nouveau jeu de certificats pour authentifier les pare-feux.

- Équipement M-600 pour le cloud privé PAN-DB
- Paramétrage du cloud privé PAN-DB

## Équipement M-600 pour le cloud privé PAN-DB

Pour déployer un cloud privé PAN-DB, vous avez besoin d'un ou plusieurs appareils M-600. L'appareil M-600 est fourni en mode Panorama, et pour pouvoir le déployer en tant que cloud privé PAN-DB, vous devez le paramétrer pour fonctionner en mode PAN-URL-DB. En mode PAN-URL-DB, le périphérique propose des services de catégorisation d'URL pour les entreprises ne souhaitant pas utiliser le cloud public PAN-DB.

L'appareil M-600, lorsqu'il est déployé en tant que cloud privé PAN-DB, utilise deux ports : MGT (Eth0) et Eth1. Le port Eth2 ne peut pas être utilisé. Le port de gestion est utilisé pour l'accès administrateur au périphérique et pour obtenir les dernières mises à jour du contenu du cloud public PAN-DB ou d'un serveur sur votre réseau. Pour établir une communication entre le cloud privé PAN-DB et les pare-feu de votre réseau, vous pouvez utiliser le port MGT ou Eth1.

***L'appareil M-200 ne peut pas être déployé en tant que cloud privé PAN-DB.***

L'appareil M-600 en mode PAN-URL-DB :

- N'est pas équipé d'une interface Web et prend donc seulement en charge une interface de ligne de commande (CLI).
- Ne peut pas être géré par Panorama.
- Ne peut pas être déployé dans une paire haute disponibilité.
- Ne nécessite pas une licence Filtrage des URL. Les pare-feu doivent disposer d'une licence Filtrage des URL PAN-DB valide pour pouvoir se connecter au cloud privé PAN-DB.
- Est fourni avec un jeu de certificats du serveur par défaut utilisés pour authentifier les pare-feu qui se connectent au cloud privé PAN-DB. Vous ne pouvez pas importer ou utiliser un autre certificat du serveur pour authentifier les pare-feu. Si vous modifiez le nom d'hôte sur l'appareil M-600, ce dernier génère automatique un nouveau jeu de certificats pour authentifier les pare-feu qu'il dessert.
- Peut être réinitialisé en mode Panorama uniquement. Si vous souhaitez déployer le périphérique en tant que collecteur de journaux dédié, passez en mode Panorama et définissez-le en mode Collecteur de journaux.

**Table 4: Différences entre le cloud public PAN-DB et le cloud privé PAN-DB**

| Différences | Cloud public PAN-DB | Cloud privé PAN-DB |
|---|---|---|
| **Mises à jour du contenu et de la base de données** | Des mises à jour du contenu (périodiques et critiques) et de la base de données complète sont publiées plusieurs fois par jour. Le cloud public PAN-DB met à jour les catégories d'URL malware et phishing toutes les cinq minutes. Le pare-feu recherche des mises à jour critiques lorsqu'il recherche des URL sur les serveurs de cloud. | Des mises à jour du contenu et de la base de données d'URL complète sont disponibles une fois par jour pendant la semaine de travail. |
| **Requêtes de catégorisation des URL** | Envoyez des requêtes de modification de catégorisation des URL à l'aide des options suivantes :<br>• Site Web Test A Site de Palo Alto Networks.<br>• Page de configuration du profil de Filtrage des URL sur le pare-feu.<br>• Journal de Filtrage des URL sur le pare-feu. | Envoyez uniquement des requêtes de modification de catégorisation des URL à l'aide du site Web Test A Site de Palo Alto Networks. |
| **Requêtes d'URL non résolues** | Si le pare-feu ne parvient pas à résoudre une requête d'URL, celle-ci est envoyée aux serveurs du cloud public. | Si le pare-feu ne parvient pas à résoudre une requête, celle-ci est envoyée aux appareils M-600 du cloud public. S'il n'existe aucune correspondance pour l'URL, le cloud |

| Différences | Cloud public PAN-DB | Cloud privé PAN-DB |
|---|---|---|
| | | privé PAN-DB envoie une réponse de catégorie ***inconnu*** au parte-feu. La requête n'est pas envoyée au cloud public, sauf si vous avez configuré l'appareil M-600 pour accéder au cloud public PAN-DB.<br><br>Si les appareils M-600 qui constituent votre cloud privé PAN-DB sont configurés pour être hors ligne, ils n'envoient aucune donnée ou analyse au cloud public. |

# Paramétrage du cloud privé PAN-DB

Pour déployer un ou plusieurs périphériques M-600 en tant que cloud privé PAN-DB dans votre réseau ou centre de données, utilisez les tâches suivante :

- Configuration du cloud privé PAN-DB
- Configurez les pare-feu pour accéder au cloud privé PAN-DB
- Configuration de l'authentification au moyen de certificats personnalisés sur le cloud privé PAN-DB

## Configuration du cloud privé PAN-DB

**STEP 1 |** Montez le périphérique M-600 dans une baie.

Pour obtenir des instructions, reportez-vous au Guide de référence du matériel M-600.

**STEP 2 |** Enregistrez le périphérique M-600.

Pour obtenir des instructions sur l'enregistrement du périphérique M-600, reportez-vous à la section Enregistrement du pare-feu.

**STEP 3 |** Effectuez la configuration initiale du périphérique M-600.

***Le périphérique M-600 en mode PAN-DB utilise deux ports : MGT (Eth0) et Eth1. Le port Eth2 n'est pas utilisé en mode PAN-DB. Le port de gestion est utilisé pour l'accès administrateur au périphérique et pour obtenir les dernières mises à jour du contenu du cloud public PAN-DB. Pour établir une communication le périphérique (serveur PAN-DB) et les pare-feu de votre réseau, vous pouvez utiliser le port MGT ou Eth1.***

1. Connectez-vous au périphérique M-600 d'une des façons suivantes :
   - Connectez un câble série à l'ordinateur et au port de console du périphérique M-600, puis connectez-vous en utilisant un logiciel d'émulation (9600-8-N-1).
   - Connectez un câble RJ-45 d'un ordinateur au port MGT du périphérique M-600. Depuis un navigateur, accédez à https://192.168.1.1. Permettre l'accès à cette URL

pourrait nécessiter de modifier l'adresse IP de l'ordinateur à une adresse dans le réseau 192.168.1.0 (par exemple, 192.168.1.2).

2. Lorsque vous y êtes invité, connectez-vous au périphérique. Connectez-vous en utilisant le nom d'utilisateur et le mot de passe par défaut (admin/admin). Le périphérique commence son initialisation.
3. Configurez des paramètres d'accès réseau, notamment l'adresse IP de l'interface MGT :

```
set deviceconfig system ip-address  <server-IP>
 netmask <netmask> default-gateway <gateway-IP> dns-setting
 servers primary <DNS-IP>
```

où ***<adresse IP du serveur>*** est l'adresse IP que vous voulez affecter à l'interface de gestion du serveur, ***<masque réseau>*** est le masque de sous-réseau, ***<adresse IP de la passerelle>*** est l'adresse IP de la passerelle réseau et ***<adresse IP du serveur DNS>*** est l'adresse IP du serveur DNS principal.

4. Configurez des paramètres d'accès réseau, notamment l'adresse IP de l'interface Eth1 :

```
set deviceconfig system eth1 ip-address  <server-IP>
 netmask <netmask> default-gateway <gateway-IP> dns-setting
 servers primary <DNS-IP>
```

où <***adresse IP du serveur***> est l'adresse IP que vous voulez affecter à l'interface de données du serveur, <***masque réseau***> est le masque de sous-réseau, <***adresse IP de la passerelle***> est l'adresse IP de la passerelle réseau et <***adresse IP du serveur DNS***> est l'adresse IP du serveur DNS.

5. Enregistrez vos modifications sur le serveur PAN-DB.

   **commit**

**STEP 4 |** Passez en mode cloud privé PAN-DB.

1. Pour passer en mode PAN-DB, utilisez la commande CLI suivante :

```
request system system-mode pan-url-db
```

> *Vous pouvez basculer du mode Panorama au mode PAN-DB et vice-versa, et du* Mode Panorama au mode Collecteur de journaux *et vice-versa. Le passage direct du mode PAN-DB au mode Collecteur de journaux, ou vice versa, n'est pas possible. Une réinitialisation des données est effectuée lorsque vous changez de mode opérationnel. À l'exception des paramètres d'accès de gestion, l'ensemble de la configuration et des journaux existants est supprimé au redémarrage.*

2. Les commandes suivantes vous permettent de vérifier que le mode a changé :

```
show pan-url-cloud-status
hostname: M-600
ip-address: 1.2.3.4
netmask: 255.255.255.0
default-gateway: 1.2.3.1
ipv6-address: unknown
```

```
ipv6-link-local-address: fe80:00/64
ipv6-default-gateway:
mac-address: 00:56:90:e7:f6:8e
time: Mon Apr 27 13:43:59 2015
uptime: 10 days, 1:51:28
family: m
model: M-600
serial: 0073010000xxx
sw-version: 7.0.0
app-version: 492-2638
app-release-date: 2015/03/19  20:05:33
av-version: 0
av-release-date: unknown
wf-private-version: 0
wf-private-release-date: unknown
logdb-version: 7.0.9
platform-family: m
pan-url-db: 20150417-220
system-mode: Pan-URL-DB
operational-mode: normal
```

3. Utilisez la commande suivante pour vérifier la version de la base de données du cloud sur le périphérique :

```
show pan-url-cloud-status
Cloud status:            Up
URL database version:    20150417-220
```

**STEP 5 |** Installez les mises à jour du contenu et de la base de données.

*Le périphérique stocke uniquement la version en cours d'exécution du contenu et une version antérieure.*

Sélectionnez l'une des méthodes suivantes d'installation des mises à jour du contenu et de la base de données :

- Si le serveur PAN-DB dispose d'un accès direct à Internet, utilisez les commandes suivantes :
  1. Pour vérifier si une nouvelle version est publiée, utilisez :

     **request pan-url-db upgrade check**
  2. Pour connaître la version actuellement installée sur votre serveur, utilisez :

     **request pan-url-db upgrade info**
  3. Pour télécharger et installer la dernière version :
     - **request pan-url-db upgrade download latest**
     - **request pan-url-db upgrade install** *<version latest | file>*
  4. Pour planifier le périphérique M-600 pour rechercher automatiquement des mises à jour :

     ```
     set deviceconfig system update-schedule pan-url-db recurring
      weekly action download-and-install day-of-week  <day of week>
      at <hr:min>
     ```
- Si le serveur PAN-DB est hors ligne, accédez au site Web de support aux clients de Palo Alto Networks pour télécharger et enregistrer les mises à jour du contenu sur un serveur SCP sur votre réseau. Vous pouvez ensuite importer et installer les mises à jour à l'aide des commandes suivantes :
  - **scp import pan-url-db remote-port** *<port-number>* from username@host:path
  - **request pan-url-db upgrade install file** *<filename>*

**STEP 6 |** Paramétrez l'accès administrateur au cloud privé PAN-DB.

*Le périphérique dispose d'un compte `admin` par défaut. Tous les utilisateurs administrateurs supplémentaires que vous créez peuvent être des super utilisateurs (accès intégral) ou des super utilisateurs avec un accès en lecture seule.*

Le cloud privé PAN-DB ne prend pas en charge l'utilisation de VSA RADIUS. Un échec d'authentification se produit si les VSA utilisés sur le pare-feu ou Panorama sont utilisés pour accéder au cloud privé PAN-DB.

- Pour paramétrer un utilisateur administrateur local sur le serveur PAN-DB :
  1. **configure**
  2. **set mgt-config users** *<username>* permissions role-based <superreader | superuser> yes
  3. **set mgt-config users** *<username>* password
  4. **Enter password:xxxxx**
  5. **Confirm password:xxxxx**
  6. **commit**
- Pour paramétrer un utilisateur administrateur avec l'authentification RADIUS :
  1. Créez un profil de serveur RADIUS.

     **set shared server-profile radius** *<server_profile_name>* server *<server_name>* ip-address *<ip_address>* port *<port_no>* secret *<shared_password>*
  2. Créez un profil d'authentification.

     **set shared authentication-profile** *<auth_profile_name>* user-domain *<domain_name_for_authentication>* allow-list <all> method radius server-profile *<server_profile_name>*
  3. Associez le profil d'authentification à l'utilisateur.

     **set mgt-config users** *<username>* authentication-profile *<auth_profile_name>*
  4. Commit (Validez) les modifications.

     **commit**
- Pour afficher la liste des utilisateurs :

```
show mgt-config users
users {
admin {
phash fnRL/G5lXVMug;
permissions {
```

```
role-based {
superuser yes;
}
}
}
admin_user_2 {
permissions {
role-based {
superreader yes;
}
}
authentication-profile RADIUS;
}
}
```

**STEP 7 |** Configure the firewalls to access the PAN-DB private cloud (Configurez les pare-feu pour accéder au cloud privé PAN-DB)

## Configurez les pare-feu pour accéder au cloud privé PAN-DB

Lors de l'utilisation du cloud public PAN-DB, chaque pare-feu accède aux serveurs PAN-DB du cloud AWS pour télécharger la liste des serveurs éligibles auxquels il peut se connecter pour rechercher des URL. Avec le cloud privé PAN-DB, vous devez configurer les pare-feu avec une liste (statique) de vos serveurs de cloud privé PAN-DB qui seront utilisés pour la recherche d'URL. La liste importée peut contenir jusqu'à 20 entrées ; les adresses IPv4, les adresses IPv6 et les FQDN sont pris en charge. Chaque entrée de la liste (adresse IP ou FQDN) doit être affectée au port de gestion et/ou eth1 du serveur PAN-DB.

**STEP 1 |** From the PAN-OS CLI (À partir de la CLI PAN-OS), ajoutez une liste de serveurs cloud privés PAN-DB statiques utilisés pour les recherches d'URL.

- Utilisez la commande CLI suivante pour ajouter des adresses IP de serveur PAN-DB privées :

```
> configure
```

```
# set deviceconfig setting pan-url-db cloud-static-list <IP
 addresses>
```

Ou, dans l'interface Web de chaque pare-feu, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Content-ID (Content-ID)**, modifiez la section URL Filtering (Filtrage des URL) et saisissez la ou les adresses IP ou les FQDN du **PAN-DB Server (Serveur PAN-DB)**. La liste doit être séparée par des virgules.

- Pour supprimer les entrées des serveurs PAN-DB privés, utilisez la commande suivante :

```
# delete deviceconfig setting pan-url-db cloud-static-list <IP
 addresses>
```

Lorsque vous supprimez la liste de serveurs PAN-DB privés, un processus de resélection est démarré sur le pare-feu. Le pare-feu recherche d'abord dans la liste de serveurs de cloud privé PAN-DB et, s'il n'en trouve aucun, il accède aux serveurs PAN-DB du cloud AWS pour télécharger la liste des serveurs éligibles auxquels il peut se connecter.

**STEP 2 |** Entrez**# commit (valider)** pour enregistrer vos modifications.

**STEP 3 |** Pour vérifier que la modification est appliquée, utilisez la commande CLI suivante sur le pare-feu :

```
> show url-cloud status
Cloud status:            Up
URL database version:    20150417-220
```

## Configuration de l'authentification au moyen de certificats personnalisés sur le cloud privé PAN-DB

Par défaut, un serveur PAN-DB utilise des certificats prédéfinis pour l'authentification mutuelle afin d'établir les connexions SSL utilisées pour l'accès de gestion et la communication entre appareils. Cependant, vous pouvez configurer l'authentification à l'aide de certificats personnalisés. Les certificats personnalisés vous permettent d'établir une chaîne de confiance unique pour assurer une authentification mutuelle entre votre serveur PAN-DB et vos pare-feu. Dans le cas d'un cloud privé PAN-DB, le pare-feu fait office de client et le serveur PAN-DB, de serveur.

**STEP 1 |** Obtenez des paires de clés et des certificats d'autorité de certification (CA) pour le serveur PAN-DB et le pare-feu.

**STEP 2 |** Importez le certificat d'autorité de certification pour valider le certificat sur le pare-feu.

1. Connectez-vous à la CLI du serveur PAN-DB, puis saisissez le mode de configuration.

   ```
   admin@M-600> configure
   ```

2. Utilisez TFTP ou SCP pour importer le certificat de l'autorité de certification.

   ```
   admin@M-600# {tftp | scp} import certificate from <value> file
    <valeur> remote-port <1-65535> source-ip <adresse-ip/masque-
   réseau> certificate-name <valeur> passphrase <valeur> format
    {pkcs12 | pem}
   ```

**STEP 3 |** Utilisez TFTP ou SCP pour importer la paire de clés qui contient le certificat du serveur et la clé privée de l'appareil M-600 PAN-DB.

```
admin@M-600# {tftp | scp} import keypair from <value> file <valeur>
 remote-port <1-65535> source-ip <adresse-ip/masque-réseau>
 certificate-name <valeur> passphrase <valeur> format {pkcs12 |
 pem}
```

**STEP 4 |** Configurez un profil de certificat incluant l'autorité de certification racine et l'autorité de certification intermédiaire. Ce profil de certificat définit l'authentification des périphériques entre le serveur PAN-DB et le pare-feu.

1. Dans la CLI du serveur PAN-DB, saisissez le mode de configuration.

```
admin@M-600> configure
```

2. Nommez le profil de certificat.

```
admin@M-600# set shared certificate-profile <name>
```

3. (Facultatif) Définissez le domaine d'utilisateur.

```
admin@M-600# set shared certificate-profile <name> domain
 <valeur>
```

4. Configurez le CA.

   *Les paramètres **Default-ocsp-url** et **ocsp-verify-cert** sont facultatifs.*

admin@M-600# **set shared certificate-profile <*nom*> CA <*nom*>**

```
admin@M-600# set shared certificate-profile <name> CA <nom>
 [default-ocsp-url <valeur>]
```

```
admin@M-600# set shared certificate-profile <name> CA <nom>
 [ocsp-verify-cert <valeur>]
```

**STEP 5 |** Configurez un profil SSL / TLS pour l'appareil M-600 PAN-DB. Ce profil définit le certificat et la plage de protocoles utilisés par PAN-DB et les périphériques client pour les services SSL / TLS.

1. Identifiez le profil SSL/TLS.

```
admin@M-600# set shared ssl-tls-service-profile <name>
```

2. Sélectionnez le certificat.

```
admin@M-600# set shared ssl-tls-service-profile <name>
 certificate <valeur>
```

3. Définissez la plage SSL/TLS.

*Les versions de PAN-OS 8.0 et les versions ultérieures prennent uniquement en charge les versions TLS 1.2 et les versions ultérieures. Vous devez définir la version maximale sur **TLS 1.2** ou sur **max**.*

```
admin@M-600# set shared ssl-tls-service-profile <name>
 protocol-settings min-version {tls1-0 | tls1-1 | tls1-2
```

```
admin@M-600# set shared ssl-tls-service-profile <name>
 protocol-settings max-version {tls1-0 | tls1-1 | tls1-2 | max
```

**STEP 6 |** Configurez la communication sécurisée avec le serveur sur PAN-DB.

1. Définissez le profil de SSL/TLS. Ce profil de service SSL/TLS s'applique à toutes les connexions SSL entre PAN-DB et les pare-feu.

```
admin@M-600# set deviceconfig setting management secure-conn-
server ssl-tls-service-profile <ssltls-profile>
```

2. Définissez le profil de certificat.

```
admin@M-600# set deviceconfig setting management secure-conn-
server certificate-profile <certificate-profile>
```

3. Définissez le délai d'attente de déconnexion en nombre de minutes que PAN-DB doit attendre avant de mettre fin à la connexion et de la rétablir avec son pare-feu (la plage est comprise entre 0 et 44 640).

```
admin@M-600# set deviceconfig setting management secure-conn-
server disconnect-wait-time <0-44640
```

**STEP 7 |** Importez le certificat d'autorité de certification pour valider le certificat de l'appareil M-600 PAN-DB.

1. Connectez-vous à l'interface Web du pare-feu.
2. Importez le certificat de l'autorité de certification.

**STEP 8 |** Configurez un certificat local ou SCEP pour le pare-feu.

1. Si vous un certificat local, importez la paire de clés pour le pare-feu.
2. Si vous un certificat SCEP pour le pare-feu, configurez un profil SCEP.

**STEP 9 |** Configurez le profil de certificat sur le pare-feu. Vous pouvez le configurer sur chaque pare-feu individuellement ou vous pouvez envoyer cette configuration de Panorama aux périphériques dans le cadre d'un modèle.

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil du certificat)** pour les pare-feu ou **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil du certificat)** pour Panorama.
2. Configuration d'un profil de certificat.

**STEP 10 |** Déployez des certificats personnalisés sur chaque pare-feu. Vous pouvez déployer des certificats de manière centralisée à partir de Panorama ou le configurer manuellement sur chaque pare-feu.

1. Connectez-vous à l'interface Web du pare-feu.
2. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** pour les pare-feu ou **Panorama** > **Setup (Configuration)** > **Management (Gestion)** pour Panorama, puis **Edit (Modifiez)** la communication sécurisée.
3. Sélectionnez le **Certificate Type (type de certificat)**, le **Certificate (Certificat)**, et le **Certificate Profile (profil du certificat)** dans leurs menus déroulants respectifs.
4. Sous Customize Communication (Personnaliser la communication), sélectionnez **PAN-DB Communication (Communication PAN-DB)**.
5. Cliquez sur **OK**.
6. **Commit (Validez)** vos modifications.

Une fois vos changements validés, les pare-feu ne mettent pas fin aux sessions actives avec le serveur PAN-DB tant que le **Disconnect Wait Time (Délai d'attente de déconnexion)** n'a pas été atteint. Le délai d'attente de déconnexion commence le compte à rebours après que vous appliquez l'utilisation des certificats personnalisés à l'étape suivante.

**STEP 11 |** Après avoir déployé des certificats personnalisés sur tous les pare-feu, appliquez l'authentification des certificats personnalisés.

1. Connectez-vous à la CLI du serveur PAN-DB, puis saisissez le mode de configuration.

```
admin@M-600> configure
```

2. Appliquez l'utilisation des certificats personnalisés.

```
admin@M-600# set deviceconfig setting management secure-conn-
server disable-pre-defined-cert yes
```

Une fois ce changement validé, le délai d'attente de déconnexion commence son compte à rebours (si vous avez configuré le paramètre sur PAN-DB). Lorsque le délai d'attente de déconnexion prend fin, PAN-DB et son pare-feu se connectent au moyen des certificats configurés uniquement.

**STEP 12 |** Deux choix s'offrent à vous lorsque vient le temps d'ajouter de nouveaux pare-feu ou Panorama à votre déploiement de cloud privé PAN-DB.

- Si vous n'avez pas coché **Custom Certificates Only (Certificats personnalisés uniquement)**, vous pouvez alors ajouter un nouveau pare-feu au cloud privé PAN-DB, puis déployer le certificat personnalisé, comme décrit ci-dessus.
- Si vous avez activé l'option **Custom Certificates Only (Certificats personnalisés uniquement)** sur le cloud privé PAN-DB, vous pouvez alors déployer les certificats personnalisés sur les pare-feu avant de les connecter au cloud privé PAN-DB.

# Activer l'inspection d'établissement de liaison SSL/TLS

L'inspection d'établissement de liaison SSL/TLS comble une lacune dans la détection des menaces pour le trafic Web SSL/TLS marqué pour le déchiffrement. Lorsqu'il est activé, le moteur de détection de contenu et de menaces (CTD) du pare-feu inspecte le trafic HTTPS à la recherche de menaces potentielles pendant la négociation SSL/TLS. Le pare-feu utilise les données de la poignée de main pour identifier le trafic et appliquer les règles de politique de sécurité applicables. L'examen de la poignée de main améliore la sécurité du réseau et optimise notre solution de filtrage d'URL en empêchant les menaces et en appliquant les actions de politique de sécurité sur le trafic Web le plus tôt possible.

Plus précisément, le pare-feu analyse le message Client Hello pour le champ ***Server Name Indication (SNI)***, une extension du protocole SSL/TLS qui contient le nom d'hôte d'un site Web demandé. À partir du nom d'hôte, le pare-feu peut dériver la catégorie d'URL et la destination du serveur du trafic. Ensuite, il évalue la catégorie d'URL par rapport aux profils de filtrage d'URL des règles de stratégie de sécurité correspondantes pour déterminer les actions à appliquer. Si le pare-feu détecte une menace, telle qu'un serveur Web malveillant dans le champ SNI, ou si la politique dicte que le site Web soit bloqué, il mettra fin à la poignée de main et mettra immédiatement fin à la session Web. Si aucune menace n'est détectée et que le trafic est autorisé par stratégie, le client et le serveur peuvent terminer la négociation SSL/TLS et échanger des données d'application via la connexion sécurisée.

*Les pages de réponse du filtrage d'URL ne s'affichent pas pour les sites bloqués par le pare-feu lors des inspections d'établissement de liaison SSL/TLS. Après avoir détecté le trafic des catégories bloquées, le pare-feu réinitialise la connexion HTTPS, mettant fin à la poignée de main et empêchant la notification de l'utilisateur par page de réponse. Au lieu de cela, le navigateur affiche un message d'erreur de connexion standard.*

*Les détails des négociations et des sessions SSL/TLS réussies figureront dans les journaux de trafic et de déchiffrement. Si le pare-feu bloque les sessions Web pendant la négociation SSL/TLS, il ne générera pas de journaux de décryptage. Vous pouvez cependant trouver des détails sur les sessions ayant échoué dans les journaux de Filtrage d'URL.*

La procédure suivante détaille les exigences et les étapes nécessaires pour activer l'inspection d'établissement de liaison SSL/TLS :

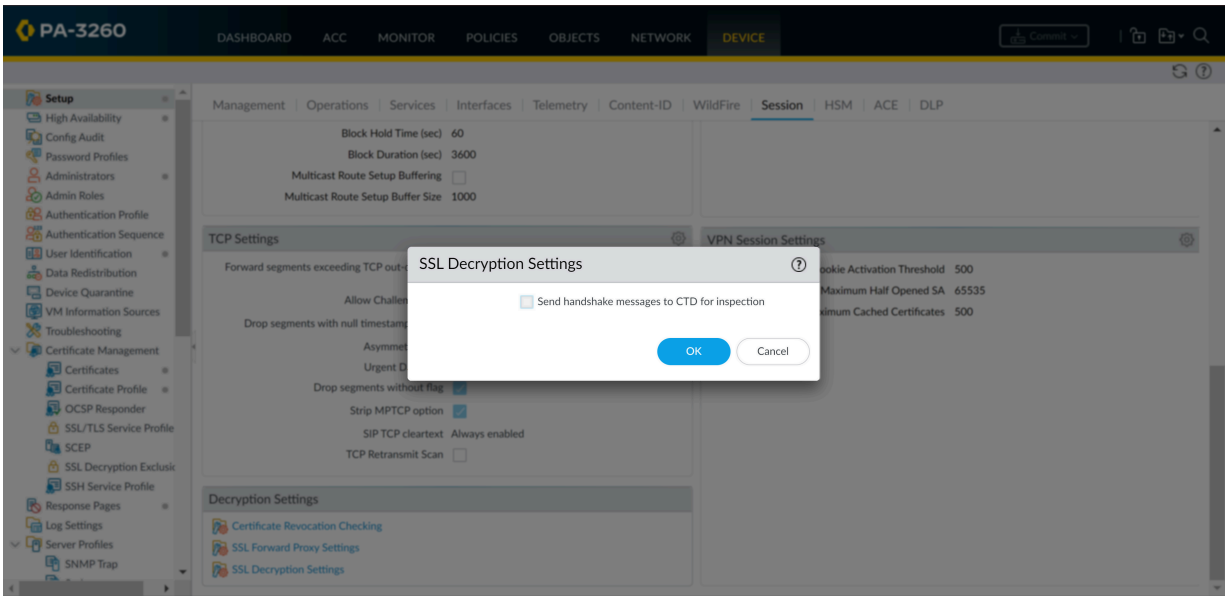
**STEP 1 |** Sélectionnez **Device > Licenses (Appareil > Licences)** pour confirmer que vous disposez d'une active URL Filtering license (licence de filtrage d'URL active).

**STEP 2 |** Vérifiez que vous déchiffrez le trafic SSL/TLS via SSL Forward Proxy (proxy de transfert SSL) ou SSL Inbound Inspection (inspection SSL entrante).

**STEP 3 |** Activez l'inspection des poignées de main SSL/TLS par CTD. Par défaut, l'option est désactivée.



1. Sélectionnez**Device (périphérique)** > **Setup (Configuration)** > **Session** > **Decryption Settings (Paramètres de décryptage)** > **SSL Decryption Settings (paramètres de décryptage SSL)**.
2. Sélectionnez **Send handshake messages to CTD for inspection (Envoyer les messages d'établissement de connexion à CTD pour inspection)**.

   Vous pouvez aussi utiliser la commande CLI **`set deviceconfig setting ssl-decrypt scan-handshake <yes|no> (<yes|no>`**.
3. Cliquez sur **OK**.

**STEP 4 |** **Commit (validez)** vos modifications de configuration.

# Qualité de service (QOS)

La Quality of Service (qualité de service ; QoS) est un ensemble de technologies fonctionnant sur un réseau pour garantir sa capacité à exécuter des applications et du trafic à priorité élevée dans des conditions de capacité réseau limitée. Pour cela, les technologies QoS permettent un traitement et une allocation de capacité distincts de flux spécifiques du trafic réseau. Ceci permet à l'administrateur réseau de déterminer l'ordre dans lequel le trafic est traité, ainsi que la quantité de bande passante mise à disposition du trafic.

La Quality of Service (qualité de service ; QoS) d'application Palo Alto Networks propose une QoS de base appliquée aux réseaux et l'étend pour permettre la QoS des applications et des utilisateurs.

Consultez les rubriques suivantes pour en savoir plus sur la configuration de la QoS basée sur une application Palo Alto Networks :



L'outil de comparaison de produits Palo Alto Networks vous permet d'afficher la fonctionnalité QoS prise en charge par votre modèle de pare-feu. Sélectionnez deux plates-formes de produits ou plus et cliquez sur **Compare Now (Comparez maintenant)** pour afficher la prise en charge de la fonctionnalité QoS par chaque modèle (par exemple, vous pouvez vérifier si votre modèle de pare-feu prend en charge la QoS sur des sous-interfaces et, si oui, le nombre maximum de sous-interfaces sur lesquelles la QoS peut être activée).

La QoS sur les interfaces Aggregate Ethernet (Ethernet agrégées ; AE) est prise en charge sur les pare-feu PA-7000 Series, PA-5200 Series et PA-3200 Series qui utilisent la version 7.0 de PAN-OS ou toute version ultérieure.

# Présentation de la QoS

Utilisez la QoS pour définir la priorité et ajuster les notions de qualité du trafic réseau. Vous pouvez déterminer l'ordre dans lequel les paquets sont traités et affecter de la bande passante, garantissant ainsi qu'un traitement prioritaire et des niveaux de performances optimaux sont appliqués à du trafic, des applications et des utilisateurs sélectionnés.

Les mesures de qualité de service soumises à l'implémentation d'une QoS sont la bande passante (débit de transfert maximum), le débit (débit de transfert réel), la latence (délai) et la gigue (écart de latence). La capacité à partager et à contrôler ces mesures de qualité de service rend la QoS d'autant plus importante dans le cas de la bande passante élevée, du trafic en temps réel comme la Voice Over IP (voix sur IP ; VoIP), de la vidéoconférence et de la vidéo à la demande qui sont extrêmement sensibles à la latence et à la gigue. Utilisez également la QoS pour parvenir à des résultats tels que les suivants :

- Définir la priorité du réseau et du trafic d'application, en garantissant une priorité élevée au trafic important ou en limitant le trafic non essentiel.
- Parvenir à une bande passante uniforme en la partageant entre différents sous-réseaux, classes ou utilisateurs d'un réseau.
- Allouer de la bande passante en externe, en interne ou les deux, en appliquant la QoS au trafic de chargement et de téléchargement ou à l'un des deux uniquement.
- Garantir une faible latence pour le client et le trafic source de revenus dans un environnement d'entreprise.
- Déterminer le profil du trafic des applications afin de vérifier l'utilisation de la bande passante.

L'implémentation de la QoS sur un pare-feu Palo Alto Networks commence par trois composants de configuration principaux qui prennent en charge une solution QoS complète : un Profil Qos, une Politique QoS et le paramétrage de l'Interface de sortie QoS. Chacune de ces options de la tâche de configuration de la QoS simplifie un processus plus large qui permet d'optimiser et de déterminer la priorité du flux de trafic et d'allouer et de garantir la bande passante sur la base de paramètres configurables.

La figure Flux de trafic QoS illustre le flux de trafic depuis sa source, comment il est mis en forme par le pare-feu sur lequel la QoS est activée, puis priorisé et distribué vers sa destination.

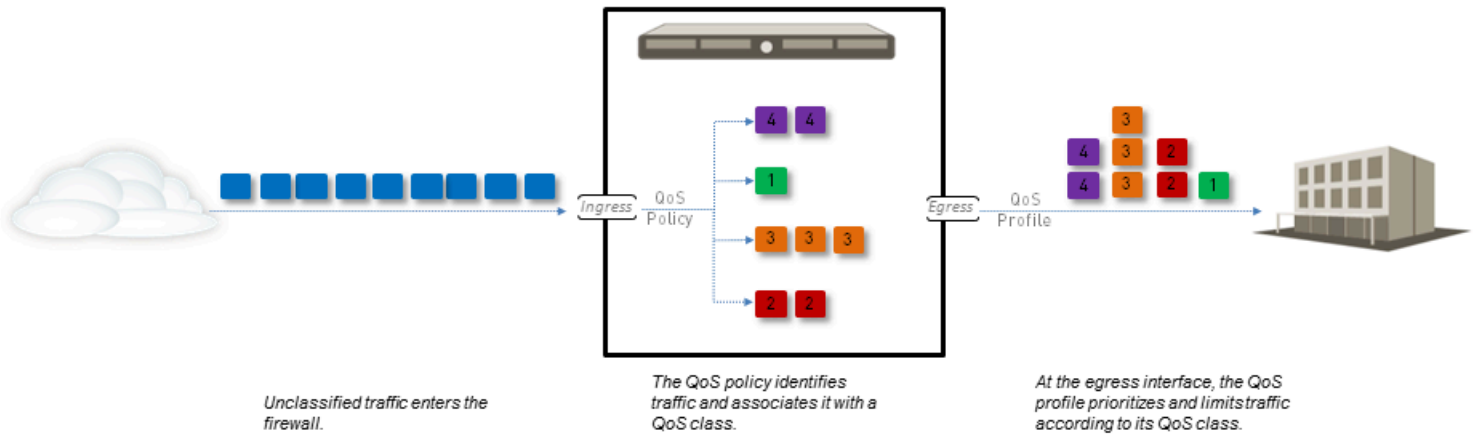



**Figure 6: Flux de trafic QoS**

Les options de configuration de la QoS vous permettent de contrôler le flux de trafic et de définir le trafic à différents points du flux. La figure Flux de trafic QoS indique où les options configurables définissent le flux de trafic. Une règle de politique QoS vous permet de définir le trafic qui doit recevoir le traitement QoS et d'affecter une classe de service QoS à ce trafic. Le trafic correspondant est par la suite mis en forme selon les paramètres de la classe du profil QoS alors qu'il sort de l'interface physique.

Chacun des composants de configuration de la QoS ont un impact sur les autres composants et les options de configuration de la QoS peuvent être utilisées pour créer une implémentation de la QoS complète et granulaire, ou être appliquées avec une interaction minimale de l'administrateur.

Chaque modèle de pare-feu prend en charge un nombre maximum de ports pouvant être configurés avec la QoS. Consultez la fiche technique de votre modèle de pare-feu ou utilisez l'outil de comparaison de produits pour afficher sur une même page la prise en charge de la fonctionnalité QoS de deux pare-feu ou plus.

# Concepts de la QoS

Consultez les rubriques suivantes pour en savoir plus sur les différents composants et mécanismes d'une configuration QoS sur un pare-feu Palo Alto Networks :

- QoS pour des applications et des utilisateurs
- Politique QoS
- Profil QoS
- Classes QoS
- Mise en file d'attente par priorité QoS
- Gestion de la bande passante de classe QoS :
- Interface de sortie QoS
- QoS applicable au trafic en texte clair et au trafic tunnellisé

## QoS pour des applications et des utilisateurs

Un pare-feu Palo Alto Networks propose une QoS de base, en contrôlant le trafic sortant du pare-feu en fonction du réseau ou sous-réseau, et étend les capacités de la QoS afin de classer et de mettre en forme le trafic en fonction de l'application et de l'utilisateur. Le pare-feu Palo Alto Networks offre cette capacité en ajoutant les fonctionnalités App-ID et User-id à la configuration de la QoS. Les entrées App-ID et User-ID permettant d'identifier des applications et utilisateurs spécifiques sur votre réseau sont désormais disponibles dans la configuration de la QoS pour vous permettre de spécifier facilement les applications et utilisateurs pour lesquels vous voulez gérer ou garantir la bande passante.

## Politique QoS

Une règle de politique QoS vous permet de définir le trafic pour recevoir le traitement QoS (traitement préférentiel ou à bande passante limitée) et d'affecter une classe de service QoS à ce trafic.

Définissez une règle de politique QoS à mettre en correspondance avec le trafic en fonction des éléments suivants :

- Applications et groupes d'applications.
- Zones source, adresses source et utilisateurs source.
- Zones de destination et adresses de destination.
- Services et groupes de services limités à des numéros de ports TCP et/ou UDP spécifiques.
- Catégories d'URL, catégories d'URL personnalisées incluses.
- Les valeurs Differentiated Services Code Point (code d'accès aux services différenciés ; DSCP) et Type of Service (type de service ; ToS) qui permettent d'indiquer le niveau de service demandé pour le trafic, tel que la remise au mieux ou de haute priorité.

***Vous ne pouvez pas appliquer de points de code DSCP ou de QoS au trafic Proxy de transfert SSL, à l'inspection SSL entrante et Proxy SSH.***

Configurez plusieurs règles de politique QoS (**Policies (Politiques)** > **QoS** pour associer différents types de trafic aux différentes Classes QoS de service.

Comme la QoS est appliquée sur le trafic à son entrée dans le pare-feu, votre règle de politique QoS est appliquée au trafic après que le pare-feu a appliqué toutes les autres règles de politique de sécurité, y compris les règles de Network Address Translation (traduction d'adresse réseau ; NAT). Si vous voulez appliquer le traitement QoS au trafic en fonction de la source, vous devez spécifier l'adresse source post-NAT dans une règle de politique QoS (n'utilisez pas l'adresse source pré-NAT).

## Profil QoS

Utilisez une règle de profil QoS pour définir les valeurs d'un maximum de huit Classes QoS contenues dans cette règle de profil unique.

Si vous disposez d'une règle de profil QoS, vous pouvez définir la Priority Queing QoS et la Gestion de la Bande passante QoS applicables aux classes QoS. Chaque règle de profil QoS vous permet de configurer la bande passante et les paramètres de priorité de chacune des classes QoS (jusqu'à concurrence de huit classes), ainsi que la bande passante totale destinée à l'ensemble des huit classes. Associez la règle de profil QoS (ou plusieurs règles de profil QoS) à une interface physique afin d'appliquer au trafic sortant de l'interface les paramètres de bande passante et de priorité que vous avez définis.

Une règle de profil QoS par défaut est disponible sur le pare-feu. Aucune limite de bande passante maximale ou garantie n'est prédéfinie dans la règle de profil par défaut et les classes définies dans le profil.

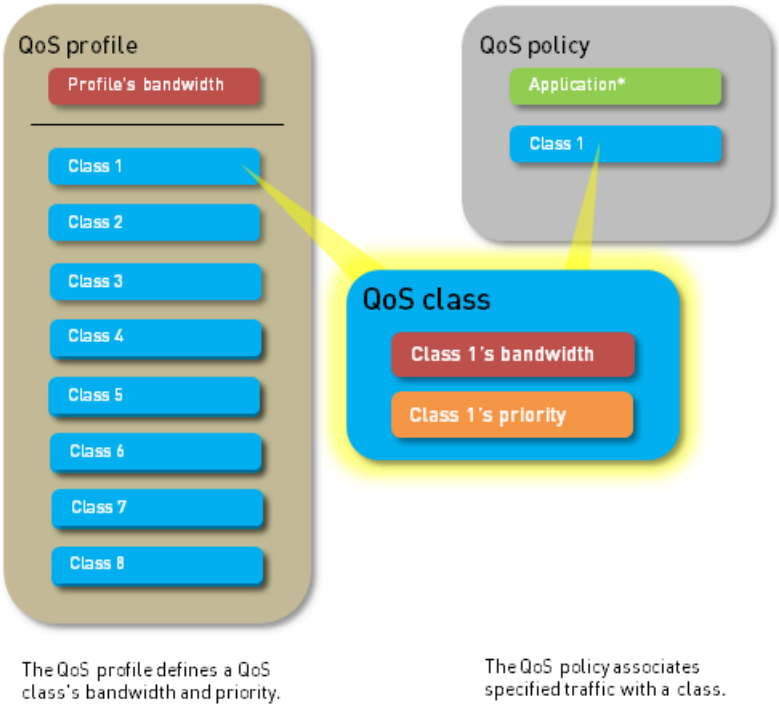
Pour définir les priorités ainsi que les paramètres de la bande passante pour les classes QoS, reportez-vous à Ajouter un rôle de profil QoS.

## Classes QoS

Une classe QoS détermine la priorité et la bande passante du trafic correspondant à une règle de Politique QoS. Vous pouvez utiliser une règle de Profil QoS pour définir des classes QoS. Jusqu'à huit classes QoS peuvent être définies dans un même profil QoS. Sauf configuration contraire, le trafic ne correspondant pas à une classe QoS est affecté à la classe 4.

La QoS Priority Queuing (Mise en file d'attente par priorité QoS) et la QoS Bandwidth Management (gestion de la bande passante QoS), qui sont les mécanismes de base d'une configuration QoS, sont configurées dans la définition de la classe QoS (reportez-vous à 4). Vous pouvez définir la priorité (temps réel, élevée, moyenne ou basse) de chaque classe QoS ainsi que la bande passante garantie et maximale du trafic correspondant. La mise en file d'attente par priorité QoS et la gestion de la bande passante déterminent l'ordre du trafic et comment il est traité lorsqu'il entre ou sort d'un réseau.




## Mise en file d'attente par priorité QoS

Une des quatre priorités suivantes peut être appliquée dans une classe QoS : temps réel, élevée, moyenne ou basse. Le trafic correspondant à une règle de politique QoS se voit attribuer la classe QoS qui est associée à cette règle, et le pare-feu traite le trafic correspondant selon la priorité associée à la classe QoS. Les paquets du flux de trafic sortant sont mis en file d'attente en fonction de leur priorité jusqu'à ce que le réseau soit prêt à les traiter. La mise en file d'attente par priorité vous permet de vous assurer que le trafic, les applications et les utilisateurs importants sont traités en priorité. La priorité en temps réel est généralement utilisée pour les applications particulièrement sensibles à la latence comme les applications voix et vidéo.

## Gestion de la bande passante de classe QoS :

La gestion de la bande passante de QoS vous permet de contrôler les flux de trafic sur un réseau de sorte que le trafic ne dépasse pas la capacité du réseau (ce qui entraînerait une congestion du réseau) et vous permet également d'allouer une bande passante à certains types de trafic ainsi qu'aux applications et aux utilisateurs. Grâce à la QoS, vous pouvez appliquer la bande passante au trafic à grande échelle ou à échelle réduite. Une règle de profil QoS vous permet de définir des limites de bande passante pour chacune des classes QoS ainsi que la bande passante totale des huit classes QoS. Dans le cadre des étapes à suivre pour procéder à la Configuration QoS, vous pouvez associer la règle de profil QoS à une interface physique pour appliquer les paramètres de bande passante au trafic qui sort de cette interface — les paramètres de chaque classe QoS sont appliqués au trafic correspondant à cette classe QoS (les classes QoS sont attribuées au trafic qui correspond aux règles de la Politique QoS), et la limite de bande passante globale du profil peut être appliquée à l'ensemble du trafic en texte clair, au trafic en texte clair provenant de différentes interfaces et sous-réseaux source, à l'ensemble du trafic tunnellisé et à chaque interface de tunnel. Vous pouvez ajouter

plusieurs règles de profil à une seule interface QoS si vous souhaitez appliquer divers paramètres de bande passante au trafic qui sort de cette interface.

Les champs suivants se rapportent aux paramètres de la bande passante QoS :

- **Egress Guaranteed (Sortie garantie)** : la quantité de bande passante garantie qui sera mise à la disposition du trafic correspondant. Dans l'éventualité où le trafic dépasse la bande passante de sortie garantie, le pare-feu achemine le trafic dans la mesure du possible. La bande passante qui est garantie, mais qui n'est pas utilisée demeure disponible pour l'acheminement de l'ensemble du trafic. Selon votre configuration QoS, vous pouvez garantir la bande passante d'une seule classe QoS, de l'intégralité ou d'une partie du trafic en texte clair ainsi que de l'intégralité ou d'une partie du trafic tunnellisé.

  Exemple :

  Le trafic de classe 1 dispose d'une bande passante de sortie garantie de 5 Gbit/s, ce qui signifie qu'une quantité de 5 Gbit/s de bande passante est disponible, sans toutefois être réservée au trafic de classe 1. Si le trafic de classe 1 n'utilise pas la bande passante garantie, ou qu'il n'en utilise qu'une portion, la quantité de bande passante restante peut être utilisée par toute autre classe de trafic. Toutefois, pendant les périodes où le trafic est élevé, l'intégralité des 5 Gbit/s de bande passante est réservé au trafic de classe 1. Au cours de ces périodes de congestion, tout trafic de classe 1 qui dépasse les 5 Gbit/s alloués est acheminé dans la mesure du possible.
- **Egress Max (Sortie max.)** : l'allocation de bande passante globale mise à la disposition du trafic correspondant. Le pare-feu ignore le trafic qui dépasse la limite de sortie maximale que vous avez définie. Selon votre configuration QoS, vous pouvez définir la limite de bande passante maximale d'une classe QoS, de l'intégralité ou d'une partie du trafic en texte clair, de l'intégralité ou d'une partie du trafic tunnellisé ainsi que de l'ensemble du trafic qui sort de l'interface QoS.

  ***La valeur cumulative de la bande passante garantie qui a été définie dans les règles de profil QoS associées à l'interface ne doit pas dépasser la bande passante totale qui est allouée à l'interface.***

Pour définir les paramètres de la bande passante pour les classes QoS, reportez-vous à Ajouter un rôle de profil QoS. Pour appliquer ensuite ces paramètres de bande passante à du trafic en texte clair et à du trafic tunnellisé, et pour définir une limite de bande passante globale pour une interface QoS, reportez-vous à Activer QoS sur une interface physique.

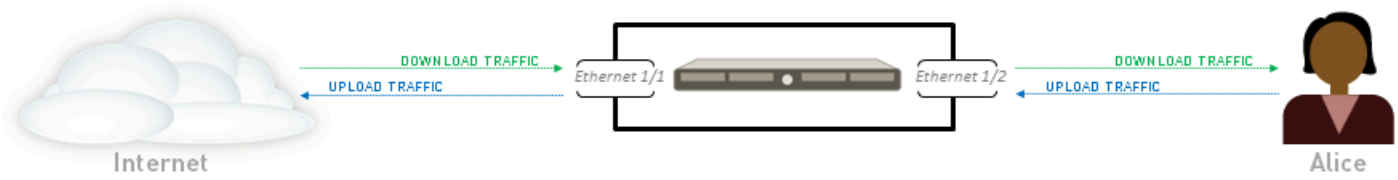
## Interface de sortie QoS

L'activation d'une règle de profil QoS sur l'interface de sortie du trafic identifié pour le traitement QoS complète une configuration QoS. L'interface d'entrée du trafic QoS est l'interface par laquelle le trafic entre dans le pare-feu. L'interface de sortie du trafic QoS est l'interface par laquelle le trafic sort du pare-feu. Pour assurer le flux du trafic, la QoS est toujours activée et appliquée sur l'interface de sortie. L'interface de sortie d'une configuration QoS peut être une interface orientée vers l'extérieur ou l'intérieur du pare-feu, en fonction du flux de trafic concerné par le traitement QoS.

Par exemple, dans un réseau d'entreprise, si vous limitez le trafic de téléchargement des employés à partir d'un site Web spécifique, l'interface de sortie de la configuration QoS correspond à l'interface interne du pare-feu car le flux de trafic provient d'Internet, et passe par le pare-feu pour parvenir à votre réseau d'entreprise. Parallèlement, lors de la limitation du trafic de charge des employés au même site Web, l'interface de sortie de la configuration QoS correspond à l'interface externe du

pare-feu car le trafic que vous limitez provient de votre réseau d'entreprise, et passe par le pare-feu pour parvenir à Internet.




- The egress interface for Alice's download traffic is Ethernet 1/2. To prioritize or limit her download traffic, Alice enables QoS on Ethernet 1/2.
- The egress interface for Alice's upload traffic is Ethernet 1/1. To prioritize or limit her upload traffic, Alice enables QoS on Ethernet 1/1.

Comme la QoS est appliquée sur le trafic à son entrée dans le pare-feu, votre règle de politique QoS est appliquée au trafic après que le pare-feu a appliqué toutes les autres règles de politique de sécurité, y compris les règles de Network Address Translation (traduction d'adresse réseau ; NAT). Si vous voulez appliquer le traitement QoS au trafic en fonction de la source, vous devez spécifier l'adresse source post-NAT dans une règle de politique QoS (n'utilisez pas l'adresse source pré-NAT).

Apprenez-en davantage sur l'identification de l'interface de sortie des applications qui doivent recevoir un traitement QoS.

## QoS applicable au trafic en texte clair et au trafic tunnellisé

Afin de pouvoir activer une interface QoS, vous devez au moins sélectionner une règle de profil QoS qui définit les paramètres de priorité et de bande passante qui s'appliquent au trafic en texte clair qui sort de l'interface. Cependant, lors de la configuration ou de la modification d'une interface QoS, vous pouvez appliquer des paramètres QoS granulaires au trafic en texte clair et tunnellisé sortant. Le traitement préférentiel et à bande passante limitée QoS peut être mis en œuvre pour le trafic tunnellisé, pour chaque interface de tunnel et/ou pour le trafic en texte clair provenant de différentes interfaces et sous-réseaux source. Sur les pare-feu Palo Alto Networks, le terme ***trafic tunnellisé*** fait référence au trafic d'interface de tunnel, et plus particulièrement au trafic IPSec en mode tunnel.

# Configuration de la QoS

Suivez les étapes ci-dessous pour configurer la Quality of Service (qualité de service ; QoS), notamment pour créer un profil QoS, créer une politique QoS et activer la QoS sur une interface.

**STEP 1 |** Établissez le trafic que vous souhaitez gérer au moyen de la QoS.

Cet exemple montre comment utiliser la QoS pour limiter la navigation Web.

Sélectionnez **ACC (ACC)** pour afficher la page **Application Command Center (Centre de commande des applications)**. Les paramètres et les diagrammes de la page **ACC (ACC)** vous permettent d'afficher les tendances et le trafic relatifs aux éléments Applications (Applications), URL Filtering (Filtrage des URL), Threat Prevention (Prévention des menaces), Data Filtering (Filtrage des données) et HIP Matches (Correspondances HIP).

Cliquez sur le nom d'une application pour afficher des informations détaillées sur celle-ci.

**STEP 2 |** Identifiez l'interface de sortie des applications qui doivent recevoir un traitement QoS.

*L'interface de sortie du trafic dépend du flux de trafic. Si vous mettez en forme du trafic entrant, l'interface de sortie est l'interface orientée vers l'intérieur. Si vous mettez en forme du trafic sortant, l'interface de sortie est l'interface orientée vers l'extérieur.*

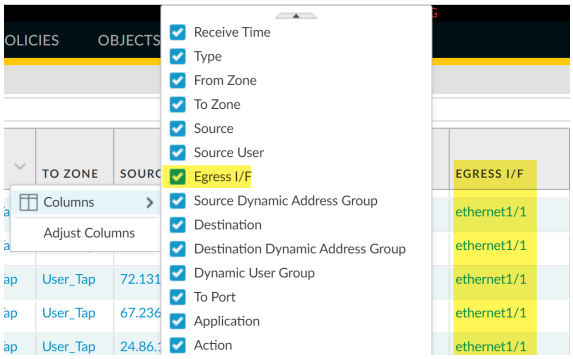
Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)** pour afficher les journaux de trafic.

Pour filtrer et afficher uniquement les journaux d'une application spécifique :

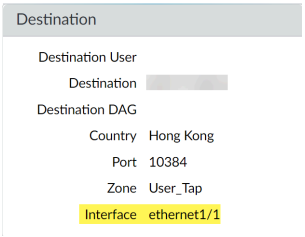
- Si une entrée s'affiche pour l'application, cliquez sur le lien souligné dans la colonne Application (Application), puis cliquez sur l'icône d'envoi.
- Si aucune entrée ne s'affiche pour l'application, cliquez sur l'icône d'ajout de journal et recherchez l'application.

L'**Egress I/F (Interface de sortie)** dans les journaux de trafic indique l'interface de sortie de chaque application. Pour afficher la colonne **Egress I/F (Interface de sortie)** si elle ne s'affiche pas par défaut :

- Cliquez sur un en-tête de colonne pour ajouter une colonne au journal :




- Cliquez sur l'icône loupe à gauche d'une entrée pour afficher un journal détaillé dans lequel l'interface de sortie de l'application est indiquée dans la section Destination (Destination) :



**STEP 3 |** Ajoutez une règle de politique QoS.

Une règle de politique QoS définit le trafic devant recevoir le traitement de la QoS. Le pare-feu attribue une classe de service QoS au trafic mis en correspondance avec la règle de la politique.

*Comme la QoS est appliquée sur le trafic à son entrée dans le pare-feu, votre règle de politique QoS est appliquée au trafic après que le pare-feu a appliqué toutes les autres règles de politique de sécurité, y compris les règles de Network Address Translation (traduction d'adresse réseau ; NAT). Si vous voulez appliquer le traitement QoS au trafic en fonction de la source, vous devez spécifier l'adresse source post-NAT dans une règle de politique QoS (n'utilisez pas l'adresse source pré-NAT).*

1. Sélectionnez **Policies (Politiques)** > **QoS (QoS)**, puis **Add (Ajoutez)** une nouvelle règle de politique.
2. Dans l'onglet **General (Général)**, donnez un **Name (Nom)** descriptif à la règle de politique QoS.
3. Précisez le trafic qui doit recevoir le traitement de la QoS, en fonction des valeurs **Source (Source)**, **Destination (Destination)**, **Application (Application)**, **Service/URL Category (Catégorie de service/d'URL)** et **DSCP/ToS (DSCP/ToS)** (les paramètres **DSCP/ToS (DSCP/ToS)** vous permettent de procéder à la mise en œuvre de la QoS en fonction de la classification DSCP).

   Par exemple, sélectionnez l'onglet **Application (Application)**, cliquez sur **Add (Ajouter)**, puis sélectionnez la **web-browsing (navigation Web)** pour appliquer la QoS au trafic de navigation Web.
4. (Facultatif) Continuez à définir d'autres paramètres. Par exemple, sélectionnez **Source (Source)**, puis **Add (Ajoutez)** un **Source User (Utilisateur source** pour fournir le traitement de la QoS au trafic Web d'un utilisateur donné.
5. Sélectionnez **Other Settings (Autres paramètres)**, puis affectez une **QoS Class (Classe QoS)** au trafic correspondant à la règle de politique. Par exemple, affectez Class 2 au trafic de navigation Web de user1 :
6. Cliquez sur **OK**.

**STEP 4 |** Ajoutez une règle de profil QoS.

Une règle de profil QoS vous permet de définir les huit classes de service que le trafic peut recevoir, y compris la priorité, et permet la gestion de la bande passante de QoS.

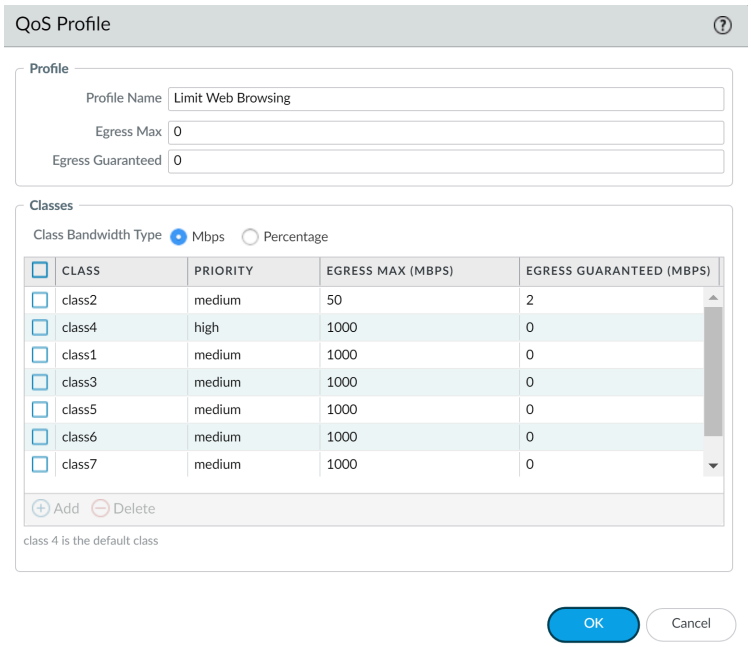
Vous pouvez modifier un profil QoS existant, y compris le profil par défaut, en cliquant sur le nom du profil QoS.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **QoS Profile (Profil QoS)**, puis **Add (Ajoutez)** un nouveau profil.
2. Saisissez un **Profile Name (Nom de profil)** descriptif.
3. Définissez les limites de bande passante globale de la règle de profil QoS :
   - Saisissez une valeur de **Egress Max (Sortie max.)** pour définir l'allocation de bande passante globale de la règle du profil QoS.
   - Saisissez une valeur de **Egress Guaranteed (Sortie garantie)** pour définir la bande passante garantie du profil QoS.

   *L'acheminement du trafic dépassant la valeur de Egress Guaranteed (Sortie garantie) se fait dans la mesure du possible et n'est pas garanti. La bande passante qui est garantie, mais qui n'est pas utilisée demeure disponible pour l'acheminement de l'ensemble du trafic.*
4. Dans la section Classes (Classes), spécifiez comment traiter jusqu'à huit classes QoS individuelles :
   1. Cliquez sur **Add (Ajouter)** pour ajouter une classe au profil QoS.
   2. Sélectionnez la **Priority (Priorité)** de la classe : temps réel, élevée, moyenne ou basse.
   3. Saisissez la valeur de la bande passante de **Egress Max (Sortie max.)** et de **Egress Guaranteed (Sortie garantie)** qui sera mise à la disposition du trafic affecté à chaque classe QoS.
5. Cliquez sur **OK**.

Dans l'exemple suivant, la règle de profil QoS nommée Limit Web Browsing (limiter le trafic de navigation Web) limite le trafic de classe 2 à une bande passante maximale de 50 Mbits/s et une bande passante garantie de 2 Mbits/s.




**STEP 5 |** Activez la QoS sur une interface physique.

Au cours de cette étape, vous pourrez choisir que le trafic en texte clair et le trafic tunnellisé reçoivent un traitement unique de la QoS.

*Vérifiez si le modèle de pare-feu que vous utilisez prend en charge l'activation de la QoS sur une sous-interface en consultant un résumé des* Spécifications du produit.

1. Sélectionnez **Network (Réseau)** > **QoS (QoS)**, puis **Add (Ajoutez)** une interface de QoS.
2. Sélectionnez **Physical Interface (Interface physique)**, puis choisissez le **Interface Name (Nom de l'interface)** sur laquelle activer la QoS.

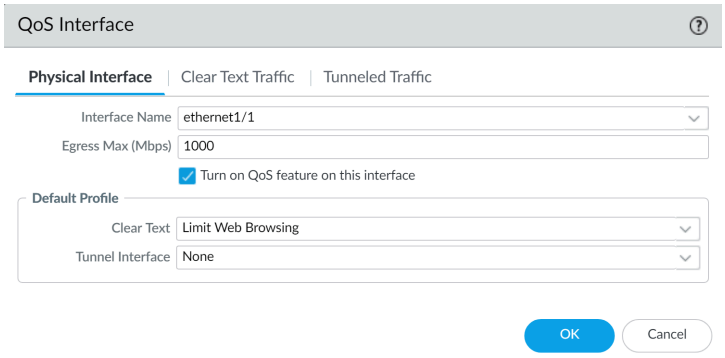
   Dans l'exemple, Ethernet 1/1 est l'interface de sortie du trafic de navigation Web (reportez-vous à l'étape 2).
3. Définissez la bande passante de **Egress Max (Sortie max.)** qui est applicable à l'ensemble du trafic qui sort de cette interface.

   *Il convient de toujours définir la valeur de Sortie max. d'une interface QoS. Veillez à ce que la valeur cumulative de la bande passante garantie qui a été définie pour les règles de profil de QoS associées à l'interface ne dépasse pas la bande passante totale qui est allouée à l'interface.*
4. Sélectionnez **Turn on QoS feature on this interface (Activer la fonctionnalité de QoS sur cette interface)**.
5. Dans la section Default Profile (Profil par défaut), sélectionnez une règle de profil QoS à appliquer à l'ensemble du trafic en **Clear Text (Texte clair)** qui sort de l'interface physique.
6. (Facultatif) Sélectionnez une règle de profil QoS à appliquer à l'ensemble du trafic tunnellisé qui sort de l'interface.

Par exemple, activez la QoS sur Ethernet 1/1 et appliquez les paramètres de priorité et de bande passante que vous avez définis pour que la règle de profil QoS intitulée Limit Web Browsing

(Limiter le trafic de navigation Web) (étape 4) soit utilisée par défaut pour le trafic en texte clair sortant.




1. (Facultatif) Passez à la définition de paramètres plus granulaires pour fournir la QoS applicable au trafic en texte clair et au trafic tunnellisé. Les paramètres configurés à l'onglet **Clear Text Traffic (Trafic en texte clair)** et à l'onglet **Tunneled Traffic (Trafic tunnellisé)** remplacent automatiquement les paramètres du profil par défaut applicables au trafic en texte clair et au trafic tunnellisé qui sont définis à l'onglet Physical Interface (Interface physique).
   - Sélectionnez **Clear Text Traffic (Trafic en texte clair)** et :
     - Définissez les bandes passantes de **Egress Guaranteed (Sortie garantie)** et de **Egress Max (Sortie max.)** du trafic en texte clair.
     - Cliquez sur **Add (Ajouter)** et appliquez une règle de profil QoS à appliquer au trafic en texte clair en fonction de l'interface et du sous-réseau sources.

       *(PA-3200 Series, PA-5200 Series, PA-5400 Series, PA-7000 Series only (Série PA-3200, Série PA-5200, Série PA-5400, Série PA-7000 uniquement)) Vous devez également sélectionner une interface de destination lors de la configuration d'une règle de stratégie QoS si la règle est appliquée à une sous-interface spécifique.*
   - Sélectionnez **Tunneled Traffic (Trafic tunnellisé)** et :
     - Définissez les bandes passantes de **Egress Guaranteed (Sortie garantie)** et de **Egress Max (Sortie max.)** du trafic tunnellisé.
     - Cliquez sur **Add (Ajouter)** pour affecter un profil QoS à une seule interface de tunnel.
2. Cliquez sur **OK**.

**STEP 6 |** Validez vos modifications.

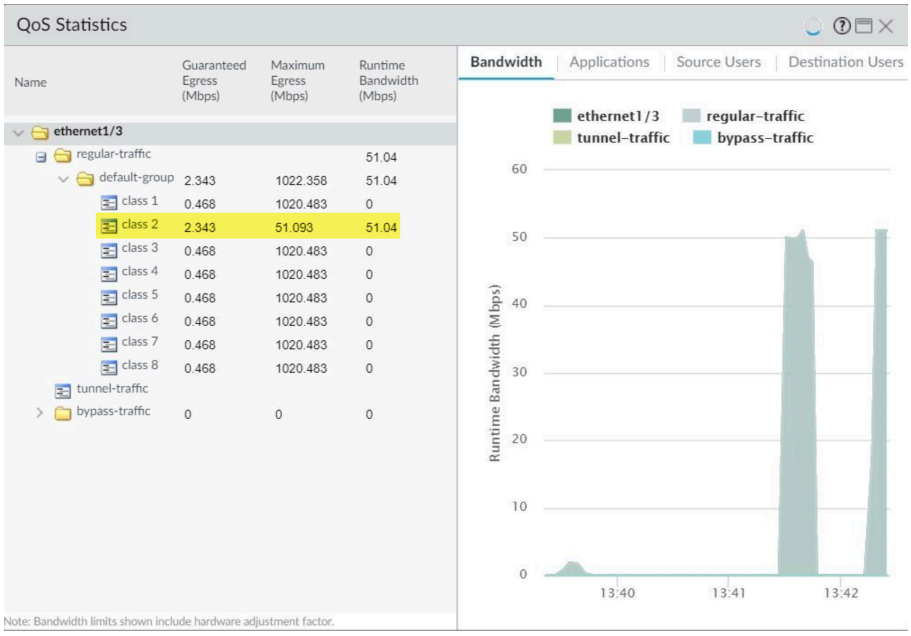
Cliquez sur **Commit (Valider)**.

**STEP 7 |** Vérifiez la configuration de la QoS.

Sélectionnez **Network (Réseau)** > **QoS (QoS)**, puis **Statistics (Statistiques)** pour afficher la bande passante QoS, les sessions actives d'un nœud ou d'une classe QoS sélectionné(e) et les applications actives du nœud ou de la classe QoS sélectionné(e).

Par exemple, consultez les statistiques pour Ethernet 1/3 avec QoS activée :




Trafic de classe 2 limité à une bande passante garantie de 2,343 Mbits/s et une bande passante maximale de 51,093 Mbits/s.

Cliquez sur les onglets pour afficher d'autres informations sur les applications, utilisateurs sources, utilisateurs de destination, règles de sécurité et règles QoS.

*Les limites de bande passante indiquées dans la fenêtre **QoS Statistics (Statistiques QoS)** incluent un facteur d'ajustement matériel.*

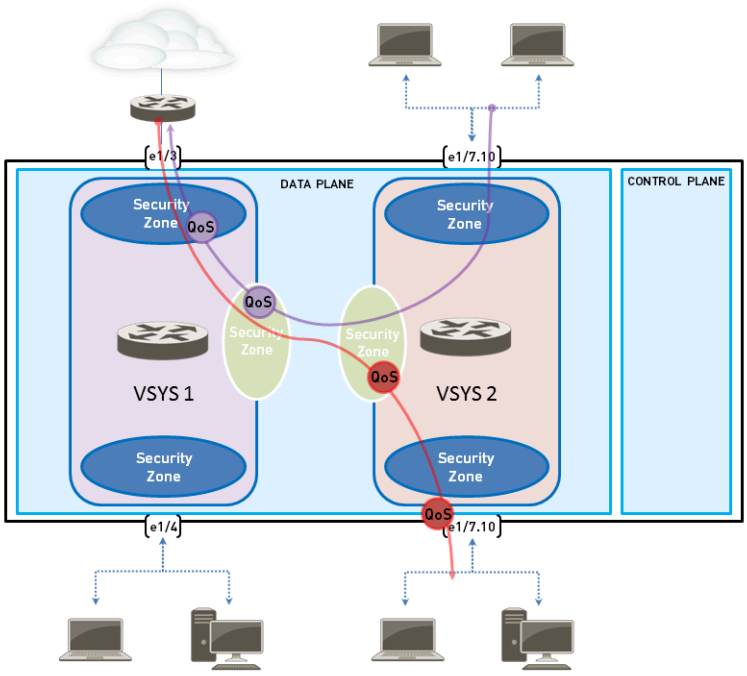
 

# Configuration de la QoS pour un système virtuel

La QoS peut être configurée pour un ou plusieurs systèmes virtuels configurés sur un pare-feu Palo Alto Networks. Un système virtuel étant un pare-feu indépendant, la QoS doit être configurée indépendamment pour un système virtuel unique.

La configuration de la QoS pour un système virtuel est similaire à celle sur un pare-feu physique, à l'exception que la configuration de la QoS pour un système virtuel nécessite la spécification de la source et de la destination du trafic. Étant donné qu'un système virtuel n'inclut pas de frontières physiques définies et que le trafic transite par plusieurs systèmes virtuels dans un environnement virtuel, la spécification de zones et d'interfaces sources et de destination du trafic est nécessaire pour contrôler et mettre en forme le trafic pour un système virtuel unique.

L'exemple ci-dessous illustre deux systèmes virtuels configurés sur un pare-feu. VSYS 1 (violet) et VSYS 2 (rouge) incluent une QoS configurée afin de définir la priorité ou de limiter deux flux de trafic distincts, indiqués par leurs lignes violette (VSYS 1) et rouge (VSYS 2) correspondantes. Les nœuds QoS indiquent les points auxquels le trafic est mis en correspondance avec une politique QoS et se voit affecter une classe de service QoS, puis indiquent ensuite le point auquel le trafic est mis en forme lorsqu'il sort du pare-feu.




Pour plus d'informations sur les systèmes virtuels et leur configuration, reportez-vous à la section Systèmes virtuels.

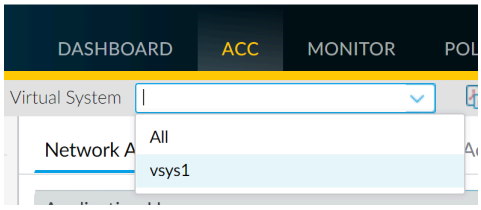
**STEP 1 |** Vérifiez que les interfaces, routeurs virtuels et zones de sécurité appropriés sont associés à chaque système virtuel.

- Pour afficher les interfaces configurées, sélectionnez **Network (Réseau)** > **Interface (Interface)**.
- Pour afficher les zones configurées, sélectionnez **Network (Réseau)** > **Zones (Zones)**.
- Pour afficher des informations sur les routeurs virtuels définis, sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**.

**STEP 2 |** Identifiez le trafic auquel appliquer la QoS.

Sélectionnez **ACC (ACC)** pour afficher la page **Application Command Center (Centre de commande des applications)**. Les paramètres et les diagrammes de la page **ACC (ACC)** vous permettent d'afficher les tendances et le trafic relatifs aux éléments Applications (Applications), URL Filtering (Filtrage des URL), Threat Prevention (Prévention des menaces), Data Filtering (Filtrage des données) et HIP Matches (Correspondances HIP).

Pour afficher des informations sur un routeur virtuel spécifique, sélectionnez le routeur virtuel dans la liste déroulante **Virtual System (Système virtuel)** :




Cliquez sur le nom d'une application pour afficher des informations détaillées sur celle-ci.

**STEP 3 |** Identifiez l'interface de sortie des applications identifiées comme nécessitant un traitement QoS.

Dans un environnement de système virtuel, la QoS est appliquée au trafic sur le point de sortie du trafic sur le système virtuel. En fonction de la configuration et de la politique QoS d'un

système virtuel, le point de sortie du trafic QoS peut être associé à une interface physique ou être une zone.

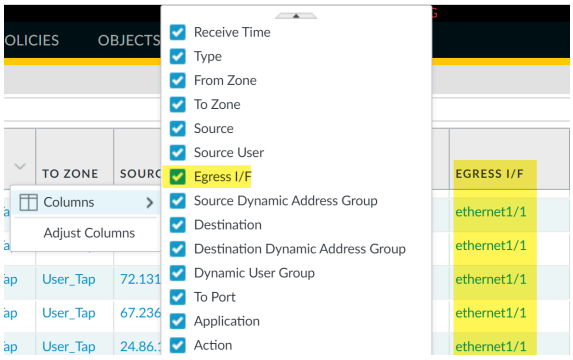
Cet exemple illustre comment limiter le trafic de navigation Web sur vsys 1.

Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)** pour afficher les journaux de trafic. Chaque entrée permet d'afficher des colonnes fournissent les informations nécessaires à la configuration de la QoS dans un environnement de système virtuel :

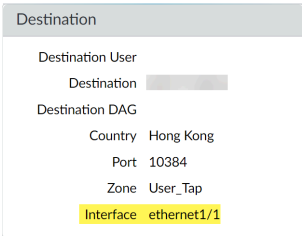
- système virtuel
- interface de sortie
- interface d'entrée
- zone source
- zone de destination

Pour afficher une colonne si elle ne s'affiche pas par défaut :

- Cliquez sur un en-tête de colonne pour ajouter une colonne au journal :




- Cliquez sur l'icône loupe à gauche d'une entrée pour afficher un journal détaillé dans lequel l'interface de sortie de l'application, ainsi que les zones source et de destination, sont indiquées dans les sections **Source (Source)** et **Destination (Destination)** :




Par exemple, pour le trafic de navigation Web provenant de VSYS 1, l'interface d'entrée est Ethernet 1/2, l'interface de sortie est Ethernet 1/1, la zone source est trust et la zone de destination est untrust.

**STEP 4 |** Créez un profil QoS.

Vous pouvez modifier un profil QoS existant, y compris le profil par défaut, en cliquant sur le nom du profil QoS.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseaux)** > **QoS Profile (Profil QoS)**, puis cliquez sur **Add (Ajouter)** pour ouvrir la boîte de dialogue QoS Profile (Profil QoS).
2. Saisissez un **Profile Name (Nom de profil)** descriptif.
3. Saisissez une valeur de **Egress Max (Sortie max.)** pour définir l'allocation de bande passante globale du profil QoS.
4. Saisissez une valeur de **Egress Guaranteed (Sortie garantie)** pour définir la bande passante garantie du profil QoS.

   *Tout trafic dépassant la limite de sortie garantie du profil QoS correspond au meilleur effort mais n'est pas garanti.*
5. Dans la section Classes (Classes) du **QoS Profile (Profil QoS)**, spécifiez comment traiter jusqu'à huit classes QoS individuelles :
   1. Cliquez sur **Add (Ajouter)** pour ajouter une classe au profil QoS.
   2. Sélectionnez la **Priority (Priorité)** de la classe.
   3. Saisissez une valeur de **Egress Max (Sortie max.)** d'une classe pour définir la limite de bande passante globale de cette classe.
   4. Saisissez une valeur de **Egress Guaranteed (Sortie garantie)** d'une classe pour définir la bande passante garantie de cette classe.
6. Cliquez sur **OK (OK)** pour enregistrer le profil QoS.

**STEP 5 |** Créez une politique QoS.

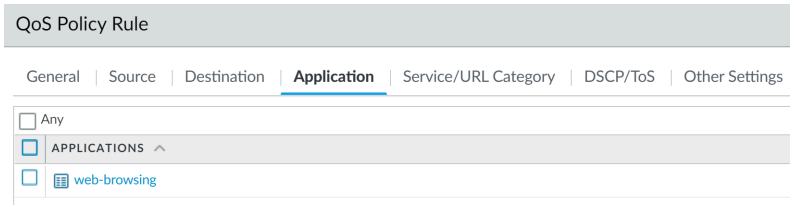
Dans un environnement de systèmes virtuels multiples, le trafic transite par plusieurs systèmes virtuels. Ainsi, lorsque vous activez la QoS pour un système virtuel, vous devez définir le trafic pour recevoir le traitement QoS en fonction des zones source et de destination. Cela permet de définir la priorité et de mettre en forme le trafic uniquement pour ce système virtuel (et non pour d'autres systèmes virtuels par lesquels le trafic peut transiter).

1. Sélectionnez **Policies (Politiques)** > **QoS (QoS)**, puis **Add (Ajoutez)** une règle de politique QoS.
2. Sélectionnez **General (Général)**, puis donnez un **Name (Nom)** descriptif à la règle de politique QoS.
3. Spécifiez le trafic auquel la règle de politique QoS s'appliquera. Utilisez les onglets **Source (Source)**, **Destination (Destination)**, **Application (Application)** et **Service/URL**

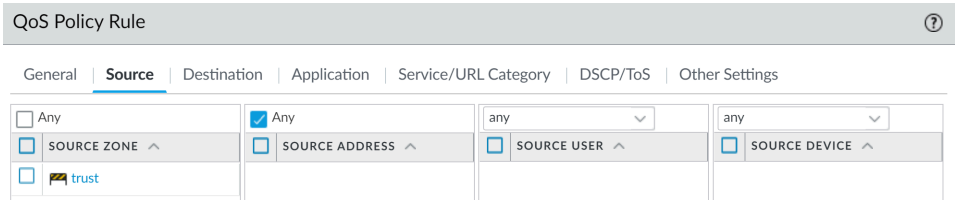
 

**Category (Catégorie de service/d'URL)** pour définir les paramètres de correspondance d'identification de trafic.

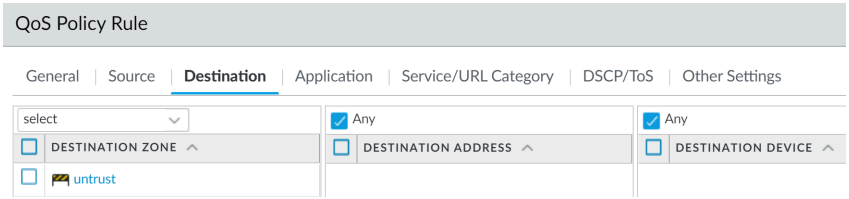
Par exemple, sélectionnez l'onglet **Application (Application)**, puis cliquez sur **Add (Ajouter)** pour ajouter la navigation Web afin d'appliquer la règle de politique QoS à cette application :



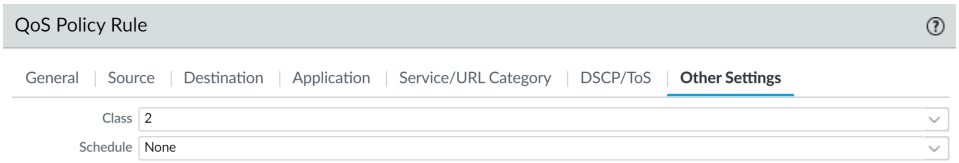

4. Sélectionnez **Source (Source)**, puis **Add (Ajoutez)** la zone source du trafic de navigation Web de vsys 1.




5. Sélectionnez **Destination (Destination)**, puis cliquez sur **Add (Ajouter)** pour ajouter la zone de destination du trafic de navigation Web de vsys 1.




6. Sélectionnez **Other Settings (Autres paramètres)**, puis une **QoS Class (Classe QoS)** à affecter à la règle de politique QoS. Par exemple, affectez la classe 2 au trafic de navigation Web sur vsys 1 :




7. Cliquez sur **OK (OK)** pour enregistrer la règle de politique QoS.

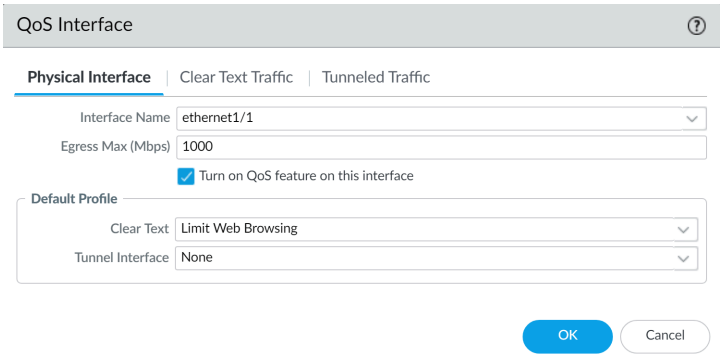
 

**STEP 6 |** Activez le profil QoS sur une interface physique.

*Il est recommandé de toujours définir la valeur de **Egress Max (Sortie max.)** d'une interface QoS.*

1. Sélectionnez **Network (Réseau)** > **QoS (QoS)**, puis cliquez sur **Add (Ajouter)** pour ouvrir la boîte de dialogue QoS Interface (Interface QoS).
2. Activez la QoS sur l'interface physique :
   1. Dans l'onglet **Physical Interface (Interface physique)**, sélectionnez le **Interface Name (Nom de l'interface)** à laquelle appliquer le profil QoS.

      Dans l'exemple, Ethernet 1/1 est l'interface de sortie du trafic de navigation Web sur vsys 1 (reportez-vous à l'étape 2).

   2. Sélectionnez **Turn on QoS feature on this interface (Activer la fonctionnalité de QoS sur cette interface)**.
3. Dans l'onglet **Physical Interface (Interface physique)**, sélectionnez le profil QoS par défaut à appliquer à l'ensemble du trafic en **Clear Text (Texte clair)**.

   (Facultatif) Le champ **Tunnel Interface (Interface de tunnel)** vous permet d'appliquer un profil QoS par défaut à l'ensemble du trafic tunnellisé.
4. (Facultatif) Dans l'onglet **Clear Text Traffic (Trafic en texte clair)**, configurez d'autres paramètres QoS pour le trafic en texte clair :
   - Définissez les bandes passantes de **Egress Guaranteed (Sortie garantie)** et de **Egress Max (Sortie max.)** du trafic en texte clair.
   - Cliquez sur **Add (Ajouter)** pour appliquer un profil QoS au trafic en texte clair sélectionné, en sélectionnant en plus le trafic pour le traitement QoS en fonction de l'interface source et du sous-réseau source (création d'un nœud QoS).
5. (Facultatif) Dans l'onglet **Tunneled Traffic (Trafic tunnellisé)**, configurez d'autres paramètres QoS pour les interfaces de tunnel :
   - Définissez les bandes passantes de **Egress Guaranteed (Sortie garantie)** et de **Egress Max (Sortie max.)** du trafic tunnellisé.
   - Cliquez sur **Add (Ajouter)** pour associer une interface de tunnel sélectionnée à un profil QoS.
6. Cliquez sur **OK** pour enregistrer les modifications.
7. **Commit (Validez)** les modifications.

**STEP 7 |** Vérifiez la configuration de la QoS.

- Sélectionnez **Network (Réseau)** > **QoS (QoS)** pour afficher la page QoS Policies (Politiques QoS). La page **QoS Policies (Politiques QoS)** permet de vérifier si la QoS est activée et inclut un lien **Statistics (Statistiques)**. Cliquez sur le lien Statistics (Statistiques) pour afficher la bande passante QoS, les sessions actives d'un nœud ou d'une classe QoS sélectionné(e) et les applications actives du nœud ou de la classe QoS sélectionné(e).
- Dans un environnement à plusieurs systèmes virtuels, les sessions ne peuvent pas concerner plusieurs systèmes. Plusieurs sessions sont créées pour un flux de trafic si le trafic transite par plusieurs systèmes virtuels. Pour parcourir les sessions en cours d'exécution sur le pare-feu et afficher les règles QoS appliquées et les classes QoS, sélectionnez **Monitor (Surveillance)** > **Session Browser (Navigateur de session)**.

# Mise en œuvre de la QoS en fonction de la classification DSCP

Un Differentiated Services Code Point (code d'accès aux services différenciés ; DSCP) est une valeur de l'en-tête de paquet qui peut servir à demander, pour le trafic, (par exemple) le traitement de priorité élevée ou l'acheminement dans la mesure du possible. La classification DSCP basée sur la session vous permet de respecter les valeurs DSCP du trafic entrant et de marquer une session avec une valeur DSCP dès que le trafic de la session sort du pare-feu. L'ensemble du trafic entrant et sortant pour une session peut ainsi recevoir un traitement QoS continu lorsqu'il transite par votre réseau. Par exemple, le trafic de retour (entrant) d'un serveur externe peut désormais être traité avec la même priorité QoS que celle initialement mise en œuvre par le pare-feu pour le flux sortant en fonction de la valeur DSCP que le pare-feu a décelé au début de la session. Les périphériques réseau entre le pare-feu et l'utilisateur final mettront également en œuvre la même priorité pour le trafic de retour (et tout trafic entrant ou sortant pour la session).

***Vous ne pouvez pas appliquer de points de code DSCP ou de QoS au trafic Proxy de transfert SSL, à l'inspection SSL entrante et Proxy SSH.***

Différents types de marquage DSCP indiquent différents niveaux de service :

L'exécution de cette étape permet au pare-feu de marquer le trafic avec la même valeur DSCP que celle détectée au début d'une session (dans cet exemple, le pare-feu marque le trafic de retour avec la valeur DSCP AF11). Alors que la configuration de la QoS vous permet de mettre en forme le trafic lorsqu'il sort du pare-feu, l'activation de cette option dans une règle de sécurité permet aux autres périphériques réseau entre le pare-feu et le client de continuer à mettre en œuvre la priorité du trafic marqué DSCP.

- **Expedited Forwarding (EF)** (transfert expédié ; EF) : permet de demander une bande passante garantie à faible perte et faible latence pour le trafic. Les paquets qui comportent des valeurs de point de code EF indiquent généralement une remise de priorité la plus haute garantie.
- **Assured Forwarding (AF) (transfert assuré ; AF)** : permet une remise fiable pour les applications. Les paquets avec un point de code AF indiquent une requête de marquage du trafic pour recevoir un traitement de haute priorité fourni par le service au mieux (bien que les paquets avec un point de code EF soient toujours prioritaires par rapport à ceux avec un point de code AF).
- **Class Selector (CS)** (sélecteur de classe ; CS) : permet une rétrocompatibilité avec les périphériques réseau qui utilisent le champ Priorité IP pour marquer le trafic prioritaire.
- **IP Precedence (ToS)** (priorité IP ; ToS) : permet aux périphériques réseau de marquer le trafic prioritaire (le champ d'en-tête Priorité IP était utilisé pour indiquer la priorité d'un paquet avant d'introduire la classification DSCP).
- **Custom Codepoint** (point de code personnalisé) : permet de créer un point de code personnalisé à mettre en correspondance avec le trafic en saisissant un **Codepoint Name** (Nom de point de code) et une **Binary Value** (Valeur binaire).

Par exemple, sélectionnez le **Assured Forwarding (AF)** (transfert assuré ; AF) de façon à ce que le trafic marqué avec une valeur de point de code AF (AF) ait une priorité supérieure pour une remise fiable par rapport aux applications marquées pour recevoir une priorité inférieure. Suivez les étapes ci-dessous pour activer la classification DSCP basée sur la session, Commencez par configurer la QoS en fonction du marquage DSCP détecté au début d'une session. Vous pouvez ensuite

permettre au pare-feu de marquer le flux de retour pour une session avec la même valeur DSCP utilisée pour mettre en œuvre la QoS pour le flux sortant initial.

**STEP 1 |** Effectuez les étapes préliminaires pour procéder à la Configuration de la QoS.

**STEP 2 |** Définissez le travail qui doit recevoir le traitement QoS en fonction de la valeur DSCP.

1. Sélectionnez **Policies (Politiques)** > **QoS (QoS)**, puis cliquez sur **Add (Ajouter)** pour ajouter une règle QoS ou modifier une règle QoS existante et renseignez les champs requis.
2. Sélectionnez **DSCP/ToS (DSCP/ToS)** et sélectionnez les **Codepoints (Points de code)**.
3. **Add (Ajoutez)** des points de code DSCP/ToS auxquels vous voulez appliquer la QoS.
4. Sélectionnez le **Type (Type)** de marquage DSCP/ToS pour la règle QoS à mettre en correspondance avec le trafic :

   *Il est recommandé d'utiliser un seul type DSCP pour gérer et définir la priorité de votre trafic réseau.*
5. Mettez en correspondance la politique QoS avec le trafic à une échelle plus granulaire en spécifiant la valeur de **Codepoint (Point de code)**. Par exemple, lorsque Assured Forwarding (Transfert assuré ; AF) est sélectionné comme **Type (Type)** de valeur DSCP pour la politique à mettre en correspondance avec le trafic, spécifiez une valeur de **Codepoint (Point de code)**, telle que AF11.

   *Lorsque Expedited Forwarding (EF) (Transfert expédié ; EF) est sélectionné comme **Type (Type)** de marquage DSCP, une valeur de **Codepoint (Point de code)** granulaire ne peut pas être spécifiée. La règle de politique QoS correspond au trafic marqué avec une valeur de point de code EF.*
6. Sélectionnez **Other Settings** (Autres paramètres), puis affectez une **QoS Class** (Classe QoS) au trafic correspondant à la règle QoS. Dans cet exemple, affectez la classe 1 aux sessions où un marquage DSCP de valeur AF11 est détecté pour le premier paquet dans la session.
7. Cliquez sur **OK (OK)** pour enregistrer la règle QoS.

**STEP 3 |** Définissez la priorité QoS pour le trafic à recevoir pour lorsqu'il est mis en correspondance avec une règle QoS en fonction du marquage DSCP détecté au début d'une session.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **QoS Profile (Profil QoS)**, puis **Add (Ajoutez)** ou modifiez un profil QoS existant. Pour plus d'informations sur les options de profil permettant de définir la priorité et la bande passante du trafic, reportez-vous aux sections Concepts de la QoS et Configuration de la QoS.
2. **Add (Ajoutez)** ou modifiez une classe de profil. Par exemple, comme vous avez classé AF11 comme trafic de classe 1 à l'étape 2, vous pouvez ajouter ou modifier une entrée de **class1 (classe 1)**.
3. Sélectionnez une **Priority (Priorité)** pour la classe de trafic, telle que **high (élevée)**.
4. Cliquez sur **OK** pour enregistrer le profil QoS.

**STEP 4 |** Activer la QoS sur une interface.

Sélectionnez **Network (Réseau)** > **QoS (QoS)**, puis **Add (Ajoutez)** ou modifiez une interface et choisissez **Turn on QoS feature on this interface (Activer la fonctionnalité QoS sur cette interface)**.

Dans cet exemple, le trafic avec un marquage DSCP de valeur AF11 est mis en correspondance avec la règle QoS et se voit affecté la classe 1. Le profil QoS activé sur l'interface met en œuvre un traitement de haute priorité pour le trafic de classe 1 lorsqu'il sort du pare-feu (le trafic ***sortant*** pour la session).

**STEP 5 |** Activez le marquage DSCP.

Marquez le trafic de retour avec une valeur DSCP de façon à ce que le flux entrant pour une session soit marqué avec la même valeur DSCP détectée pour le flux sortant.

1. Sélectionnez **Policies (Stratégies)** > **Security (Sécurité)**, puis **Add (Ajoutez)** ou modifiez une stratégie de sécurité.
2. Sélectionnez **Actions (Actions)** puis, dans le menu déroulant **QoS Marking (Marquage QoS)**, choisissez **Follow-Client-to-Server-Flow (Suivre le flux du client au serveur)**.
3. Cliquez sur **OK** pour enregistrer vos modifications.

L'exécution de cette étape permet au pare-feu de marquer le trafic avec la même valeur DSCP que celle détectée au début d'une session (dans cet exemple, le pare-feu marque le trafic de retour avec la valeur DSCP AF11). Alors que la configuration de la QoS vous permet de mettre en forme le trafic lorsqu'il sort du pare-feu, l'activation de cette option dans une règle de sécurité permet aux autres périphériques réseau entre le pare-feu et le client de continuer à mettre en œuvre la priorité du trafic marqué DSCP.

**STEP 6 |** Commit (Validez) la configuration.

**Commit (Validez)** vos modifications.

# Cas pratiques relatifs à la QoS

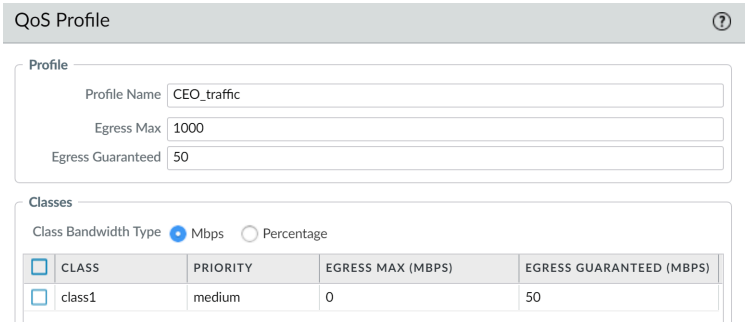
Les cas pratiques suivants montrent comment utiliser la QoS dans des scénarios courants :

- Cas d'utilisation : QoS pour un utilisateur
- Cas d'utilisation : QoS pour des applications voix et vidéo

## Cas d'utilisation : QoS pour un utilisateur

Une directrice générale constate, pendant des périodes de forte utilisation du réseau, qu'elle ne peut pas accéder aux applications de l'entreprise pour répondre efficacement à des communications professionnelles critiques. L'administrateur informatique souhaite vérifier que l'ensemble du trafic destiné et provenant de la directrice générale reçoit un traitement préférentiel par rapport au trafic des autres employés afin qu'elle puisse non seulement accéder mais également obtenir des performances élevées des ressources réseau critiques.

**STEP 1 |** L'administrateur crée le profil QoS ***CEO_traffic*** pour définir comment le trafic provenant de la directrice générale sera traité et mis en forme lorsqu'il est acheminé en dehors du réseau de l'entreprise :




L'administrateur affecte une bande passante garantie (**Egress Guaranteed (Sortie garantie)**) de 50 Mbits/s pour s'assurer que la directrice générale disposera à tout moment de la quantité de bande passante garantie (plus que ce dont elle a besoin), quelle que soit la congestion du réseau.

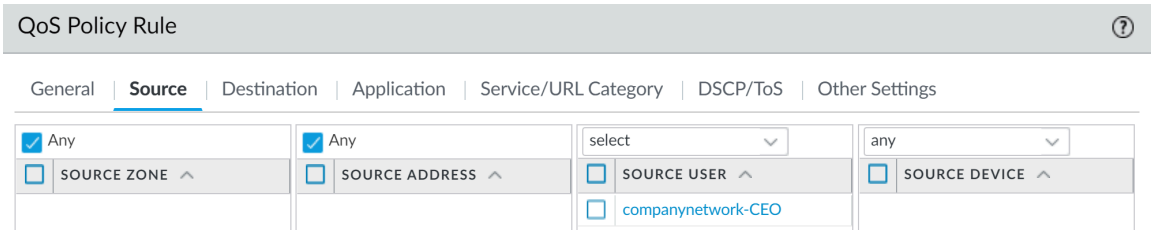
L'administrateur désigne ensuite le trafic de classe 1 comme étant de priorité élevée et définit l'utilisation de bande passante maximale du profil (**egress Max (Sortie max)**) sur 1 000 Mbits/s, la même bande passante maximale que celle de l'interface sur laquelle l'administrateur activera la QoS. L'administrateur choisit de ne pas limiter l'utilisation de la bande passante de la directrice générale.

***Il convient de renseigner le champ Egress Max (Sortie max) d'un profil QoS, même si la bande passante maximale du profil correspond à la bande passante maximale de l'interface. La bande passante maximale du profil QoS ne doit jamais dépasser la bande passante maximale de l'interface sur laquelle vous envisagez d'activer la QoS.***

**STEP 2 |** L'administrateur crée une politique QoS afin d'identifier le trafic de la directrice générale (**Policies (Politiques)** > **QoS (QoS)**) et lui affecte la classe qu'il a définie dans le profil QoS (reportez-vous à l'étape précédente). Le User-ID étant configuré, l'administrateur utilise l'onglet **Source** de la politique QoS pour bien différencier le trafic de la directrice générale grâce à son nom d'utilisateur sur le réseau de l'entreprise. (Si le User-ID n'est pas configuré, l'administrateur

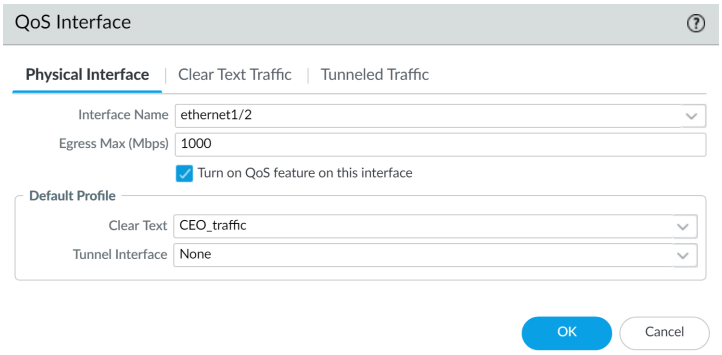
peut **Add (Ajouter)** l'adresse IP de la directrice générale sous **Source Address (Adresse source)**. Voir User-ID.) :




L'administrateur associe le trafic de la directrice générale à la classe 1 (onglet **Other Settings (Autres paramètres)**, puis renseigne les autres champs requis de la politique ; l'administrateur donne à la politique un **Name (Nom)** descriptif (onglet **General (Général)**), puis sélectionnez **Any (Tout)** pour la **Source Zone (Zone Source)** (source )(onglet **Source**) et la **Destination Zone (Zone de destination)** (onglet **Destination** ) :

| | NAME | TAGS | Source | | | | Destination | | | APPLICATION | SERVICE | DSCP/TOS | CLASS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS | DEVICE | | | | |
| 1 | HTTPS | none | trust | any | any | any | untrust | any | any | web-browsing | any | any | 2 |
| 2 | Voice-Video | none | any | any | any | any | any | any | any | voip-video-l... | any | any | 1 |
| 3 | Guarantee CEO bandwidth | none | any | any | companynet... | any | any | any | any | any | any | any | 1 |

**STEP 3 |** Maintenant que la classe 1 est associée au trafic de la directrice générale, l'administrateur active la QoS en cochant **Turn on QoS feature on interface (Activer la fonctionnalité de QoS sur cette interface)** et en sélectionnant l'interface de sortie du flux de trafic. L'interface de sortie du flux de trafic de la directrice générale est l'interface orientée vers l'extérieur, ici ethernet 1/2 :



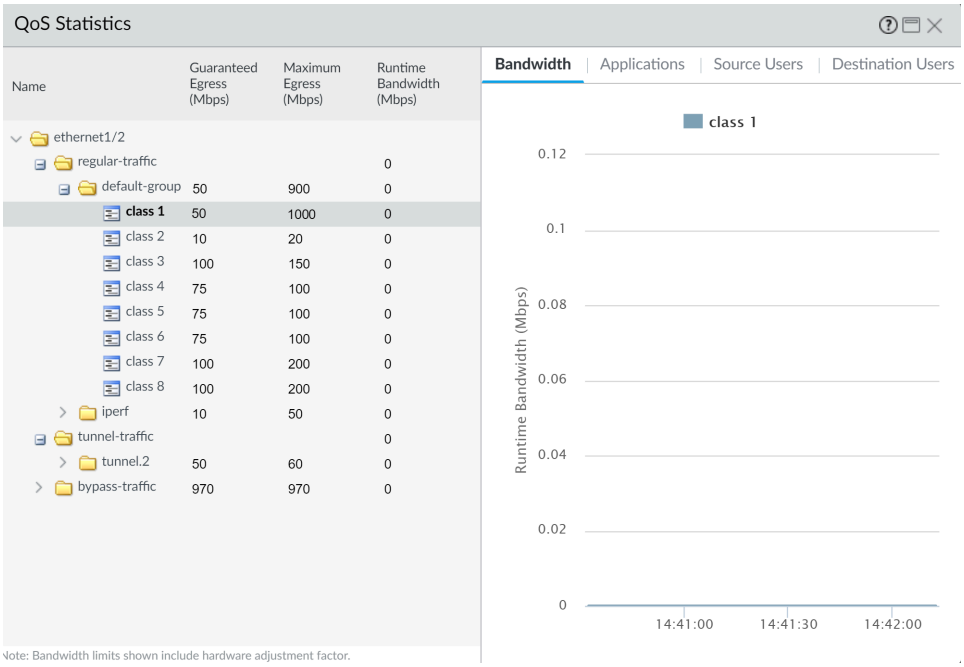

Étant donné que l'administrateur souhaite s'assurer que l'ensemble du trafic provenant de la directrice générale est garanti par le profil QoS et la politique QoS associée qu'il a créés, il sélectionne le profil *CEO_traffic* à appliquer au trafic **Clear Text (Texte clair)** provenant d'ethernet 1/2.

**STEP 4 |** Une fois la configuration QoS validée, l'administrateur accède à la page **Network (Réseau)** > **QoS (QoS)** pour vérifier si le profil QoS CEO_traffic est activé sur l'interface orientée vers l'extérieur, à savoir ethernet 1/2 :

| NAME | GUARANTEED EGRESS (MBPS) | MAXIMUM EGRESS (MBPS) | PROFILE | ENABLED | |
|---|---|---|---|---|---|
| ethernet1/2 | | 1,000.000 | | ✓ | Statistics |
| Tunneled Traffic | | | | | |
| Clear Text Traffic | 50.000 | | CEO_traffic | | |

**STEP 5 |** Il clique sur **Statistics (Statistiques)** pour voir comment le trafic provenant de la directrice générale (classe 1) est mis en forme lorsqu'il provient d'ethernet 1/2:




*Ce cas montre comment appliquer la QoS au trafic provenant d'un utilisateur source unique. Toutefois, si vous souhaitez également garantir ou mettre en forme le trafic vers un utilisateur de destination, vous pouvez procéder à une configuration QoS similaire. À la place, ou en plus de ce flux de travail, créez une politique QoS qui spécifie l'adresse IP de l'utilisateur comme* ***Destination Address (Adresse de destination)*** *dans la page* ***Policies (Politiques)*** *>* ***QoS (QoS)*** *(plutôt que de spécifier les informations source de l'utilisateur), puis activez la QoS sur l'interface orientée vers l'intérieur du réseau dans la page* ***Network (Réseau)*** *>* ***QoS (QoS)*** *(plutôt que l'interface orientée vers l'extérieur)*

## Cas d'utilisation : QoS pour des applications voix et vidéo

Le trafic voix et vidéo est particulièrement sensible aux mesures que la QoS met en forme et contrôle, notamment la latence et la gigue. Pour que les transmissions voix et vidéo soient audibles et nettes, les paquets voix et données ne peuvent pas être arrêtés, différés ou envoyés de manière incohérente. Pour les applications voix et vidéo, il est recommandé non seulement de garantir la bande passante mais aussi la priorité au trafic voix et vidéo.

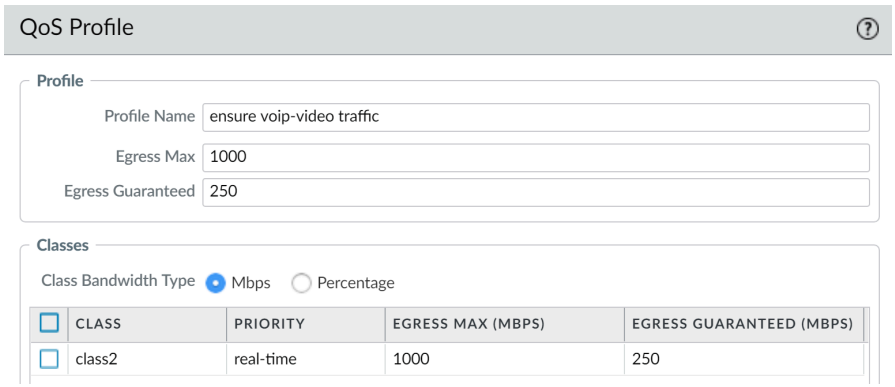
Dans cet exemple, les employés d'une filiale rencontrent des difficultés et des manques de fiabilité à utiliser les technologies de vidéoconférence et de Voice Over IP (voix sur IP ; VoIP) afin de réaliser des communications professionnelles avec d'autres filiales, des partenaires et des clients. Un administrateur informatique tente de mettre en œuvre la QoS afin de résoudre ces problèmes et de garantir des communications professionnelles efficaces et fiables aux employés de la filiale. Étant donné que l'administrateur souhaite garantir la QoS pour le trafic réseau entrant et sortant, il activera la QoS sur les interfaces vers l'intérieur et vers l'extérieur du pare-feu.

**STEP 1 |** L'administrateur crée un profil QoS, en définissant la classe 2 afin que tout trafic de classe 2 dispose d'une priorité en temps réel et sur une interface avec une bande passante maximale

de 1 000 Mbits/s, il garantit une bande passante en permanence de 250 Mbits/s, périodes de pointe d'utilisation du réseau incluses.

La priorité en temps réel est généralement recommandée pour les applications sensibles à la latence, et permet plus particulièrement de garantir les performances et la qualité des applications voix et vidéo.

Dans la page **Network (Réseau)** > **Network Profiles (Profils réseau)** > **Qos Profile (Profil QoS)**, l'administrateur clique sur **Add (Ajouter)**, saisit le **Profile Name (Nom du profil)** ensure voip-video traffic, puis définit le trafic de classe 2.

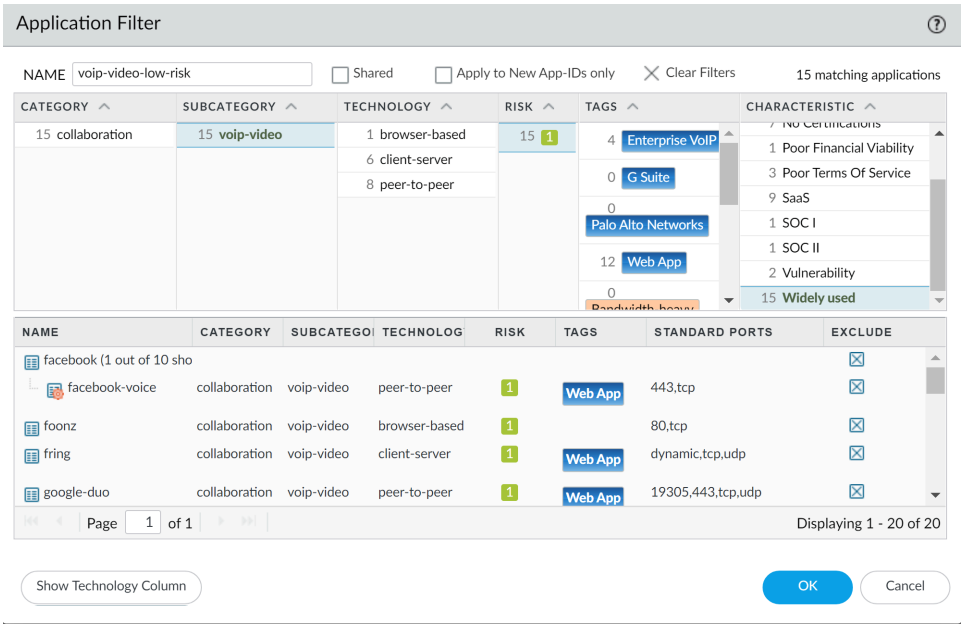



**STEP 2 |** L'administrateur crée une politique QoS afin d'identifier le trafic voix et vidéo. Étant donné que l'entreprise n'a pas d'application voix et vidéo standard, l'administrateur souhaite s'assurer que la QoS s'applique à plusieurs applications largement et régulièrement utilisées par les employés pour communiquer avec d'autres filiales, des partenaires et des clients. Dans l'onglet **Policies (Politiques)** > **QoS (QoS)** > **QoS Policy Rule (Règle de politique de QoS)** > **Applications (Applications)**, l'administrateur clique sur **Add (Ajouter)** et ouvre la fenêtre **Application Filter (Filtre d'applications)**. L'administrateur sélectionne ensuite des critères afin de filtrer les applications auxquelles il souhaite appliquer la QoS, en choisissant la sous-catégorie voip-video,

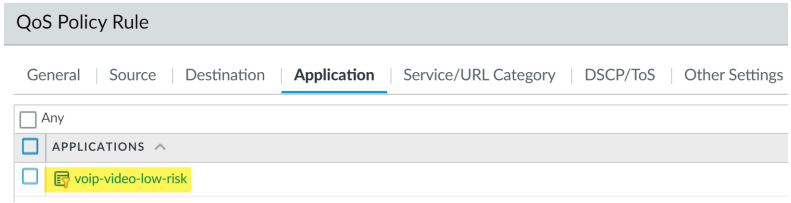
 

puis en affinant en spécifiant les applications voip-video qui sont à la fois à faible risque et largement utilisées.

Le filtre d'application est un outil dynamique qui, lorsqu'il est utilisé pour filtrer des applications dans la politique QoS, permet d'appliquer la QoS à toutes les applications correspondant aux critères voip-video, low risk et widely used à un moment donné.




L'administrateur nomme le **Application Filter (Filtre d'applications)** voip-video-low-risk, et l'inclut dans la politique QoS :




L'administrateur nomme la politique QoS Voice-Video et sélectionne Other Settings (Autres paramètres) pour affecter tout le trafic correspondant à la classe 2 de la politique. Il utilisera la politique QoS Voice-Video pour le trafic QoS entrant et sortant. Il définit dont les informations **Source** et **Destination** sur **Any (Tout)** :

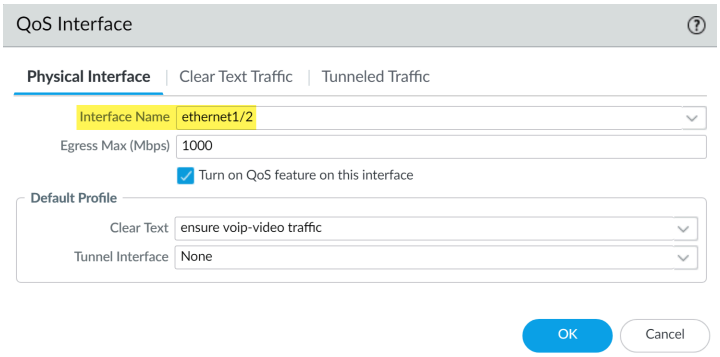
| | | | Source | | | | Destination | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | NAME | TAGS | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS | DEVICE | APPLICATION | SERVICE | DSCP/TOS | CLASS |
| 1 | HTTPS | none | trust | any | any | any | untrust | any | any | web-browsing | any | any | 2 |
| 2 | Voice-Video | none | any | any | any | any | any | any | any | voip-video-l... | any | any | 1 |

**STEP 3 |** Étant donné que l'administrateur souhaite appliquer la QoS aux communications voix et vidéo entrantes et sortantes, il active la QoS sur l'interface orientée vers l'extérieur du réseau (pour

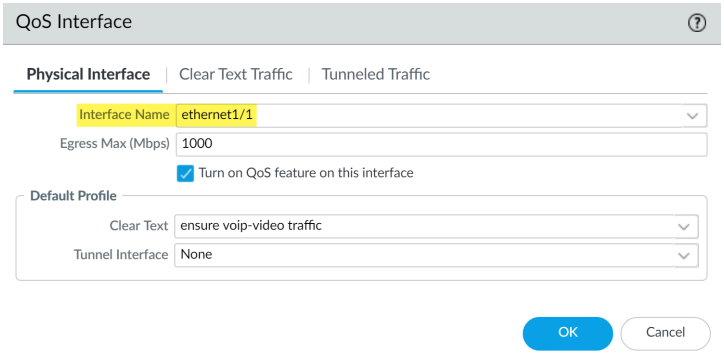
 

appliquer la QoS aux communications sortantes) et sur l'interface orientée vers l'intérieur (pour appliquer la QoS aux communications entrantes).

L'administrateur commence par activer le profil QoS qu'il a créé, ensure voice-video traffic (dans ce profil, la classe 2 est associée à la politique créée, Voice-Video) sur l'interface orientée vers l'extérieur, ici ethernet 1/2.




Il active ensuite le même profil QoS ensure voip-video traffic sur une seconde interface, soit l'interface orientée vers l'intérieur (ici ethernet 1/1).




**STEP 4 |** L'administrateur sélectionne **Network (Réseau)** > **QoS (QoS)** pour vérifier si la QoS est activée pour le trafic voix et vidéo entrant et sortant :

| NAME | GUARANTEED EGRESS (MBPS) | MAXIMUM EGRESS (MBPS) | PROFILE | ENABLED | |
|---|---|---|---|---|---|
| ethernet1/1 | | 1,000.000 | | ☑ | Statistics |
| Tunneled Traffic | | | | | |
| Clear Text Traffic | 250.000 | | ensure voip-video traffic | | |
| ethernet1/2 | | 1,000.000 | | ☑ | Statistics |
| Tunneled Traffic | | | | | |
| Clear Text Traffic | 250.000 | | ensure voip-video traffic | | |

L'administrateur a bien activé la QoS sur les deux interfaces du réseau, vers l'intérieur et l'extérieur. La priorité en temps réel est désormais garantie pour le trafic d'applications voix et vidéo lorsqu'il entre et sort du réseau, garantissant ainsi que ces communications, qui sont particulièrement sensibles à la latence et à la gigue, peuvent être utilisées en toute confiance et efficacité pour des communications professionnelles internes et externes.

# VPN

Les Virtual Private Networks (réseaux privés virtuels ; VPN) créent des tunnels qui permettent aux utilisateurs/systèmes de se connecter en toute sécurité à un réseau public comme s'ils se connectaient à Local Area Network (réseau local) (LAN). Pour configurer un tunnel VPN, vous avez besoin d'une paire de périphériques qui peuvent s'authentifier mutuellement et crypter le flux d'informations entre eux. Ces périphériques peuvent être une paire de pare-feu Palo Alto Networks, ou un pare-feu Palo Alto Networks et un périphérique VPN d'un autre fournisseur.

# Déploiements de VPN

Le pare-feu Palo Alto Networks prend en charge les déploiements de VPN suivants :

- **VPN de site à site** : un VPN simple qui connecte un site central et un site distant, ou un VPN Hub and Spoke qui connecte un site central à plusieurs sites distants. Le pare-feu utilise l'ensemble de protocoles IP Security (protocole de sécurité pour IP ; IPSec) afin de configurer un tunnel sécurisé pour le trafic entre deux sites. Consultez Présentation du VPN de site à site.
- **VPN d'utilisateur distant à site** : une solution qui utilise l'agent GlobalProtect pour permettre à un utilisateur distant d'établir une connexion sécurisée via le pare-feu. Cette solution utilise SSL et IPSec pour établir une connexion sécurisée entre l'utilisateur et le site. Reportez-vous au Guide de l'administrateur GlobalProtect.
- **VPN à grande échelle** : le VPN à grande échelle GlobalProtect de Palo Alto Networks (LSVPN) fournit une méthode simplifiée pour déployer un VPN Hub and Spoke évolutif comportant jusqu'à 1 024 bureaux satellites. Cette solution nécessite le déploiement de pare-feu Palo Alto Networks sur le concentrateur et sur chaque terminaison. Elle utilise des certificats pour l'authentification des périphériques, SSL pour sécuriser la communication entre tous les composants et IPSec pour sécuriser les données. Reportez-vous à la section VPN à grande échelle (LSVPN).

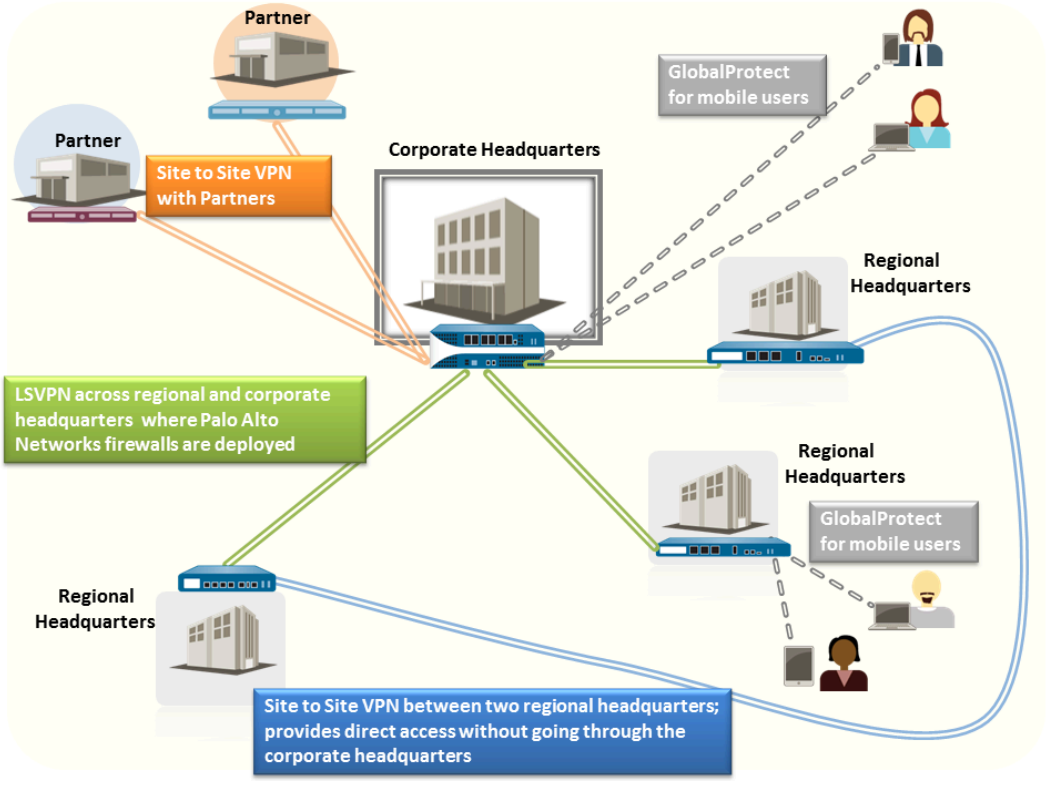



**Figure 7: Déploiements de VPN**

# Présentation du VPN de site à site

Une connexion VPN qui vous permet de connecter deux Local Area Networks (réseaux locaux ; LAN) est appelée un VPN de site à site. Vous pouvez configurer des réseaux privés virtuels de routage pour connecter des pare-feu Palo Alto Networks à deux sites ou un pare-feu Palo Alto Networks à un périphérique de sécurité tiers à un autre emplacement. Le pare-feu peut également interagir avec des périphériques VPN tiers basés sur une politique ; le pare-feu Palo Alto Networks prend en charge les VPN de routage.

Le pare-feu Palo Alto Networks configure un VPN de routage, où il prend une décision de routage en fonction de l'adresse IP de destination. Si le trafic est routé vers une destination spécifique via un tunnel VPN, il est alors traité en tant que trafic VPN.

L'ensemble de protocoles IPSec permet de configurer un tunnel sécurisé pour le trafic VPN et les informations contenues dans le paquet TCP/IP sont sécurisées (et cryptées si le type de tunnel est ESP). Le paquet IP (en-tête et charge utile) est incorporé dans une autre charge utile IP, et un nouvel en-tête est appliqué puis envoyé via le tunnel IPSec. L'adresse IP source contenue dans le nouvel en-tête est celle de l'homologue VPN local et l'adresse IP de destination est celle de l'homologue VPN à l'autre extrémité du tunnel. Lorsque le paquet atteint l'homologue VPN distant (le pare-feu à l'autre extrémité du tunnel), l'en-tête externe est supprimé et le paquet d'origine est envoyé à sa destination.

Les homologues doivent d'abord être authentifiés afin de pouvoir configurer le tunnel VPN. Une fois authentifiés, les homologues négocient la méthode de cryptage et les algorithmes pour sécuriser la communication. Le processus Internet Key Exchange (échange de clés Internet ; IKE) permet d'authentifier les homologues VPN, et les associations de sécurité IPSec sont définies à chaque extrémité du tunnel pour sécuriser la communication VPN. IKE utilise des certificats numériques ou des clés prépartagées, et des clés Diffie Hellman pour configurer les associations de sécurité pour le tunnel IPSec. Les associations de sécurité spécifient tous les paramètres requis pour la transmission sécurisée [notamment le Security Parameter Index (index de paramètre de sécurité ; SPI), le protocole de sécurité, les clés cryptographiques et l'adresse IP de destination], le cryptage, l'authentification des données, l'intégrité des données et l'authentification du point de terminaison.

La figure suivante illustre un tunnel VPN entre deux sites. Lorsqu'un client sécurisé par l'homologue VPN A nécessite le contenu d'un serveur se trouvant sur l'autre site, l'homologue VPN A initie une requête de connexion auprès de l'homologue VPN B. Si la politique de sécurité autorise la connexion, l'homologue VPN A utilise les paramètres du profil crypto IKE (IKE de phase 1) pour établir une connexion sécurisée et authentifier l'homologue VPN B. Ensuite, l'homologue VPN A établit le tunnel VPN à l'aide du profil crypto IPSec, qui définit les paramètres IKE de phase 2 pour permettre le transfert sécurisé des données entre les deux sites.

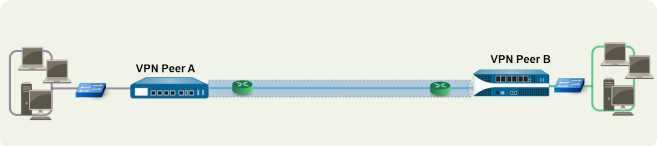



**Figure 8: VPN de site à site**

# Concepts du VPN de site à site

Une connexion VPN fournit un accès sécurisé aux informations entre deux sites ou plus. Afin de fournir un accès sécurisé aux ressources et une connexion fiable, une connexion VPN nécessite les composants suivants :

- Passerelle IKE
- en texte clair
- Surveillance du tunnel
- Internet Key Exchange (échange de clés Internet ; IKE) pour VPN
- IKEv2

## Passerelle IKE

Des pare-feu Palo Alto Networks ou un pare-feu et un autre périphérique de sécurité qui établissent et mettent fin à des connexions VPN entre deux réseaux sont appelés des passerelles IKE. Pour configurer le tunnel VPN et envoyer le trafic entre les passerelles IKE, chaque homologue doit disposer d'une adresse IP (statique ou dynamique) ou d'un FQDN. Les homologues VPN utilisent des clés prépartagées ou des certificats pour s'authentifier mutuellement.

Les homologues doivent également négocier le mode (Principal ou Agressif) de configuration du tunnel VPN et de la durée de vie de la SA dans la phase 1 du protocole IKE. Le mode Principal protège l'identité des homologues et est davantage sécurisé, car plus de paquets sont échangés lors de la configuration du tunnel. Le mode Principal est recommandé pour la négociation IKE si les deux homologues la prennent en charge. Le mode Agressif utilise moins de paquets pour configurer le tunnel VPN et est donc plus rapide mais moins sécurisé.

Pour plus d'informations sur la configuration, reportez-vous à la section Configuration d'une passerelle IKE.

## en texte clair

Afin de pouvoir configurer un tunnel VPN, l'interface de couche 3 à chaque extrémité doit disposer d'une interface de ***tunnel*** à laquelle le pare-feu doit se connecter pour établir un tunnel VPN. Une interface de tunnel est une interface (virtuelle) logique utilisée pour acheminer le trafic entre deux terminaux. Si vous configurez des ID de proxy, l'ID de proxy est compté pour la capacité de tunnel IPsec.

L'interface de tunnel doit appartenir à une zone de sécurité pour pouvoir appliquer la politique et être affectée à un routeur virtuel afin d'utiliser l'infrastructure de routage existante. Assurez-vous que l'interface de tunnel et l'interface physique sont affectées au même routeur virtuel pour que le pare-feu puisse effectuer une recherche d'itinéraire et déterminer le tunnel approprié à utiliser.

Généralement, l'interface de couche 3 à laquelle l'interface de tunnel est associée appartient à une zone externe, par exemple, la zone non approuvée. Bien que l'interface de tunnel puisse être dans la même zone de sécurité que l'interface physique, pour renforcer la sécurité et améliorer la visibilité, vous pouvez créer une zone distincte pour l'interface de tunnel. Si vous créez une zone distincte pour l'interface de tunnel, par exemple, une zone VPN, vous devrez créer des politiques de sécurité pour permettre au trafic de circuler entre la zone VPN et la zone approuvée.

Pour acheminer le trafic entre les sites, une interface de tunnel n'a pas besoin d'adresse IP. Une adresse IP est uniquement requise si vous souhaitez activer la surveillance des tunnels ou si vous utilisez un protocole de routage dynamique pour acheminer le trafic vers le tunnel. Lors du routage dynamique, l'adresse IP du tunnel sert d'adresse IP de saut suivant pour acheminer le trafic vers le tunnel VPN.

Si vous configurez le pare-feu Palo Alto Networks avec un homologue VPN qui utilise un VPN basé sur une politique, vous devez configurer un ID de proxy local et distant lors de la configuration du tunnel IPSec. Chaque homologue compare les ID de proxy configurés avec le contenu réel du paquet reçu afin de permettre la réussite d'une négociation IKE de phase 2. Si plusieurs tunnels sont requis, configurez des ID de proxy uniques pour chaque interface de tunnel ; une interface de tunnel peut disposer de 250 ID de proxy maximum. Chaque ID de proxy est pris en compte dans le calcul de la capacité du tunnel VPN IPSec du pare-feu, et la capacité du tunnel varie en fonction du modèle de pare-feu.

Pour plus d'informations sur la configuration, reportez-vous à la section Configuration d'un tunnel IPSec.

## Surveillance du tunnel

Pour un tunnel VPN, vous pouvez vérifier la connexion à une adresse IP de destination via le tunnel. Le profil de surveillance réseau sur le pare-feu vous permet de vérifier la connexion (à l'aide d'ICMP) à une adresse IP de destination ou un saut suivant à un intervalle d'interrogation donné, et de spécifier une action en cas d'échec de l'accès à l'adresse IP surveillée.

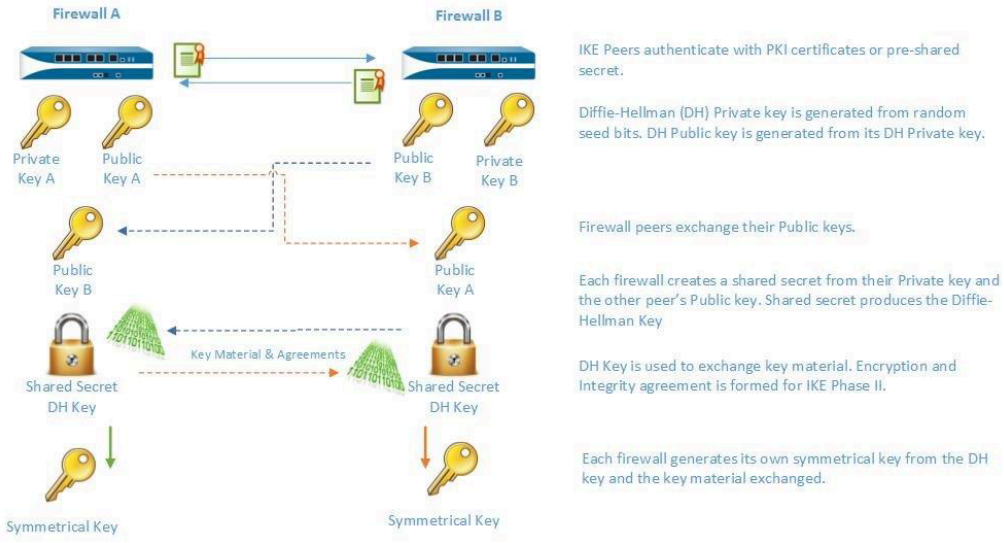
Si l'adresse IP de destination est inaccessible, configurez le pare-feu pour attendre la récupération du tunnel ou configurez le basculement automatique vers un autre tunnel. Dans tous les cas, le pare-feu génère un journal système qui vous alerte d'une défaillance du tunnel et renégocie les clés IPSec pour accélérer la récupération.

Pour plus d'informations sur la configuration, reportez-vous à la section Configuration de la surveillance des tunnels.

## Internet Key Exchange (échange de clés Internet ; IKE) pour VPN

Le processus IKE permet aux homologues VPN à chaque extrémité du tunnel de crypter et de décrypter à l'aide de clés mutuellement convenues ou d'un certificat et d'une méthode de cryptage. Ce processus se déroule en deux phases : IKE de phase 1 et IKE de phase 2. Chacune de ces phases utilise des clés et des algorithmes de cryptage qui sont définis à l'aide de profils cryptographiques (profil crypto IKE et profil crypto IPSec) ; le résultat de la négociation IKE est une Security Association (association de sécurité - SA). Une SA est un ensemble d'algorithmes et de clés mutuellement convenues qui sont utilisés par les deux homologues VPN pour autoriser la circulation des données via le tunnel VPN. L'illustration suivante décrit le processus d'échange de clés pour la configuration du tunnel VPN :




## Phase 1 du protocole IKE

Dans cette phase, les pare-feu utilisent les paramètres définis dans la configuration de passerelle IKE et le profil crypto IKE pour s'authentifier mutuellement et configurer un canal de contrôle sécurisé. Cette phase prend en charge l'utilisation de clés prépartagées ou de certificats numériques (qui utilisent l'infrastructure à clé publique [PKI]) pour l'authentification mutuelle des homologues VPN. Les clés prépartagées sont une solution simple pour sécuriser des réseaux plus petits, car elles ne nécessitent pas la prise en charge d'une infrastructure PKI. Les certificats numériques peuvent être plus pratiques pour les réseaux plus grands ou les implémentations qui nécessitent une sécurité d'authentification renforcée.

Lors de l'utilisation de certificats, assurez-vous que l'autorité de certification qui émet le certificat est approuvée par les deux homologues de passerelle et que le nombre maximum de certificats dans la chaîne de certificats est de 5. Lorsque la fragmentation IKE est activée, le pare-feu peut réassembler les messages IKE avec un nombre maximum de 5 certificats dans la chaîne de certificats et établir un tunnel VPN.

Le profil crypto IKE définit les options suivantes qui sont utilisées dans la négociation de SA IKE :

- Le groupe Diffie-Hellman (DH) pour la génération de clés symétriques pour IKE.

  L'algorithme Diffie-Hellman utilise la clé privée d'une partie et la clé publique de l'autre pour créer un secret partagé, qui est une clé cryptée partagée par les deux homologues du tunnel PN. Les groupes DH pris en charge sur le pare-feu sont les suivants : Groupe 1 : 768 bits, Groupe 2 : 1 024 bits (valeur par défaut), Groupe 5 : 1 536 bits ; Groupe 14 : 2 048 bits, Groupe 19 : groupe de courbe elliptique 256 bits et Groupe 20 : groupe de courbe elliptique 384 bits.
- Algorithmes d'authentification : sha1, sha 256, sha 384, sha 512 ou md5.
- Algorithmes de chiffrement : aes-256-gcm, aes-128-gcm, 3des, aes-128-cbc, aes-192-cbc, aes-256-cbc ou des

## Phase 2 du protocole IKE

Une fois le tunnel sécurisé et authentifié, dans la phase 2, le canal est davantage sécurisé pour le transfert de données entre les réseaux. La phase 2 utilise les clés qui ont été établies à la phase 1 du

processus et le profil crypto IPSec, qui définit les clés et les protocoles IPSec utilisés pour la SA IKE de phase 2.

IPSec utilise les protocoles suivants pour permettre la communication sécurisée :

- Encapsulating Security Payload (encapsulation de la charge utile de sécurité - ESP) : vous permet de crypter l'ensemble du paquet IP, d'authentifier la source et de vérifier l'intégrité des données. Bien qu'ESP nécessite le cryptage et l'authentification du paquet, vous pouvez choisir le cryptage seul (ou l'authentification seule) en sélectionnant Nul en regard de l'option de cryptage (ou d'authentification) ; l'utilisation du cryptage sans l'authentification n'est pas recommandée.
- Authentication Header (en-tête d'authentification - AH) : vous permet d'authentifier la source du paquet et de vérifier l'intégrité des données. AH ne crypte pas la charge utile de données et n'est pas adapté aux déploiements où la confidentialité des données est importante. AH est communément utilisé lorsque l'objectif principal est la vérification de la légitimité de l'homologue et lorsque la confidentialité des données n'est pas requise.

**Table 5: Algorithmes pris en charge pour le cryptage et l'authentification IPSec**

| ESP | AH |
|---|---|
| Options d'échange Diffie-Hellman (DH) prises en charge | |
| • Groupe 1 : 768 bits<br>• Groupe 2 : 1 024 bits (valeur par défaut)<br>• Groupe 5 : 1536 bits<br>• Groupe 14 : 2 048 bits<br>• Groupe 19 : groupe de courbe elliptique 256 bits<br>• Groupe 20 : groupe de courbe elliptique 384 bits<br>• PFS désactivé : par défaut, le secret de transfert idéal (PFS) est activé, ce qui signifie qu'une nouvelle clé DH est générée dans la phase 2 du protocole IKE à l'aide de l'un des groupes indiqués ci-dessus. Cette clé est indépendante des clés échangées dans la phase 1 du protocole IKE et offre une meilleure sécurité du transfert de données. Si vous sélectionnez PFS désactivé, la clé DH créée à la phase 1 n'est pas renouvelée et une seule clé est utilisée pour les négociations SA IPSec. Les deux homologues VPN doivent être activés ou désactivés pour l'option PFS. | |
| Algorithmes de cryptage pris en charge | |
| • 3des | Triple Data Encryption Standard (norme de cryptage de données triple, 3DES) avec une puissance de sécurité de 112 bits |
| • aes-128-cbc | Advanced Encryption Standard (norme de cryptage avancée - AES) utilisant le chaînage de bloc de cryptage (CBC) avec une puissance de sécurité de 128 bits |
| • aes-192-cbc | AES utilisant CBC avec une puissance de sécurité de 192 bits |

| ESP | AH |
|---|---|
| • aes-256-cbc | AES utilisant CBC avec une puissance de sécurité de 256 bits |
| • aes-128-ccm | AES utilisant Counter with CBC-MAC (compteur avec CBC-MAC - CCM) avec une puissance de sécurité de 128 bits |
| • aes-128-gcm | AES utilisant Galois/Counter Mode (mode Galois/Compteur - GCM) avec une puissance de sécurité de 128 bits |
| • aes-256-gcm | AES utilisant GCM avec une puissance de sécurité de 256 bits |
| • des | Data Encryption Standard (norme de cryptage de données ; DES) avec une puissance de sécurité de 56 bits |
| Algorithmes d'authentification pris en charge | |
| • md5 | • md5 |
| • sha 1 | • sha 1 |
| • sha 256 | • sha 256 |
| • sha 384 | • sha 384 |
| • SHA512 | • sha512 |

### Méthodes de sécurisation des tunnels VPN IPSec (phase 2 du protocole IKE)

Les tunnels VPN IPSec peuvent être sécurisés à l'aide de clés manuelles ou automatiques. De plus, les options de configuration IKE incluent le groupe Diffie-Hellman pour l'accord de clés et/ou un algorithme de cryptage et un hachage pour l'authentification des messages.

- **Clé manuelle** : une clé manuelle est généralement utilisée si le pare-feu Palo Alto Networks établit un tunnel VPN avec un périphérique d'ancienne génération, ou si vous souhaitez réduire les frais de génération de clés de session. Lors de l'utilisation de clés manuelles, la même clé doit être configurée sur les deux homologues.

  Les clés manuelles ne sont pas recommandées pour l'établissement d'un tunnel VPN, car les clés de session peuvent être compromises lors de la transmission des informations de clé entre les homologues ; si les clés sont compromises, le transfert de données n'est plus sécurisé.
- **Clé automatique** : une clé automatique vous permet de générer automatiquement des clés pour la configuration et la gestion du tunnel IPSec en fonction des algorithmes définis dans le profil crypto IPSec.

## IKEv2

Une passerelle VPN IPSec utilise IKEv1 ou IKEv2 pour négocier l'association de sécurité (SA) IKE et le tunnel IPSec. IKEv2 est défini dans RFC 5996.

Contrairement à IKEv1, qui utilise une SA de phase 1 et une SA de phase 2, IKEv2 utilise une SA enfant pour l'encapsulation de la charge utile de sécurité (ESP) ou l'en-tête d'authentification (AH), qui est configuré avec une SA IKE.

NAT traversal (NAT-T) doit être activé sur les deux passerelles si NAT se produit sur un périphérique situé entre les deux passerelles. Une passerelle peut uniquement voir l'adresse IP publique (globalement routable) du périphérique NAT.

IKEv2 offre les avantages suivants par rapport à IKEv1 :

- Les terminaux du tunnel échangent moins de messages pour établir un tunnel. IKEv2 utilise quatre messages; IKEv1 en utilise neuf messages (en mode Principal) ou six (en mode Agressif).
- La fonctionnalité NAT-T intégrée améliore la compatibilité entre les fournisseurs.
- La vérification de l'état intégrée rétablit automatiquement un tunnel s'il est arrêté. La vérification de l'activité remplace la détection des homologues inactifs utilisée dans IKEv1.
- Prend en charge des sélecteurs de trafic (un par échange). Les sélecteurs de trafic sont utilisés dans les négociations IKE pour contrôler le trafic pouvant accéder au tunnel.
- Prend en charge l'échange de certificat Hachage et URL pour réduire la fragmentation.
- Protection contre les attaques DoS avec une meilleure validation de l'homologue. Un nombre excessif de SA demi-ouvertes peut déclencher une validation du cookie.

Avant de configurer IKEv2, vous devez connaître les concepts suivants :

- Vérification de l'activité
- Seuil d'activation du cookie et validation du cookie stricte
- Sélecteurs de trafic
- Échange de certificat Hachage et URL
- Durée de vie de la clé et intervalle de réauthentification SA

Après la Configuration d'une passerelle IKE, si vous avez choisi IKEv2, effectuez les tâches facultatives suivantes liées à IKEv2 si nécessaire dans votre environnement :

- Exportation d'un certificat pour l'accès d'un homologue à l'aide de Hachage et URL
- Importation d'un certificat pour l'authentification de passerelle IKEv2
- Modification de la durée de vie de la clé ou de l'intervalle d'authentification pour IKEv2
- Modification du seuil d'activation du cookie pour IKEv2
- Configuration des sélecteurs de trafic IKEv2

## Vérification de l'activité

La vérification de l'activité pour IKEv2 est identique à la Dead Peer Detection (détection des homologues inactifs ; DPD), qui est utilisée dans IKEv1 pour déterminée si un homologue est toujours disponible.

Dans IKEv2, la vérification de l'activité est possible via la transmission de tout paquet IKEv2 ou un message informatif vide envoyé par la passerelle à l'homologue à un intervalle pouvant être configuré (cinq secondes par défaut). Si nécessaire, l'expéditeur tente de le retransmettre jusqu'à dix fois. S'il ne reçoit pas de réponse, l'expéditeur ferme et supprime les IKE_SA et CHILD_SA correspondants. L'expéditeur commence à envoyer un autre message IKE_SA_INIT.

## Seuil d'activation du cookie et validation du cookie stricte

La validation du cookie est toujours activée pour IKEv2 ; elle vous protège contre les attaques DoS SA demi-ouvertes. Vous pouvez configurer le nombre limite global de SA demi-ouvertes qui déclenchera une validation du cookie. Vous pouvez également configurer des passerelles IKE pour appliquer la validation du cookie pour chaque nouvelle SA IKEv2.

- Le **Cookie Activation Threshold (Seuil d'activation du cookie)** est un paramètre de session VPN global qui limite le nombre de SA demi-ouvertes simultanées (par défaut, 500). Lorsque le nombre de SA IKE demi-ouvertes est supérieur au **Cookie Activation Threshold (Seuil d'activation du cookie)**, le répondeur demande un cookie, et l'initiateur doit répondre par un IKE_SA_INIT contenant un cookie pour valider la connexion. Si la validation du cookie réussit, une autre SA peut être ouverte. Une valeur de 0 signifie que la validation du cookie est toujours activée.

  Le répondeur ne garde pas l'état d'initiateur, et ne procède pas à un échange de clé Diffie-Hellman, tant que l'initiateur n'a pas renvoyé le cookie. La validation du cookie IKEv2 atténue une attaque DoS qui tenterait de maintenir plusieurs connexions demi-ouvertes.

  Le **Cookie Activation Threshold (Seuil d'activation du cookie)** doit être inférieur au paramètre **Maximum Half Opened SA (Nombre max de SA demi-ouvertes)**. En cas de Modification du seuil d'activation du cookie pour IKEv2 sur un nombre très élevé (65534 par exemple) et que le paramètre **Maximum Half Opened SA (Nombre maximum de SA demi-ouvertes)** est toujours défini sur la valeur par défaut de 65535, la validation du cookie est désactivée.
- Vous pouvez activer l'option **Strict Cookie Validation (Validation du cookie stricte)** si vous souhaitez qu'une validation du cookie soit effectuée pour chaque nouvelle SA IKEv2 reçue par une passerelle, quel que soit le seuil global. La **Strict Cookie Validation (Validation du cookie stricte)** n'affecte que la passerelle IKE configurée et est désactivée par défaut. Lorsque la **Strict Cookie Validation (Validation du cookie stricte)** est désactivée, le système utilise le **Cookie Activation Threshold (Seuil d'activation du cookie)** pour déterminer si un cookie est nécessaire ou non.

## Sélecteurs de trafic

Dans IKEv1, un pare-feu comprenant un VPN basé sur un itinéraire doit utiliser un ID de proxy local et distant pour configurer un tunnel IPSec. Chaque homologue compare ses ID de proxy avec ceux qu'il a reçu dans le paquet afin de négocier avec succès IKE phase 2. IKE phase 2 concerne la négociation des SA pour configurer un tunnel IPSec. (Pour plus d'informations sur les ID de proxy, reportez-vous à la section en texte clair.)

Dans IKEv2, une Configuration des sélecteurs de trafic IKEv2 est possible, qui sont des composants de trafic réseau utilisés pendant une négociation IKE. Les sélecteurs de trafic sont utilisés pendant CHILD_SA (création de tunnel) phase 2 pour configurer le tunnel et déterminer le trafic autorisé dans le tunnel. Les deux homologues de passerelle IKE doivent négocier et s'accorder sur leurs sélecteurs de trafic ; sinon, un côté réduit sa plage d'adresses pour parvenir à un accord. Une connexion IKE peut comporter plusieurs tunnels ; par exemple, vous pouvez affecter différents tunnels à chaque service pour isoler son trafic. La séparation du trafic permet également de mettre en œuvre des fonctionnalités telles que QoS.

Les sélecteurs de trafic IPv4 et IPv6 sont les suivants :

- **Adresse IP source** : préfixe réseau, plage d'adresses, hôte spécifique ou caractère générique.
- **Adresse IP de destination** : préfixe réseau, plage d'adresses, hôte spécifique ou caractère générique.

- **Protocole** : protocole de transport, TCP ou UDP par exemple.
- **Port source** : port d'origine du paquet.
- **Port de destination** : port auquel le paquet est destiné.

Pendant une négociation IKE, plusieurs sélecteurs de trafic sont possibles pour différents réseaux et protocoles. Par exemple, l'initiateur peut indiquer qu'il souhaite envoyer des paquets TCP de l'adresse 172.168.0.0/16, via le tunnel, à son homologue de destination 198.5.0.0/16. Il souhaite également envoyer des paquets UDP de l'adresse 172.17.0.0/16, via le même tunnel, à la même passerelle de destination 0.0.0.0 (n'importe quel réseau). La passerelle homologue doit accepter ces sélecteurs de trafic pour pouvoir déterminer à quoi s'attendre.

Il est possible qu'une passerelle commence une négociation à l'aide d'un sélecteur de trafic avec une adresse IP plus spécifique que l'adresse IP de l'autre passerelle.

- Par exemple, la passerelle A propose une adresse IP source 172.16.0.0/16 et une adresse IP de destination 192.16.0.0/16. Cependant, la passerelle B est configurée avec l'adresse IP source 0.0.0.0 (n'importe quelle source) et l'adresse IP de destination 0.0.0.0 (n'importe quelle destination). La passerelle B réduit donc son adresse IP source à 192.16.0.0/16 et son adresse IP de destination à 172.16.0.0/16. Ainsi, la réduction permet d'inclure les adresses de la passerelle A et les sélecteurs de trafic des deux passerelles correspondent.
- Si la passerelle B (configurée avec l'adresse IP source 0.0.0.0) est l'initiateur et non le répondeur, la passerelle A répondra avec son adresse IP plus spécifique, et la passerelle B réduira ses adresses pour parvenir à un accord.

## Échange de certificat Hachage et URL

IKEv2 prend en charge l'échange de certificat Hachage et URL, qui est utilisé pendant une négociation IKEv2 d'une SA. Vous stockez le certificat sur un serveur HTTP, qui est spécifié par une URL. L'homologue extrait le certificat du serveur à la réception de l'URL vers le serveur. Le hachage permet de vérifier si le contenu du certificat est valide ou non. Les deux homologues échangent ainsi des certificats avec la CA HTTP plutôt qu'entre eux.

La partie hachage de Hachage et URL réduit la taille du message et l'échange de certificat Hachage et URL permet donc de réduire le risque de fragmentation des paquets pendant une négociation IKE. L'homologue reçoit le certificat et le hachage attendu, ce qui signifie que la phase 1 du protocole IKE a validé l'homologue. La réduction de la fragmentation permet de vous protéger contre les attaques DoS.

Vous pouvez activer l'échange de certificat Hachage et URL pendant la configuration d'une passerelle IKE en sélectionnant **HTTP Certificate Exchange (Échange de certificat HTTP)** et en saisissant la **Certificate URL (URL du certificat)**. L'homologue doit également utiliser l'échange de certificat Hachage et URL pour que l'échange réussisse. Si l'homologue ne peut pas utiliser la méthode Hachage et URL, les certificats X.509 sont échangés comme dans IKEv1.

Si vous activez l'échange de certificat Hachage et URL, vous devez exporter votre certificat vers le serveur de certificats (s'il ne s'y trouve pas déjà). Lorsque vous exportez le certificat, le format du fichier doit être **Binary Encoded Certificate (DER) (Certificat codé en binaire (DER))**. Reportez-vous à la section Exportation d'un certificat pour l'accès d'un homologue à l'aide de Hachage et URL.

## Durée de vie de la clé et intervalle de réauthentification SA

Dans IKEv2, deux valeurs de profil crypto IKE, **Key Lifetime (Durée de vie de la clé)** et **IKEv2 Authentication Multiple (Multiple d'authentification IKEv2)**, contrôlent l'établissement de SA

IKEv2. La durée de vie de la clé correspond à la durée de validité d'une clé SA IKE négociée. Avant que la durée de vie de la clé expire, la clé de la SA doit être changée sinon, lors de l'expiration, la SA doit démarrer un nouveau changement de clé de SA IKEv2. La valeur par défaut est 8 heures.

L'intervalle de réauthentification est obtenu en multipliant la **Key Lifetime (Durée de vie de la clé)** par le **IKEv2 Authentication Multiple (Multiple d'authentification IKEv2)**. Le multiple d'authentification par défaut est 0, ce qui désactive la fonction de réauthentification.

La plage des multiples d'authentification est comprise entre 0 et 50. Par exemple, si vous envisagiez de configurer un multiple d'authentification de 20, le système effectuerait une réauthentification toutes les 20 nouvelles clés, à savoir toutes les 160 heures. Cela signifie que la passerelle pourrait créer une SA enfant de 160 heures avant qu'elle ne doive se réauthentifier auprès d'IKE pour créer la toute nouvelle SA IKE.

Dans IKEv2, les passerelles initiateur et répondeur disposent de valeurs de durée de vie de la clé propres, et la passerelle présentant la durée de vie de la clé la plus courte est celle qui demandera la nouvelle SA.

# Configuration d'un VPN site à site

Pour configurer un VPN site à site :

- Vérifiez que vos interfaces Ethernet, vos routeurs virtuels et vos zones sont correctement configurés. Pour plus d'informations, reportez-vous à la section Configuration des interfaces et des zones.
- Créez vos interfaces de tunnel. Dans l'idéal, placez les interfaces de tunnel dans une zone distincte, afin que le trafic par tunnel puisse utiliser des politiques différentes.
- Configurez des itinéraires statiques ou affectez des protocoles de routage pour rediriger le trafic vers les tunnels VPN. Pour prendre en charge le routage dynamique (les protocoles OSPF, BGP et RIP sont pris en charge), vous devez affecter une adresse IP à l'interface de tunnel.
- Définissez des passerelles IKE pour établir la communication entre les homologues à chaque extrémité du tunnel VPN ; définissez également le profil cryptographique qui spécifie les protocoles et les algorithmes d'identification, d'authentification et de cryptage à utiliser pour la configuration de tunnels VPN dans la phase 1 du protocole IKEv1. Consultez les sections Configuration d'une passerelle IKE et Définition de profils crypto IKE.
- Configurez les paramètres requis pour établir la connexion IPSec pour le transfert de données via le tunnel VPN ; reportez-vous à la section Configuration d'un tunnel IPSec. Pour la phase 2 du protocole IKEv1, consultez la section Définition de profils crypto IPSec.
- (Facultatif) Indiquez la manière dont le pare-feu surveillera les tunnels IPSec. Reportez-vous à la section Configuration de la surveillance des tunnels.
- Définissez des politiques de sécurité pour filtrer et inspecter le trafic.

***Si une règle de refus figure à la fin de la base de règles de sécurité, le trafic intra-zone est bloqué, sauf autorisation contraire. Les règles pour autoriser des applications IKE et IPSec doivent être explicitement incluses au-dessus de la règle de refus.***

***Si votre trafic VPN traverse (mais qu'il ne provient pas ni n'ayant comme destination) un pare feu PA-7000 Series ou PA-5200 Series, configurez des règles de politique de sécurité bidirectionnelles pour permettre le trafic ESP ou AH dans les deux directions.***

Une fois ces tâches terminées, le tunnel est prêt à être utilisé. Le trafic destiné aux zones/adresses définies dans la politique est automatiquement acheminé en fonction de l'itinéraire de destination de la table de routage et traité en tant que trafic VPN. Pour obtenir quelques exemples de VPN de site à site, reportez-vous à la section Configurations rapides de VPN site à site.

À des fins de dépannage, une Activation/désactivation, actualisation ou redémarrage d'une passerelle IKE ou d'un tunnel IPSec est possible.

## Configuration d'une passerelle IKE

Pour configurer un tunnel VPN, les passerelles ou les homologues VPN doivent s'authentifier mutuellement à l'aide de clés prépartagées ou de certificats numériques et établir un canal sécurisé dans lequel négocier l'association de sécurité SA IPSec qui sera utilisée pour sécuriser le trafic entre les homologues de chaque côté.

**STEP 1 |** Définissez la passerelle IKE.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Gateways (Passerelles IKE)**, **Add (Ajoutez)** une passerelle, puis saisissez le **Name (Nom)** de la passerelle (onglet **General (Général)**).
2. Définissez la **Version** sur **IKEv1 only mode (Mode IKEv1 uniquement)**, **IKEv2 only mode (Mode IKEv2 uniquement)** ou **IKEv2 preferred mode (Mode IKEv2 préféré)**. La passerelle IKE commence sa négociation avec son homologue dans le mode que vous spécifiez ici. Si vous sélectionnez **IKEv2 preferred mode (Mode IKEv2 préféré)**, les deux homologues utiliseront IKEv2 si l'homologue distant le prend en charge ; sinon, ils utiliseront IKEv1.

   La **Version** que vous sélectionnez détermine également les options que vous pouvez configurer dans l'onglet **Advanced Options (Options avancées)**.

**STEP 2 |** Établissez le terminal local du tunnel (passerelle).

1. Sélectionnez le **Address Type (Type d'adresse)** : **IPv4** ou **IPv6**.
2. Sélectionnez l'**Interface** sortante physique sur le pare-feu sur laquelle se trouve la passerelle locale.
3. Dans la liste **Local IP Address (Adresse IP locale)**, sélectionnez l'adresse IP qui sera utilisée comme terminal de la connexion VPN. Il s'agit de l'interface externe qui dispose d'une adresse IP pouvant être acheminée en public sur le pare-feu.

**STEP 3 |** Établissez l'homologue à l'autre extrémité du tunnel (passerelle).

Sous **Peer IP Address Type (Type d'adresse IP de l'homologue)**, sélectionnez l'un des paramètres suivants et saisissez les informations correspondantes de l'homologue :

- **IP** : saisissez une **Peer Address (Adresse de l'homologue)** qui est une adresse IPv4 ou IPv6 ou saisissez un objet d'adresse qui est une adresse IPv4 ou IPv6.
- **FQDN** : saisissez une **Peer Address (Adresse de l'homologue)** qui est une chaîne de FQDN ou un objet d'adresse utilisant une chaîne de FQDN. Si le FQDN ou l'objet d'adresse FQDN se résout en plus d'une adresse IP, le pare-feu choisit l'adresse préférée dans l'ensemble d'adresses qui correspondent au Type d'adresse (IPv4 ou IPv6) de la passerelle IKE, comme suit :
  - Si aucune Security Association (association de sécurité ; SA) IKA n'est négociée, l'adresse préférée correspond à l'adresse IP qui possède la plus faible valeur.
  - Si la passerelle IKE utilise une adresse qui figure dans l'ensemble d'adresses renvoyées, le pare-feu sélectionne cette adresse (qu'il s'agisse de l'adresse qui possède la plus faible valeur de la liste ou non).
  - Si la passerelle IKE utilise une adresse qui ne figure pas dans l'ensemble d'adresses renvoyées, le pare-feu sélectionne une nouvelle adresse et il s'agit de l'adresse qui possède la plus faible valeur de la liste.
- **Dynamic (Dynamique)** : sélectionnez **Dynamic (Dynamique)** si l'adresse IP ou le FQDN de l'homologue est inconnu afin que l'homologue puisse initier la négociation.

*L'utilisation d'un FQDN ou d'un objet d'adresse FQDN réduit les problèmes d'environnements où l'homologue est soumis aux changements des adresses IP dynamiques (ce qui autrement vous obligerez à reconfigurer l'adresse de cette passerelle IKE homologue).*

**STEP 4 |** Indiquez comment authentifier l'homologue.

Sélectionnez la méthode d'**Authentication (Authentification)** : **Pre-Shared Key (Clé prépartagée)** ou **Certificate (Certificat)**. Si vous choisissez une clé prépartagée, passez à l'étape suivante. Si vous choisissez un certificat, passez à l'étape 6, Configuration d'une authentification basée sur un certificat.

**STEP 5 |** Configurez une clé prépartagée.

1. Saisissez une **Pre-shared Key (Clé prépartagée)**, qui est la clé de sécurité à utiliser pour l'authentification dans le tunnel. Saisissez à nouveau la valeur pour **Confirm Pre-shared Key (Confirmer la clé prépartagée)**. Utilisez un maximum de 255 caractères ASCII ou non ASCII.

   *Générez une clé difficile à décoder par des attaques par dictionnaire ; utilisez un générateur de clés prépartagées, si nécessaire.*

2. Sous **Local Identification (Identification locale)**, sélectionnez l'un des types suivants et saisissez une valeur que vous déterminez : **FQDN (hostname) (FQDN (nom d'hôte))**, **IP address (Adresse IP)**, **KEYID (binary format ID string in HEX) (KEYID (chaîne d'ID au format binaire hexadécimal))** et **User FQDN (email address) (FQDN de l'utilisateur (adresse e-mail))**. L'identification locale définit le format et l'identification de la passerelle locale. Si vous ne spécifiez aucune valeur, l'adresse IP locale est utilisée comme valeur d'Identification locale.
3. Sous **Peer Identification (Identification de l'homologue)**, sélectionnez l'un des types suivants et saisissez une valeur que vous déterminez : **FQDN (hostname) (FQDN (nom d'hôte))**, **IP address (Adresse IP)**, **KEYID (binary format ID string in HEX) (KEYID (chaîne d'ID au format binaire hexadécimal))** et **User FQDN (email address) (FQDN de l'utilisateur (adresse e-mail))**. L'identification de l'homologue définit le format et l'identification de la passerelle homologue. Si vous ne spécifiez aucune valeur, l'adresse IP de l'homologue est utilisée comme valeur d'Identification de l'homologue.
4. Passez à l'étape 7 (Configurez des options avancées pour la passerelle).

**STEP 6 |** Configurez l'authentification basée sur les certificats.

Effectuez les étapes restantes de cette procédure si vous avez sélectionné **Certificate (Certificat)** comme méthode d'authentification de la passerelle homologue à l'extrémité opposée du tunnel.

1. Sélectionnez un **Local Certificate (Certificat local)** se trouvant déjà sur le pare-feu, **Import (Importez)** un certificat ou **Generate (Générez)** un nouveau certificat.
   - Pour **Import (Importer)** un nouveau certificat, procédez d'abord à l'Importation d'un certificat pour l'authentification de passerelle IKEv2. Revenez ensuite à cette tâche.
   - Pour **Generate (Générer)** un nouveau certificat, procédez d'abord à la Génération d'un certificat sur le pare-feu. Revenez ensuite à cette tâche.
2. (Facultatif) Activez (sélectionnez) le **HTTP Certificate Exchange (Échange des certificats HTTP)** pour configurer le hachage et l'URL (IKEv2 uniquement). Pour un échange de certificat HTTP, saisissez l'**Certificate URL (URL du certificat)**. Pour plus d'informations, reportez-vous à la section Échange de certificat Hachage et URL.
3. Sélectionnez le type de **Local Identification (Identification locale)** (**Distinguished Name (Subject), FQDN (hostname) (Nom unique (objet)), FQDN (nom d'hôte))**, **IP address (Adresse IP)** ou **User FQDN (email address) (FQDN de l'utilisateur (adresse e-mail))**), puis

saisissez la valeur. L'identification locale définit le format et l'identification de la passerelle locale.

4. Sélectionnez le type de **Peer Identification (Identification de l'homologue)** (**Distinguished Name (Subject), FQDN (hostname) (Nom unique (objet)), FQDN (nom d'hôte))**, **IP address (Adresse IP)** ou **User FQDN (email address) (FQDN de l'utilisateur (adresse e-mail))**), puis saisissez la valeur. L'identification de l'homologue définit le format et l'identification de la passerelle homologue.
5. Précisez le type de **Peer ID Check (Vérification de l'ID d'homologue)** :
   - **Exact** : vous assure que le paramètre local et la charge utile ID IKE de l'homologue correspondent parfaitement.
   - **Wildcard (Caractère générique)** : permet à l'identification de l'homologue de correspondre tant que chaque caractère situé avant le caractère générique (*) correspond. Les caractères situés après le caractère générique ne doivent pas nécessairement correspondre.
6. (Facultatif) **Permit peer identification and certificate payload identification mismatch (Autorisez une non-correspondance de l'identification de l'homologue et de l'identification des données utiles du certificat)** pour autoriser une SA IKE réussie même si l'identification de l'homologue ne correspond pas à l'identification de l'homologue dans le certificat.
7. Choisissez un **Certificate Profile (Profil de certificat)**. Un profil de certificat contient des informations sur comment authentifier la passerelle homologue.
8. (Facultatif) **Enable strict validation of peer's extended key use (Activez la validation stricte de l'utilisation de la clé étendue de l'homologue)** pour contrôler strictement l'utilisation de la clé.

**STEP 7 |** Configurez des options avancées pour la passerelle.

1. (Facultatif) **Enable Passive Mode (Activez le mode passif)** dans les Options courantes (**Advanced Options (Options avancées)**) pour indiquer que le pare-feu ne fait que répondre aux requêtes de connexion IKE et qu'il ne les initie jamais.
2. Si vous disposez d'un périphérique qui exécute NAT entre les passerelles, **Enable NAT Traversal (Activez la Traversée NAT)** pour utiliser l'encapsulation UDP sur les protocoles IKE et UDP, ce qui leur permet de passer par des périphériques NAT intermédiaires.
3. Si vous avez sélectionné **IKEv1 only mode (Mode IKEv1 uniquement)** à l'étape 1, alors, à l'onglet IKEv1 :
   - Sélectionnez le **Exchange Mode (Mode d'échange)** : **auto (automatique)**, **aggressive (agressif)** ou **main (principal)**. Lorsque vous configurez un pare-feu pour qu'il utilise le mode d'échange **auto (automatique)**, il peut accepter des demandes de négociation

en mode **main (principal)** et **aggressive (agressif)**. Toutefois, chaque fois que cela est possible, il initiera des échanges en mode **main (principal)**.

> *Si vous ne définissez pas le mode d'échange sur **auto (automatique)**, vous devez alors configurer les deux homologues avec le même mode d'échange pour permettre à chaque homologue d'accepter les requêtes de négociation.*

- Sélectionnez un profil existant ou conservez le profil par défaut dans la liste **IKE Crypto Profile (Profil crypto IKE)**. Au besoin, vous pouvez procéder à la Définition des profils crypto IKE.
- (Uniquement si vous utilisez l'authentification basée sur les certificats et que le mode d'échange n'est pas défini sur aggressive (Agressif)) Sélectionnez **Enable Fragmentation (Activer la fragmentation)** pour permettre au pare-feu de fonctionner avec la fragmentation IKE.
- Cliquez sur **Dead Peer Detection (Détection des homologues inactifs)** et saisissez un **Interval (Intervalle)** (plage de 2 à 100 secondes). Sous **Retry (Tentative)**, définissez le délai (plage de 2 à 100 secondes) avant une nouvelle tentative de vérification de la disponibilité. L'option Détection des homologues inactifs identifie les homologues IKE inactifs ou indisponibles en envoyant une charge utile de notification IKE de phase 1 à l'homologue et en attendant un accusé de réception.

4. Si vous configurez le **IKEv2 only mode (Mode IKEv2 uniquement)** ou le **IKEv2 preferred mode (Mode IKEv2 préféré)** à l'étape 1, alors, à l'onglet IKEv2 :
   - Sélectionnez un **IKE Crypto Profile (Profil crypto IKE)**, qui configure les options IKE de phase 1 comme le groupe DH, l'algorithme de hachage et l'authentification ESP. Pour plus d'informations sur les profils crypto IKE, reportez-vous à la section IKE Phase 1.
   - (Facultatif) Activez la **Strict Cookie Validation (validation du cookie stricte)** Seuil d'activation du cookie et validation du cookie stricte.
   - (Facultatif) **Enable Liveness Check (Activez la vérification de l'activité)** et saisissez un **Interval (sec) (Intervalle (sec)** (5 par défaut)si vous souhaitez que la passerelle envoie une requête de message à son homologue en lui demandant une réponse. Si nécessaire, l'initiateur tente la vérification de l'activité jusqu'à 10 fois. S'il ne reçoit pas de réponse, l'initiateur ferme et supprime les IKE_SA et CHILD_SA. L'initiateur commence à envoyer un autre message IKE_SA_INIT.

**STEP 8 |** Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.

## Exportation d'un certificat pour l'accès d'un homologue à l'aide de Hachage et URL

IKEv2 prend en charge la méthode Échange de certificat Hachage et URL permettant à l'homologue situé à l'extrémité distante du tunnel d'extraire le certificat d'un serveur sur lequel vous avez exporté le certificat. Effectuez cette tâche pour exporter votre certificat sur ce serveur. Vous devez déjà avoir créé un certificat via **Device (Périphérique)** > **Certificate Management (Gestion des certificats)**.

**STEP 1 |** Sélectionnez **Device (Périphérique)** > **Certificates (Certificats)** et, si votre plate-forme prend en charge plusieurs systèmes virtuels, dans **Location (Emplacement)**, sélectionnez le système virtuel approprié.

**STEP 2 |** Dans l'onglet **Device Certificates (Certificats de périphérique)**, sélectionnez le certificat à **Export (Exporter)** vers le serveur.

*L'état du certificat doit être valide, et non expiré. Le pare-feu ne vous empêche pas d'exporter un certificat non valide.*

**STEP 3 |** Dans **File Format (Format de fichier)**, sélectionnez **Binary Encoded Certificate (DER) (Certificat codé en binaire (DER))**.

**STEP 4 |** Ne cochez pas la case **Export private key (Exporter la clé privée)**. L'exportation de la clé privée n'est pas nécessaire pour l'échange de certificat Hachage et URL.

**STEP 5 |** Cliquez sur **OK**.

## Importation d'un certificat pour l'authentification de passerelle IKEv2

Effectuez cette tâche si vous authentifiez un homologue pour une passerelle IKEv2 et que vous n'avez pas utilisé un certificat local existant sur le pare-feu. Vous souhaitez importer un certificat depuis n'importe quel emplacement.

Cette tâche implique que vous avez sélectionné **Network (Réseau)** > **IKE Gateways (Passerelles IKE)**, que vous avez ajouté une passerelle et que, dans **Local Certificate (Certificat local)**, vous avez cliqué sur **Import (Importer)**.

**STEP 1 |** Importez un certificat.

1. Sélectionnez **Network (Réseau)** > **IKE Gateways (Passerelles IKE)**, cliquez sur **Add (Ajouter)** pour ajouter une passerelle puis, dans l'onglet **General (Général)**, sous **Authentication (Authentification)**, sélectionnez **Certificate (Certificat)**. Sous **Local Certificate (Certificat local)**, cliquez sur **Import (Importer)**.
2. Dans la fenêtre d'importation du certificat, saisissez un **Certificate Name (Nom du certificat)** pour le certificat que vous importez.
3. Sélectionnez **Shared (Partagé)** si vous souhaitez que ce certificat soit partagé par plusieurs systèmes virtuels.
4. Dans **Certificate File (Fichier de certificat)**, cliquez sur **Browse (Parcourir)** pour chercher le fichier de certificat. Cliquez sur le nom du fichier et sur **Open (Ouvrir)** pour renseigner le champ **Certificate File (Fichier de certificat)**.
5. Sous **File Format (Format de fichier)**, sélectionnez l'une des options suivantes :
   - **Base64 Encoded Certificate (PEM) (Certificat codé en Base64 (PEM))** - Contient le certificat mais pas la clé. Il s'agit de texte en clair.
   - **Encrypted Private Key and Certificate (PKCS12) (Clé privée et certificat cryptés (PKCS12))** - Contient le certificat et la clé.
6. Sélectionnez **Import private key (Importer la clé privée)** si la clé se trouve dans un autre fichier que le fichier de certificat. La clé est facultative, à l'exception suivante :
   - Vous devez importer une clé si vous avez défini **File Format (Format de fichier)** sur **PEM (PEM)**. Saisissez un **Key file (Fichier de clé)** en cliquant sur **Browse (Parcourir)** et en accédant au fichier de clé à importer.
   - Saisissez une **Passphrase (Phrase secrète)** et **Confirm Passphrase (Confirmez la phrase secrète)**.

7. Cliquez sur **OK**.

**STEP 2 |** Passez à la tâche suivante.

Étape Configurez l'authentification basée sur les certificats.

## Modification de la durée de vie de la clé ou de l'intervalle d'authentification pour IKEv2

Cette tâche est facultative ; le paramètre par défaut de durée de vie de la clé SA IKEv2 est de 8 heures. Le paramètre par défaut du multiple d'authentification IKEv2 est 0, ce qui désactive la fonction de réauthentification. Pour obtenir de plus amples renseignements, reportez-vous à la section Durée de vie de la clé et intervalle de réauthentification SA.

Procédez comme suit pour modifier les valeurs par défaut : Un profil crypto IKE doit déjà exister (condition préalable).

**STEP 1 |** Modifiez la durée de vie de la clé ou de l'intervalle d'authentification SA pour un profil crypto IKE.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Crypto (Crypto IKE)** et sélectionnez le profil crypto IKE qui s'applique à la passerelle locale.
2. Sous **Key Lifetime (Durée de vie de la clé)**, sélectionnez une unité (**Seconds (Secondes)**, **Minutes (Minutes)**, **Hours (Heures)** ou **Days (Jours)** et saisissez une valeur. La valeur minimale est trois minutes.
3. Sous **IKE Authentication Multiple (Multiple d'authentification IKE)**, saisissez une valeur qui est multipliée par la durée de vie de la clé pour déterminer l'intervalle de réauthentification.

**STEP 2 |** Validez vos modifications.

Cliquez sur **OK**, puis sur **Commit (Valider)**.

## Modification du seuil d'activation du cookie pour IKEv2

Effectuez la tâche suivante si vous souhaitez qu'un pare-feu dispose d'un seuil différent du paramètre par défaut de 500 sessions SA demi-ouvertes avant qu'une validation du cookie ne soit nécessaire. Pour obtenir de plus amples renseignements sur l'activation du cookie, reportez-vous à la section Seuil d'activation du cookie et validation du cookie stricte.

**STEP 1 |** Modifiez le seuil d'activation du cookie.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Session (Session)** et modifiez les paramètres de session VPN. Sous **Cookie Activation Threshold (Seuil d'activation du cookie)**, saisissez le nombre maximum de SA demi-ouvertes avant que le répondeur ne demande un cookie à l'initiateur (plage de 0 à 65535 ; par défaut 500).
2. Cliquez sur **OK**.

**STEP 2 |** Validez vos modifications.

Cliquez sur **OK**, puis sur **Commit (Valider)**.

### Configuration des sélecteurs de trafic IKEv2

Dans IKEv2, vous pouvez configurer des Sélecteurs de trafic, qui sont des composants de trafic réseau utilisés pendant une négociation IKE. Les sélecteurs de trafic sont utilisés pendant CHILD_SA (création de tunnel) phase 2 pour configurer le tunnel et déterminer le trafic autorisé dans le tunnel. Les deux homologues de passerelle IKE doivent négocier et s'accorder sur leurs sélecteurs de trafic ; sinon, un côté réduit sa plage d'adresses pour parvenir à un accord. Une connexion IKE peut comporter plusieurs tunnels ; par exemple, vous pouvez affecter différents tunnels à chaque service pour isoler son trafic. La séparation du trafic permet également de mettre en œuvre des fonctionnalités telles que QoS. Servez-vous des flux de travail suivants pour configurer les sélecteurs de trafic.

**STEP 1 |** Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)** > **Proxy IDs (ID de proxy)**.

**STEP 2 |** Sélectionnez l'onglet **IPv4 (IPv4)** ou **IPv6 (IPv6)**.

**STEP 3 |** Cliquez sur **Add (Ajouter)** et saisissez un **Name (Nom)** dans le champ **Proxy ID (ID de proxy)**.

**STEP 4 |** Dans le champ **Local (Local)**, saisissez la **Source IP Address (Adresse IP source)**.

**STEP 5 |** Dans le champ **Remote (Distant)**, saisissez la **Destination IP Address (Adresse IP de destination)**.

**STEP 6 |** Dans le champ **Protocol (Protocole)**, sélectionnez le protocole de transport (**TCP (TCP)** ou **UDP (UDP)**).

**STEP 7 |** Cliquez sur **OK**.

## Définition de profils cryptographiques

Un profil cryptographique spécifie les cryptages utilisés pour l'authentification et/ou le cryptage entre deux homologues IKE, ainsi que la durée de vie de la clé. La période entre chaque renégociation est appelée durée de vie ; lorsque le délai spécifié expire, le pare-feu renégocie un nouvel ensemble de clés.

Afin de sécuriser la communication via le tunnel VPN, le pare-feu nécessite des profils cryptographiques IKE et IPSec pour pouvoir effectuer respectivement les négociations IKE de phase 1 et de phase 2. Le pare-feu inclut un profil crypto IKE par défaut et un profil crypto IPSec par défaut prêts à l'emploi.

- Définition de profils crypto IKE
- Définition de profils crypto IPSec

### Définition de profils crypto IKE

Le profil crypto IKE permet de configurer les algorithmes de cryptage et d'authentification utilisés pour le processus d'échange de clés à la phase 1 du protocole IKE, ainsi que la durée de vie des clés qui spécifie leur durée de validité. Pour appeler le profil, vous devez l'associer à la configuration de passerelle IKE.

*Toutes les passerelles IKE configurées sur la même interface ou adresse IP locale doivent utiliser le même profil cryptographique lorsque le **Peer IP Address Type (Type d'adresse IP homologue)** de la passerelle IKE est configuré comme **Dynamic (Dynamique)** et que le mode principal IKEv1 ou IKEv2 est appliqué.*

**STEP 1 |** Créez un nouveau profil IKE.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Crypto (Crypto IKE)**, puis sélectionnez **Add (Ajouter)**.
2. Donnez un **Name (Nom)** au nouveau profil.

**STEP 2 |** Spécifiez le groupe DH (groupe Diffie–Hellman) pour l'échange de clé, ainsi que les algorithmes d'authentification et de cryptage.

Cliquez sur **Add (Ajouter)** dans les sections correspondances (groupe DH, authentification et cryptage), et sélectionnez dans le menu.

En cas de doute sur la prise en charge des homologues VPN, ajoutez plusieurs groupes et algorithmes dans l'ordre du plus sécurisé au moins sécurisé ; les homologues négocient le groupe ou l'algorithme pris en charge le plus fort pour établir le tunnel.

- Groupe DH—
  - **group20**
  - **group19**
  - **group14**
  - **group5**
  - **group2**
  - **group1**
- Authentification—
  - **SHA512**
  - **sha384**
  - **sha256**
  - **sha1**
  - **md5**
  - (PAN-OS 10.0.3 and later 10.1 releases (PAN-OS 10.0.3 et version 10.1 ultérieures)) **None (Aucun)**

    *Si vous sélectionnez un algorithme AES-GCM pour le cryptage, vous devez sélectionner le paramètre d'authentification **none (aucun)** sans quoi la validation échouera. Le hachage est automatiquement sélectionné sur la base du groupe DH sélectionné. Le groupe DH 19 et en-dessous utilise **sha256** ; le groupe DH 20 utilise **sha384**.*
- Cryptage—
  - (PAN-OS 10.0.3 and later 10.1 releases (PAN-OS 10.0.3 et versions 10.1 ultérieures)) **aes-256-gcm** (nécessite IKEv2 ; le groupe DH doit être réglé sur **group20**)
  - (PAN-OS 10.0.3 and later 10.1 releases (PAN-OS 10.0.3 et versions 10.1 ultérieures)) **aes-128-gcm** (nécessite IKEv2 et le groupe DH doit être réglé sur **group19**)
  - **aes-256-cbc**
  - **aes-192-cbc**
  - **aes-128-cbc**
  - **3des**
  - **des**

*Choisissez l'authentification et les algorithmes de cryptage les plus forts que l'homologue peut prendre en charge. Pour l'algorithme d'authentification, utilisez SHA-256 ou supérieur (privilégiez SHA-384 ou supérieur pour les transactions durables). N'utilisez pas SHA-1 ou MD5. Pour l'algorithme de chiffrement, utilisez AES ; DES et 3DES sont faibles et vulnérables. L'AES avec le mode Galois/Compteur (AES-GCM) offre la sécurité la plus forte et dispose d'une authentification intégrée. Vous devez donc régler l'authentification sur **none (aucune)** si vous sélectionnez le cryptage **aes-256-gcm** ou **aes-128-gcm**.*

**STEP 3 |** Spécifiez la durée de validité de la clé et l'intervalle de réauthentification.

Pour obtenir de plus amples renseignements, reportez-vous à la section Durée de vie de la clé et intervalle de réauthentification SA.

1. Dans les champs **Key Lifetime (Durée de vie de la clé)**, spécifiez la période (en secondes, minutes, heures ou jours) pendant laquelle la clé est valide (plage de 3 minutes à 365 jours ; valeur par défaut : 8 heures). Lorsque la clé expire, le pare-feu renégocie une nouvelle clé. La durée de vie correspond à la période entre chaque renégociation.
2. Dans **IKEv2 Authentication Multiple (Multiple d'authentification IKEv2)**, spécifiez une valeur (plage de 0 à 50 ; valeur par défaut : 0) qui est multipliée par la **Key Lifetime (Durée de vie de la clé)** pour déterminer le nombre d'authentifications. La valeur par défaut de 0 désactive la fonction de réauthentification.

**STEP 4 |** Validez votre profil crypto IKE.

Cliquez sur **OK (OK)**, puis sur **Commit (Valider)**.

**STEP 5 |** Associez le profil crypto IKE à la configuration de passerelle IKE.

Reportez-vous à la section Configurez des options avancées pour la passerelle.

## Définition de profils crypto IPSec

Le profil crypto IPSec est appelé à la phase 2 du protocole IKE. Il indique la manière dont les données sont sécurisées dans le tunnel lorsque l'échange de clés automatiques est utilisé pour générer automatiquement les clés pour les SA IKE.

**STEP 1 |** Créez un nouveau profil IPSec.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IPSec Crypto (Crypto IPSec)**, puis cliquez sur **Add (Ajouter)**.
2. Donnez un **Name (Nom)** au nouveau profil.
3. Sélectionnez le **IPSec Protocol (Protocole IPSec)** (ESP ou AH) que vous souhaitez appliquer pour sécuriser les données dans le tunnel.

   *Il est recommandé de sélectionner l'Encapsulating Security Payload (encapsulation de la charge utile de sécurité ; ESP) plutôt que l'Authentication Header (en-tête d'authentification ; AH), puisque ESP procure la confidentialité et l'authentification de la connexion, alors qu'AH ne procure que l'authentification.*
4. Cliquez sur **Add (Ajouter)**, puis sélectionnez les algorithmes d'**Authentication (Authentification)** et de **Encryption (Cryptage)** pour ESP, ainsi que les algorithmes

d'**Authentication (Authentification)** pour AH, de manière à ce que les homologues IKE puissent négocier les clés pour le transfert sécurisé des données via le tunnel.

En cas de doute sur les algorithmes IKE pris en charge par les homologues VPN, ajoutez-en plusieurs dans l'ordre du plus sécurisé au moins sécurisé, comme suit. Les homologues négocient l'algorithme pris en charge le plus renforcé pour établir le tunnel :

- Cryptage : **aes-256-gcm (aes-256-gcm)**, **aes-256-cbc (aes-256-cbc)**, **aes-192-cbc (aes-192-cbc)**, **aes-128-gcm (aes-128-gcm)**, **aes-128-ccm (aes-128-ccm)** (le pare-feu VM-Series ne prend pas en charge cette option), **aes-128-cbc (aes-128-cbc)**, **3des (3des)**, **des (des)**.

  *Il est recommandé de choisir l'authentification et les algorithmes de chiffrement les plus forts que l'homologue peut prendre en charge. Pour l'algorithme d'authentification, utilisez SHA-256 ou supérieur (privilégiez SHA-384 ou supérieur pour les transactions durables). N'utilisez pas SHA-1, MD5 ou aucun. Pour l'algorithme de chiffrement, utilisez AES ; DES et 3DES sont faibles et vulnérables.*

- Authentification : **sha512 (sha512)**, **sha384 (sha384)**, **sha256 (sha256)**, **sha1 (sha1)**, **md5 (md5)**.

**STEP 2 |** Sélectionnez le groupe DH à utiliser pour les négociations SA IPSec dans la phase 2 du protocole IKE.

Sous **DH Group (Groupe DH)**, sélectionnez la force de clé que vous souhaitez utiliser : **group1**, **group2**, **group5**, **group14**, **group19** ou **group20**. Pour une sécurité maximale, choisissez le groupe dont le nombre est le plus élevé.

Si vous ne souhaitez pas renouveler la clé créée par le pare-feu lors de la négociation IKE de phase 1, sélectionnez **no-pfs (Mode PFS (Perfect Forward Secrecy) désactivé)** ; le pare-feu réutilise la clé actuelle pour les négociations SA IPSec.

**STEP 3 |** Spécifiez la durée de la clé (durée et volume du trafic).

L'utilisation d'une combinaison de durée et de volume du trafic vous permet de garantir la sécurité des données.

Sélectionnez la **Lifetime (Durée de vie)** ou la période pendant laquelle la clé est valide en secondes, minutes, heures ou jours (plage de 3 minutes à 365 jours). Lorsque le délai spécifié expire, le pare-feu renégocie un nouvel ensemble de clés.

Sélectionnez la **Lifesize (Taille réelle)** ou le volume de données après lequel les clés doivent être renégociées.

**STEP 4 |** Validez votre profil IPSec.

Cliquez sur **OK (OK)**, puis sur **Commit (Valider)**.

**STEP 5 |** Associez le profil IPSec à une configuration de tunnel IPSec.

Reportez-vous à la section Configuration de l'échange de clés.

# Configuration d'un tunnel IPSec

La configuration du tunnel IPSec vous permet de vous authentifier et/ou de crypter les données (paquet IP) dans le tunnel.

Si vous configurez le pare-feu pour fonctionner avec un homologue qui prend en charge un VPN basé sur une politique, vous devez définir des ID de proxy. Les périphériques qui prennent en charge un VPN basé sur une politique utilisent des règles/politiques de sécurité spécifiques ou des listes d'accès (adresses sources, adresses de destination et ports) pour autoriser le trafic intéressant via un tunnel IPSec. Ces règles sont référencées lors de la négociation de phase 2 du protocole IKE/en mode rapide et sont échangées sous forme d'ID de proxy dans le premier ou le second message du processus. Par conséquent, si vous configurez le pare-feu pour fonctionner avec un homologue VPN basé sur une politique, pour une négociation de phase réussie, vous devez définir l'ID de proxy de manière à ce que la configuration des deux homologues soit identique. Si l'ID de proxy n'est pas configuré, comme le pare-feu prend en charge un VPN de routage, les valeurs par défaut utilisées comme ID de proxy sont les suivantes : adresse IP source : 0.0.0.0/0, adresse IP de destination : 0.0.0.0/0 et application : indifférente ; lorsque ces valeurs sont échangées avec l'homologue, il est impossible de configurer la connexion VPN.

**STEP 1 |** Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)**, puis **Add (Ajoutez)** une nouvelle configuration de tunnel.

**STEP 2 |** Dans l'onglet **General (Général)**, donnez un **Name (Nom)** au tunnel.

**STEP 3 |** Sélectionnez la **Tunnel interface (Interface de tunnel)** sur laquelle configurer le tunnel IPSec.

Pour créer une nouvelle interface de tunnel :

1. Sélectionnez **Tunnel Interface (Interface de tunnel** > **New Tunnel Interface (Nouvelle Interface de tunnel)**. Vous pouvez également sélectionner **Network (Réseau)** > **Interfaces (Interfaces)** > **Tunnel** et cliquer sur **Add (Ajouter)**.
2. Dans le champ **Interface Name (Nom de l'interface)**, spécifiez un suffixe numérique, tel que **.2**.
3. Dans l'onglet **Config (Configuration)**, sélectionnez la liste **Security Zone (Zone de sécurité)** pour définir la zone de la manière suivante :

**Utiliser votre zone approuvée comme point de terminaison du tunnel**, sélectionnez la zone. L'association de l'interface de tunnel à la même zone (et au même routeur virtuel) que l'interface externe sur laquelle les paquets traversent le pare-feu atténue le besoin de créer un routage inter-z

Ou :

**Créer une zone séparée pour la terminaison du tunnel VPN** (Recommandé) : sélectionnez une **New Zone (Nouvelle Zone)**, saisissez un **Name (Nom)** pour la nouvelle zone (par exemple vpn-corp), et cliquez sur **OK**.

1. Sous **Virtual Router (Routeur virtuel)**, sélectionnez **default (par défaut)**.
2. (Facultatif) Si vous souhaitez affecter une adresse IPv4 à l'interface de tunnel, cliquez sur l'onglet **IPv4**, puis **Add (Ajoutez)** l'adresse IP ainsi que le masque réseau, par exemple, 10.31.32.1/32.
3. Cliquez sur **OK**.

**STEP 4 |** (Facultatif )Activez IPv6 sur l'interface de tunnel.

1. Sélectionnez l'onglet IPv6 sur **Network (Réseau)** > **Interfaces (Interfaces)** > **Tunnel** > **IPv6**.
2. Sélectionnez **Enable IPv6 on the interface (Activer IPv6 sur l'interface)**.

   Cette option vous permet d'acheminer le trafic IPv6 sur un tunnel IPSec IPv4 et assurera la confidentialité entre les réseaux IPv6. Le trafic IPv6 est encapsulé par IPv4, puis ESP. Pour acheminer le trafic IPv6 vers le tunnel, vous pouvez utiliser un itinéraire statique vers le tunnel, ou OSPFv3, ou une règle de transfert basé sur une politique.
3. Saisissez l'**ID d'interface** unique étendu sur 64 bits au format hexadécimal, par exemple, 00:26:08:FF:FE:DE:4E:29. Par défaut, le pare-feu utilise l'identifiant unique étendu sur 64 bits (EUI-64) généré à partir de l'adresse MAC de l'interface physique.
4. Pour affecter une **Address (Adresse) IPv6**, à l'interface de tunnel, **Add (Ajoutez)**l'adresse IPv6 et une longueur de préfixe, par exemple, 2001:400:f00::1/64. Si aucun préfixe n'est sélectionné, l'adresse IPv6 affectée à l'interface sera intégralement définie dans la zone de saisie de l'adresse.
   1. Sélectionnez **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** pour assigner une adresse IPv6 à l'interface qui va utiliser l'ID de l'interface comme partie hôte de l'adresse.
   2. Sélectionnez **Anycast** pour inclure un routage via le nœud le plus proche.

**STEP 5 |** Configurez un échange de clés.

À l'onglet **General (Général)**, configurez l'un des types d'échange de clés suivants :

**Configurez un échange de clés automatiques**

1. Sélectionnez la passerelle IKE. Pour configurer une passerelle IKE, reportez-vous à la section Configuration d'une passerelle IKE.
2. (Facultatif) Sélectionnez le profil crypto IPSec par défaut. Pour créer un nouveau profil IPSec, reportez-vous à la section Définition de profils crypto IPSec.

**Configurez un échange de clés manuelles.**

1. Spécifiez le **Local SPI (Index de paramètre de sécurité local)** du pare-feu local. Le SPI est un index hexadécimal de 32 bits qui est ajouté à l'en-tête de tunnellisation IPSec afin de distinguer les flux de trafic IPSec ; il est utilisé pour créer la SA requise pour l'établissement d'un tunnel VPN.
2. Sélectionnez l'**Interface** qui sera le point de terminaison du tunnel ; vous pouvez également sélectionner l'adresse IP de l'interface locale qui est le point de terminaison du tunnel.
3. Sélectionnez le protocole **AH** ou **ESP**.
4. Pour AH, sélectionnez la méthode d'**Authentication (Authentification)**, puis saisissez une **Key (Clé)** et **Confirm Key (Confirmez-la)**.
5. Pour ESP, sélectionnez la méthode d'**Authentication (Authentification)**, puis saisissez une **Key (Clé)** et **Confirm Key (Confirmez-la)**. Ensuite, sélectionnez la méthode de **cryptage**, puis saisissez une **clé** et **confirmez-la**, si nécessaire.
6. Spécifiez le **Remote SPI (Index de paramètre de sécurité distant)** de l'homologue distant.
7. Saisissez l'**Remote Address (Adresse distante)**, l'adresse IP de l'homologue distant.

**STEP 6 |** Protégez-vous contre une attaque par relecture.

L'anti-rejeu est un sous-protocole d'IPSec et fait partie de la demande de commentaires (RFC) 6479 de l'Internet Engineering Task Force (IETF). Le protocole anti-rejeu est utilisé pour empêcher les pirates d'injecter ou d'apporter des modifications aux paquets qui voyagent d'une source à une destination et utilise une association de sécurité unidirectionnelle afin d'établir une connexion sécurisée entre deux nœuds du réseau.

Une fois qu'une connexion sécurisée est établie, le protocole anti-rejeu utilise des numéros de séquence de paquets pour vaincre les attaques de relecture. Lorsque la source envoie un message, elle ajoute un numéro de séquence à son paquet ; le numéro de séquence commence à 0 et est incrémenté de 1 pour chaque paquet suivant. La destination conserve la séquence de nombres dans un format de ***sliding window (fenêtre glissante)***, conserve un enregistrement des numéros de séquence des paquets reçus validés et rejette tous les paquets dont le numéro de séquence est inférieur au plus petit de la fenêtre glissante (paquets trop anciens ) ou des paquets qui apparaissent déjà dans la fenêtre glissante (paquets dupliqués ou rejoués). Les paquets acceptés, une fois validés, mettent à jour la fenêtre glissante, déplaçant le plus petit numéro de séquence hors de la fenêtre si elle était déjà pleine.

1. À l'onglet Général, sélectionnez **Show Advanced Options (Afficher les options avancées)**, puis sélectionnez **Enable Replay Protection (Activer la protection contre la relecture)** pour détecter et neutraliser les attaques par relecture.
2. Sélectionnez la **Anti Replay Window (fenêtre Anti Replay)** à utiliser. Vous pouvez sélectionner une taille de fenêtre anti-relecture de 64, 128, 256, 512, 1024, 2048 ou 4096. La valeur par défaut est 1024.

**STEP 7 |** (Facultatif) Conservez l'en-tête ToS pour la priorité ou le traitement des paquets IP.

Dans la section Afficher les options avancées, sélectionnez **Copy TOS Header (Copier l'en-tête ToS)**. Cela permet de copier l'en-tête Type of Service (type de service ; ToS) de l'en-tête IP interne vers l'en-tête IP externe des paquets encapsulés afin de conserver les informations ToS d'origine.

*Les paquets IPSec pourraient arriver dans le désordre si vous copiez l'en-tête ToS et qu'il y a plusieurs sessions dans le tunnel (chacune d'entre elles possédant une valeur de ToS différente),*

**STEP 8 |** (Facultatif) Sélectionnez **Add GRE Encapsulation (Ajouter l'encapsulation GRE)** pour activer GRE sur IPSec.

Ajoutez l'encapsulation GRE dans les cas où le point de terminaison distant exiger l'encapsulation du trafic dans un tunnel GRE avant son chiffrement par IPSec. Par exemple, certaines applications exigent l'encapsulation du trafic multidiffusion avant son chiffrement par IPSec. Ajoutez l'encapsulation GRE lorsque le paquet GRE encapsulé dans IPSec possède la même adresse IP source et le même adresse IP de destination que le tunnel IPSec procédant à l'encapsulation.

**STEP 9 |** Activez la surveillance des tunnels.

*Vous devez affecter une adresse IP à l'interface de tunnel à surveiller.*

Pour informer l'administrateur des périphériques de la défaillance d'un tunnel et pour basculer automatiquement vers une autre interface de tunnel :

1. Sélectionnez **Tunnel Monitor (Surveillance des tunnels)**.
2. Spécifiez une adresse **Destination IP (IP de destination)** de l'autre côté du tunnel pour déterminer si le tunnel fonctionne correctement.
3. Sélectionnez un **Profile (Profil)** pour déterminer l'action en cas de défaillance du tunnel. Pour créer un nouveau profil, reportez-vous à la section Définition d'un profil de surveillance des tunnels.

**STEP 10 |** Créez un ID de proxy pour identifier les homologues VPN.

(Requis uniquement si l'homologue VPN utilise un VPN basé sur une politique)

1. Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)**, puis cliquez sur **Add (Ajouter)**.
2. Sélectionnez l'onglet **ID de proxy**.
3. Sélectionnez l'onglet **IPv4 (IPv4)** ou **IPv6 (IPv6)**.
4. Cliquez sur **Add (Ajouter)** et saisissez le nom de **Proxy ID (ID de proxy)**.
5. Saisissez l'adresse IP **Local (Locale)** ou le sous-réseau de la passerelle VPN.
6. Saisissez l'adresse **Remote (Distante)** de la passerelle VPN.
7. Sélectionnez le **Protocol (Protocole)** :
   - **Number (Numéro)** - Indiquez le numéro de protocole (pour assurer l'interopérabilité avec des périphériques tiers).
   - **Any (Indifférent)** : autorisez le trafic TCP et/ou UDP.
   - **TCP** : indiquez les numéros de port TCP locaux et distants.
   - **UDP** : indiquez les numéros de port UDP locaux et distants.
8. Cliquez sur **OK**.

**STEP 11 |** Validez vos modifications.

Cliquez sur **OK**, puis sur **Commit (Valider)**.

## Configuration de la surveillance des tunnels

Pour fournir un service VPN ininterrompu, vous pouvez utiliser la détection des homologues inactifs ainsi que la fonction de surveillance des tunnels sur le pare-feu. Vous pouvez également surveiller l'état du tunnel. Ces tâches de surveillance sont décrites dans les sections suivantes :

- Définition d'un profil de surveillance des tunnels
- Affichage de l'état des tunnels

## Définition d'un profil de surveillance des tunnels

Un profil de surveillance des tunnels vous permet de vérifier la connexion entre les homologues VPN ; vous pouvez configurer l'interface de tunnel pour envoyer une requête ping à une adresse IP de destination à un intervalle donné et spécifier l'action si la communication via le tunnel est rompue.

**STEP 1 |** Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **Monitor (Surveillance)**. Un profil de surveillance des tunnels par défaut peut être utilisé.

**STEP 2 |** Cliquez sur **Add (Ajouter)**, puis donnez un **Name (Nom)** au profil.

**STEP 3 |** Sélectionnez l'**Action (Action)** à prendre si l'adresse IP de destination est inaccessible.

- **Wait Recover (Attente de la récupération)** : le pare-feu attend la récupération du tunnel. Il continue d'utiliser l'interface de tunnel dans les décisions de routage comme si le tunnel était encore actif.
- **Fail Over (Basculement)** : force le trafic vers un chemin d'accès des sauvegardes, le cas échéant. Le pare-feu désactive l'interface de tunnel, et par là même tous les itinéraires de la table de routage qui utilisent l'interface.

Dans tous les cas, le pare-feu tente d'accélérer la récupération en négociant de nouvelles clés IPSec.

**STEP 4 |** Spécifiez l'**Interval (sec) (Intervalle (sec.)** et le **Threshold (Seuil)** de déclenchement de l'action donnée.

- **Threshold (Seuil)** précise le nombre de pulsations pendant lesquelles il faut attendre avant d'appliquer l'action définie (intervalle compris entre 2 et 100 ; valeur par défaut : 5).
- **Interval (sec) (Intervalle (sec.))** précise le délai (en secondes) entre les pulsations (intervalle compris entre 2 et 10, valeur par défaut : 3).

**STEP 5 |** Associez le profil de surveillance à la configuration de tunnel IPSec. Reportez-vous à la section Activez la surveillance des tunnels.

## Affichage de l'état des tunnels

L'état du tunnel vous informe si des SA IKE de phase 1 et de phase 2 valides ont été établies, et si l'interface de tunnel est active et disponible pour la transmission du trafic.

Comme l'interface de tunnel est une interface logique, elle ne peut pas indiquer l'état d'une liaison physique. Par conséquent, vous devez activer la surveillance des tunnels de manière à ce que l'interface de tunnel puisse vérifier la connexion à une adresse IP et déterminer si le chemin d'accès peut encore être utilisé. Si l'adresse IP est inaccessible, le pare-feu attend la récupération du tunnel ou le basculement vers un autre tunnel. Lorsqu'un basculement se produit, le tunnel existant est arrêté et des modifications de routage sont déclenchées pour configurer un nouveau tunnel et rediriger le trafic.

**STEP 1 |** Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)**.

**STEP 2 |** Affichez l'**état du tunnel**.

- La couleur verte indique un tunnel de SA IPSec valide.
- La couleur rouge indique qu'une SA IPSec n'est pas disponible ou a expiré.

**STEP 3 |** Affichez l'**IKE Gateway Status (état de la passerelle IKE)**.

- La couleur verte indique une SA IKE de phase 1 valide.
- La couleur rouge indique qu'une association de sécurité IKE de phase 1 n'est pas disponible ou a expiré.

**STEP 4 |** Affichez **Tunnel Interface Status (l'état de l'interface de tunnel)**.

- La couleur verte indique que l'interface de tunnel est active.
- La couleur rouge indique que l'interface de tunnel est inactive, car la surveillance des tunnels est activée et l'état est inactif.

Pour rendre actif un tunnel VPN, reportez-vous à la section Interprétation des messages d'erreur VPN.

# Activation/désactivation, actualisation ou redémarrage d'une passerelle IKE ou d'un tunnel IPSec

Vous pouvez activer, désactiver, actualiser ou redémarrer une passerelle IKE ou un tunnel IPSec pour simplifier le dépannage.

- Activation ou désactivation d'une passerelle IKE ou d'un tunnel IPSec
- Comportements d'actualisation et de redémarrage
- Activation ou redémarrage d'une passerelle IKE ou d'un tunnel IPSec

## Activation ou désactivation d'une passerelle IKE ou d'un tunnel IPSec

Activez ou désactivez une passerelle IKE ou un tunnel IPSec pour simplifier le dépannage.

- Activez ou désactivez une passerelle IKE.
  1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Gateways (Passerelles IKE)** et sélectionnez la passerelle que vous souhaitez activer ou désactiver.
  2. Au bas de l'écran, cliquez sur **Enable (Activer)** ou **Disable (Désactiver)**.

- Activez ou désactivez un tunnel IPSec.
  1. Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)** et sélectionnez le tunnel que vous souhaitez activer ou désactiver.
  2. Au bas de l'écran, cliquez sur **Enable (Activer)** ou **Disable (Désactiver)**.

## Comportements d'actualisation et de redémarrage

Vous pouvez Actualiser ou Redémarrer une passerelle IKE ou un tunnel IPSec. Les comportements d'actualisation et de redémarrage sont différents pour une passerelle IKE et un tunnel IPSec, comme suit :

| Phase | Actualiser | Redémarrer |
|---|---|---|
| Passerelle IKE | Met à jour les statistiques à l'écran pour la passerelle IKE sélectionnée. | Redémarre la passerelle IKE sélectionnée. |

| Phase | Actualiser | Redémarrer |
|---|---|---|
| (Phase 1 du protocole IKE) | Équivalent à l'exécution d'une seconde commande **show** dans la CLI (après une première **show**). | **IKEv2** : Redémarre également toute association de sécurité (SA) IPSec enfant associée.<br>**IKEv1** : Ne redémarre pas les SA IPSec associées.<br>Un redémarrage arrête toutes les sessions existantes.<br>Équivalent à l'exécution d'une séquence de commande **clear**, **test**, **show** dans la CLI. |
| Tunnel IPSec (Phase 2 du protocole IKE) | Met à jour les statistiques à l'écran pour le tunnel IPSec sélectionné.<br>Équivalent à l'exécution d'une seconde commande **show** dans la CLI (après une première **show**). | Redémarre le tunnel IPSec.<br>Un redémarrage arrête toutes les sessions existantes.<br>Équivalent à l'exécution d'une séquence de commande **clear**, **test**, **show** dans la CLI. |

## Activation ou redémarrage d'une passerelle IKE ou d'un tunnel IPSec

N'oubliez pas que le résultat du redémarrage d'une passerelle IKE est différent, selon qu'il s'agit d'une IKEv1 ou d'une IKEv2. Reportez-vous à Comportements d'actualisation et de redémarrage pour une passerelle IKE (IKEv1 et IKEv2) et pour un tunnel IPSec.

- Actualisez ou redémarrez une passerelle IKE.
  1. Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)** et sélectionnez le tunnel pour la passerelle que vous souhaitez actualiser ou redémarrer.
  2. Dans la ligne de ce tunnel, sous la colonne État, cliquez sur **IKE Info (Informations sur IKE)**.
  3. Au bas de l'écran d'informations sur IKE, cliquez sur l'action souhaitée :
     - **Refresh (Actualiser)** : met à jour les statistiques à l'écran.
     - **Restart (Redémarrer)** : efface les SA. Le trafic est donc interrompu jusqu'à ce que la négociation IKE recommence et que le tunnel soit recréé.

- Actualisez ou redémarrez un tunnel IPSec.

  Vous pouvez déterminer que le tunnel doit être actualisé ou redémarré car vous avez utilisé la surveillance des tunnels pour surveiller l'état des tunnels, ou que vous avez utilisé une surveillance réseau externe pour surveiller la connectivité réseau via le tunnel IPSec.

  1. Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)** et sélectionnez le tunnel que vous souhaitez actualiser ou redémarrer.
  2. Dans la ligne de ce tunnel, sous la colonne État, cliquez sur **Tunnel Info (Informations sur le tunnel)**.
  3. Au bas de l'écran d'informations sur le tunnel, cliquez sur l'action souhaitée :
     - **Refresh (Actualiser)** : met à jour les statistiques à l'écran.
     - **Restart (Redémarrer)** : efface les SA. Le trafic est donc interrompu jusqu'à ce que la négociation IKE recommence et que le tunnel soit recréé.

## Test de la connexion du VPN

Effectuez cette tâche pour tester la connectivité VPN.

**STEP 1 |** Initiez la phase 1 du protocole IKE en envoyant une requête ping à un hôte via le tunnel, ou en utilisant la commande CLI suivante :

```
test vpn ike-sa gateway <gateway_name>
```

**STEP 2 |** Saisissez la commande suivante pour déterminer si la phase 1 du protocole IKE est configurée :

```
show vpn ike-sa gateway <gateway_name>
```

Vérifiez que la Security Association (Association de sécurité) s'affiche dans le résultat. Si ce n'est pas le cas, consultez les messages du journal système pour interpréter la raison de l'échec.

**STEP 3 |** Initiez la phase 2 du protocole IKE en envoyant une requête ping à un hôte via le tunnel, ou en utilisant la commande CLI suivante :

```
test vpn ipsec-sa tunnel <tunnel_name>
```

**STEP 4 |** Saisissez la commande suivante pour déterminer si la phase 2 du protocole IKE est configurée :

```
show vpn ipsec-sa tunnel <tunnel_name>
```

Vérifiez que la Security Association (Association de sécurité) s'affiche dans le résultat. Si ce n'est pas le cas, consultez les messages du journal système pour interpréter la raison de l'échec.

**STEP 5 |** Pour afficher le informations relatif au flux de trafic VPN, utilisez la commande suivante :

```
show vpn flow
total tunnels configured:                1
filter - type IPSec, state any
```

```
total IPSec tunnel configured:        1
total IPSec tunnel shown:                1

name                     id      state      local-ip       peer-ip
       tunnel-i/f
------------------------------------------------------------------------------
vpn-to-siteB       5       active
    100.1.1.1     200.1.1.1     tunnel.41
```

## Interprétation des messages d'erreur VPN

Le tableau suivant répertorie certains des messages d'erreur VPN courants consignés dans le journal système.

**Table 6: Messages d'erreur Syslog relatifs aux problèmes VPN**

| Si l'erreur est la suivante : | Essayez ce qui suit : |
|---|---|
| `IKE phase-1 negotiation is failed as initiator, main mode. Failed SA: x.x.x.x[500]-y.y.y.y[500] cookie:84222f276c2fa2e9:0000000000000000 due to timeout.`<br>OU<br>`IKE phase-1 negotiation is failed. Couldn't find configuration for IKE phase-1 request for peer IP x.x.x.x[1929]` | • Vérifiez que l'adresse IP publique de chaque homologue VPN est exacte dans la configuration de passerelle IKE.<br>• Vérifiez que les adresses IP peuvent recevoir une requête ping et que des problèmes de routage ne causent pas l'échec de la connexion. |
| `Received unencrypted notify payload (no proposal chosen) from IP x.x.x.x[500] to y.y.y.y[500], ignored...`<br>OU<br>`IKE phase-1 negotiation is failed. Unable to process peer's SA payload.` | Dans la configuration du profil crypto IKE, vérifiez que les propositions de cryptage, d'authentification et de groupe DH sont identiques des deux côtés. |
| `pfs group mismatched:my: 2peer: 0`<br>OU<br>`IKE phase-2 negotiation failed when processing SA payload. No suitable proposal found in peer's SA payload.` | Dans la configuration du profil crypto IPSec, vérifiez ce qui suit :<br>• l'option PFS est activée ou désactivée sur les deux homologues VPN ;<br>• au moins un des groupes DH proposés par chaque homologue est identique. |

| Si l'erreur est la suivante : | Essayez ce qui suit : |
| --- | --- |
| `IKE phase-2 negotiation failed when processing Proxy ID. Received local id x.x.x.x/x type IPv4 address protocol 0 port 0, received remote id y.y.y.y/y type IPv4 address protocol 0 port 0.` | L'homologue VPN à une extrémité utilise un VPN basé sur une politique. Vous devez configurer un ID de proxy sur le pare-feu Palo Alto Networks. Reportez-vous à la section Création d'un ID de proxy pour identifier les homologues VPN. |

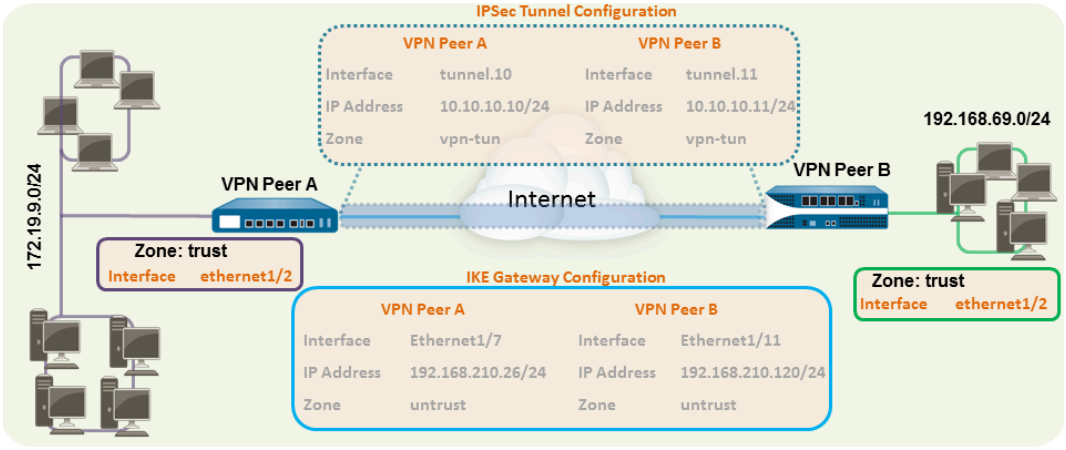
# Configurations rapides de VPN de site à site

Les sections suivantes fournissent des instructions pour la configuration de certains déploiements VPN courants :

- VPN de site à site avec routage statique
- VPN de site à site avec OSPF
- VPN de site à site avec routage statique et dynamique

## VPN de site à site avec routage statique

L'exemple suivant indique une connexion VPN entre deux sites qui utilisent des itinéraires statiques. Sans routage dynamique, les interfaces de tunnel sur les homologues VPN A et B ne nécessitent aucune adresse IP, car le pare-feu utilise automatiquement l'interface de tunnel comme saut suivant pour acheminer le trafic entre les sites. Toutefois, pour permettre la surveillance des tunnels, une adresse IP statique a été affectée à chaque interface de tunnel.



**STEP 1 |** Configurez une interface de couche 3.

Cette interface est utilisée pour le tunnel IKE de phase 1

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** et choisissez l'interface que vous souhaitez configurer pour le réseau privé virtuel.
2. Sélectionnez **Layer3 (Couche 3)** comme **Interface Type (Type de liaison)**.
3. Dans l'onglet **Config (Configuration)**, sélectionnez la **Security Zone (Zone de sécurité)** à laquelle appartient l'interface :
   - L'interface doit être accessible depuis une zone en dehors de votre réseau approuvé. Envisagez de créer une zone VPN dédiée pour améliorer la visibilité et le contrôle de votre trafic VPN.
   - Si vous n'avez pas encore créé de zone, sélectionnez **New Zone (Nouvelle zone)** dans la **Security Zone (Zone de sécurité)**, donnez un **Name (Nom)** à la zone et cliquez sur **OK (OK)**.
4. Sélectionnez le **Virtual Router (Routeur virtuel)** à utiliser.
5. Pour assigner une adresse IP à l'interface, cliquez sur l'onglet **IPv4**, puis sur **Add (Ajouter)** dans la section IP et saisissez l'adresse IP, ainsi que le masque réseau à assigner à l'interface, par exemple : 192.168.210.26/24.
6. Pour enregistrer la configuration de l'interface, cliquez sur **OK**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :

   - **Interface** : ethernet1/7
   - **Security Zone (Zone de sécurité)** : non approuvée
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** (IPv4) : 192.168.210.26/24

   La configuration de l'homologue VPN B est la suivante :

   - **Interface** : ethernet1/11
   - **Security Zone (Zone de sécurité)** : non approuvée
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** : 192.168.210.120/24

**STEP 2 |** Créez une interface de tunnel et associez-la à un routeur virtuel et une zone de sécurité.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Tunnel** et cliquez sur **Add (Ajouter)**.
2. Dans le champ **Interface Name (Nom de l'interface)**, spécifiez un suffixe numérique, tel que **.1**.
3. Dans l'onglet **Config (Configuration)**, développez la liste **Security Zone (Zone de sécurité)** pour définir la zone de la manière suivante :
   - Pour utiliser votre zone approuvée comme point de terminaison du tunnel, sélectionnez la zone.
   - (Recommandé) Pour créer une zone séparée pour la terminaison du tunnel VPN, cliquez sur **New Zone (Nouvelle zone)**. Dans la boîte de dialogue, donnez un **Name (Nom)** à la nouvelle zone (par exemple, ***vpn-tun***), puis cliquez sur **OK**.
4. Sélectionnez le **Virtual Router (Routeur virtuel)**.
5. (Facultatif) Affectez une adresse IP à l'interface de tunnel, sélectionnez l'onglet **IPv4** ou **IPv6**, puis cliquez sur **Add (Ajouter)** dans la section IP et saisissez l'adresse IP, ainsi que le masque réseau à affecter à l'interface.

   Avec les itinéraires statiques, l'interface de tunnel ne nécessite aucune adresse IP. Pour le trafic destiné à une adresse IP/un sous-réseau donné(e), l'interface de tunnel deviendra automatiquement le saut suivant. Envisagez d'ajouter une adresse IP si vous souhaitez activer la surveillance des tunnels.
6. Pour enregistrer la configuration de l'interface, cliquez sur **OK**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :
   - **Interface** : tunnel.10
   - **Zone de sécurité** : vpn_tun
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** (IPv4) : 172.19.9.2/24

   La configuration de l'homologue VPN B est la suivante :
   - **Interface** : tunnel.11
   - **Zone de sécurité** : vpn_tun
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** (IPv4) : 192.168.69.2/24

**STEP 3 |** Configurez un itinéraire statique, sur le routeur virtuel, vers le sous-réseau de destination.

1. Sélectionnez **Network (Réseau)** > **Virtual Router (Routeur virtuel)**, puis cliquez sur le routeur que vous avez défini à l'étape précédente.
2. Sélectionnez **Static Route (Itinéraire statique)**, cliquez sur **Add (Ajouter)** et saisissez un nouvel itinéraire pour accéder au sous-réseau à l'autre extrémité du tunnel.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :

   - **Destination** : 192.168.69.0/24
   - **Interface** : tunnel.10

   La configuration de l'homologue VPN B est la suivante :

   - **Destination** : 172.19.9.0/24
   - **Interface** : tunnel.11

**STEP 4 |** Configurez les profils crypto (profils crypto IKE pour la phase 1 et profil crypto IPSec pour la phase 2).

Effectuez cette tâche sur les deux homologues et assurez-vous de définir des valeurs identiques.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Crypto (Crypto IKE)**. Dans cet exemple, le profil par défaut est utilisé.
2. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IPSec Crypto (Crypto IPSec)**. Dans cet exemple, le profil par défaut est utilisé.

**STEP 5 |** Configurez la passerelle IKE.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Gateway (Passerelle IKE)**.
2. Cliquez sur **Add (Ajouter)**, puis configurez les options dans l'onglet **General (Général)**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :

   - **Interface** : ethernet1/7
   - **Adresse IP locale** : 192.168.210.26/24
   - **Type d'adresse IP/Adresse IP de l'homologue** : statique/192.168.210.120
   - **Clés prépartagées** : saisissez une valeur
   - **Local identification (Identification locale)** : aucune ; l'adresse IP locale sera utilisée comme valeur d'identification locale.
   - La configuration de l'homologue VPN B est la suivante :
   - **Interface** : ethernet1/11
   - **Local IP Address (Adresse IP locale)** : 192.168.210.120/24
   - **Type d'adresse IP/Adresse IP de l'homologue** : statique/192.168.210.26
   - **Clés prépartagées** : saisissez la même valeur que sur l'homologue A
   - **Local identification (Identification locale)** : aucune
3. Sélectionnez **Options de phase 1 avancées**, puis le profil crypto IKE créé précédemment à utiliser pour la phase 1 du protocole IKE.

**STEP 6 |** Configurez le tunnel IPSec.

1. Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)**.
2. Cliquez sur **Add (Ajouter)**, puis configurez les options dans l'onglet **General (Général)**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :

   - **Tunnel Interface (Interface de tunnel)** : tunnel.10
   - **Type** : clé automatique
   - **IKE Gateway (Passerelle IKE)** : sélectionnez la passerelle IKE définie ci-dessus
   - **IPSec Crypto Profile (Profil crypto IPSec)** : sélectionnez le profil crypto IPSec défini à l'étape 4.

   La configuration de l'homologue VPN B est la suivante :

   - **Tunnel Interface (Interface de tunnel)** : tunnel.11
   - **Type** : clé automatique
   - **IKE Gateway (Passerelle IKE)** : sélectionnez la passerelle IKE définie ci-dessus
   - **IPSec Crypto Profile (Profil crypto IPSec)** : sélectionnez le profil crypto IPSec défini à l'étape 4.
3. (Facultatif) Sélectionnez **Show Advanced Options (Afficher les options avancées)**, puis **Tunnel Monitor (Surveillance des tunnels)** et spécifiez une adresse IP de destination à laquelle envoyer une requête ping pour vérifier la connexion. Généralement, l'adresse IP de l'interface de tunnel de l'homologue VPN est utilisée.
4. (Facultatif) Pour définir l'action en cas d'échec de la connexion, reportez-vous à la section Définition d'un profil de surveillance de tunnel.

**STEP 7 |** Créez des politiques pour autoriser le trafic entre les sites (sous-réseaux).

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
2. Créez des règles pour autoriser le trafic provenant d'adresses IP source et de destination spécifiées entre la zone non approuvée et la zone vpn-tun.

**STEP 8 |** Enregistrez toutes les modifications de configuration en attente.

Cliquez sur **Commit (Valider)**.

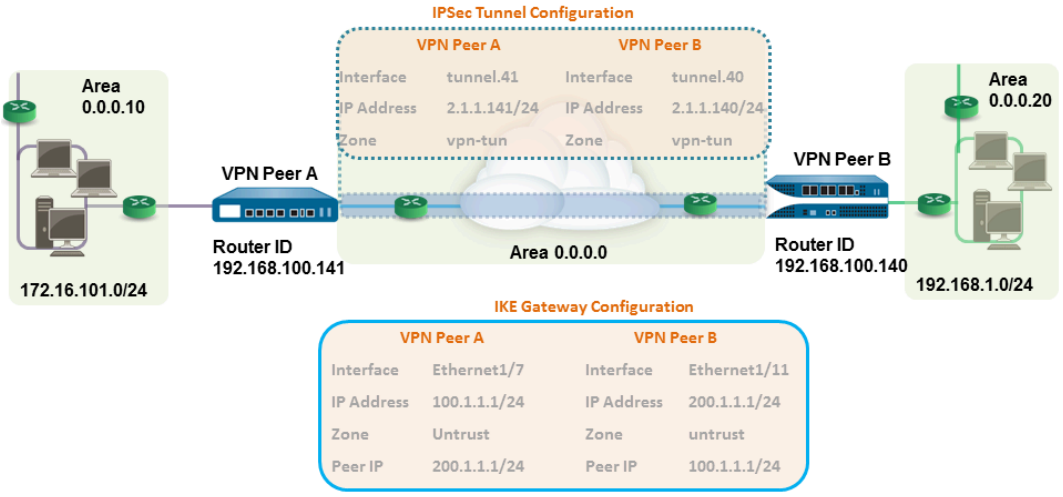
**STEP 9 |** Test de la connexion du VPN.

Reportez-vous également à la section Affichage de l'état des tunnels.

## VPN de site à site avec OSPF

Dans cet exemple, chaque site utilise OSPF pour le routage dynamique du trafic. L'adresse IP du tunnel sur chaque homologue VPN est affectée de manière statique et sert de saut suivant pour acheminer le trafic entre les deux sites.




**STEP 1 |** Configurez les interfaces de couche 3 sur chaque pare-feu.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** et choisissez l'interface que vous souhaitez configurer pour le réseau privé virtuel.
2. Sélectionnez **Layer3 (Couche 3)** dans la liste **Interface Type (Type d'interface)**.
3. Dans l'onglet **Config (Configuration)**, sélectionnez la **Security Zone (Zone de sécurité)** à laquelle appartient l'interface :
   - L'interface doit être accessible depuis une zone en dehors de votre réseau approuvé. Envisagez de créer une zone VPN dédiée pour améliorer la visibilité et le contrôle de votre trafic VPN.
   - Si vous n'avez pas encore créé de zone, sélectionnez **New Zone (Nouvelle zone)** dans la liste **Security Zone (Zone de sécurité)**, donnez un **Name (Nom)** à la zone et cliquez sur **OK (OK)**.
4. Sélectionnez le **Virtual Router (Routeur virtuel)** à utiliser.
5. Pour assigner une adresse IP à l'interface, cliquez sur l'onglet **IPv4**, puis sur **Add (Ajouter)** dans la section IP et saisissez l'adresse IP, ainsi que le masque réseau à assigner à l'interface, par exemple : 192.168.210.26/24.
6. Pour enregistrer la configuration de l'interface, cliquez sur **OK**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :

   - **Interface** : ethernet1/7
   - **Security Zone (Zone de sécurité)** : non approuvée
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** (IPv4) : 100.1.1.1/24

   La configuration de l'homologue VPN B est la suivante :

   - **Interface** : ethernet1/11
   - **Security Zone (Zone de sécurité)** : non approuvée
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** (IPv4) : 200.1.1.1/24

**STEP 2 |** Créez une interface de tunnel et associez-la à un routeur virtuel et une zone de sécurité.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Tunnel** et cliquez sur **Add (Ajouter)**.
2. Dans le champ **Interface Name (Nom de l'interface)**, spécifiez un suffixe numérique, tel que **.11**.
3. Dans l'onglet **Config (Configuration)**, développez la liste **Security Zone (Zone de sécurité)** pour définir la zone de la manière suivante :
   - Pour utiliser votre zone approuvée comme point de terminaison du tunnel, sélectionnez la zone.
   - (Recommandé) Pour créer une zone séparée pour la terminaison du tunnel VPN, cliquez sur **New Zone (Nouvelle zone)**. Dans la boîte de dialogue, donnez un **Name (Nom)** à la nouvelle zone (par exemple, vpn-tun), puis cliquez sur **OK**.
4. Sélectionnez le **Virtual Router (Routeur virtuel)**.
5. Affectez une adresse IP à l'interface de tunnel, sélectionnez l'onglet **IPv4** ou **IPv6** puis cliquez sur **Ajouter** dans la section IP et saisissez l'adresse IP, ainsi que le préfixe/masque réseau à affecter à l'interface, par exemple, 172.19.9.2/24.

   Cette adresse IP sera utilisée comme adresse IP de saut suivant pour acheminer le trafic vers le tunnel et peut également être utilisée pour surveiller l'état du tunnel.
6. Pour enregistrer la configuration de l'interface, cliquez sur **OK**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :
   - **Interface** : tunnel.41
   - **Zone de sécurité** : vpn_tun
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** (IPv4) : 2.1.1.141/24

   La configuration de l'homologue VPN B est la suivante :
   - **Interface** (Interface) : tunnel.40
   - **Zone de sécurité** : vpn_tun
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** (IPv4) : 2.1.1.140/24

**STEP 3 |** Configurez les profils crypto (profils crypto IKE pour la phase 1 et profil crypto IPSec pour la phase 2).

Effectuez cette tâche sur les deux homologues et assurez-vous de définir des valeurs identiques.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Crypto (Crypto IKE)**. Dans cet exemple, le profil par défaut est utilisé.
2. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IPSec Crypto (Crypto IPSec)**. Dans cet exemple, le profil par défaut est utilisé.

**STEP 4 |** Définissez la configuration OSPF sur le routeur virtuel et associez les zones OSPF aux interfaces appropriées sur le pare-feu.

Pour plus d'informations sur les options OSPF disponibles sur le pare-feu, reportez-vous à la section Configuration d'OSPF.

Utilisez Diffusion comme type de liaison lorsque plus de deux routeurs OSPF ont besoin d'échanger des informations de routage.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, puis choisissez le routeur par défaut ou ajoutez-en un nouveau.
2. Sélectionnez **OSPF** (pour IPv4) ou **OSPFv3** (pour IPv6), puis **Enable (Activer)**.
3. Dans cet exemple, la configuration OSPF de l'homologue VPN A est la suivante :
   - **ID de routeur** : 192.168.100.141
   - **ID de zone** : 0.0.0.0 qui est affecté à l'interface tunnel.1 avec le type de liaison p2p
   - **ID de zone** : 0.0.0.10 qui est affecté à l'interface Ethernet1/1 avec le type de liaison Diffusion

   La configuration OSPF de l'homologue VPN B est la suivante :
   - **ID de routeur** : 192.168.100.140
   - **ID de zone** : 0.0.0.0 qui est affecté à l'interface tunnel.1 avec le type de liaison p2p
   - **ID de zone** : 0.0.0.20 qui est affecté à l'interface Ethernet1/15 avec le type de liaison : Diffusion

**STEP 5 |** Configurez la passerelle IKE.

Cet exemple utilise des adresses IP statiques pour les deux homologues VPN. Généralement, le siège social utilise une adresse IP configurée de manière statique et la succursale peut

disposer d'une adresse IP dynamique ; les adresses IP dynamiques ne sont pas bien adaptées à la configuration de services stables tels que les VPN.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Gateway (Passerelle IKE)**.
2. Cliquez sur **Add (Ajouter)**, puis configurez les options dans l'onglet **General (Général)**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :

   - **Interface** : ethernet1/7
   - **Local IP Address (Adresse IP locale)** : 100.1.1.1/24
   - **Peer IP address (Adresse IP de l'homologue)** : 200.1.1.1/24
   - **Clés prépartagées** : saisissez une valeur

   La configuration de l'homologue VPN B est la suivante :

   - **Interface** : ethernet1/11
   - **Local IP Address** (Adresse IP locale) : 200.1.1.1/24
   - **Peer IP address** (Adresse IP de l'homologue) : 100.1.1.1/24
   - **Clés prépartagées** : saisissez la même valeur que sur l'homologue A
3. Sélectionnez le profil crypto IKE créé précédemment à utiliser pour la phase 1 du protocole IKE.

**STEP 6 |** Configurez le tunnel IPSec.

1. Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)**.
2. Cliquez sur **Add (Ajouter)**, puis configurez les options dans l'onglet **General (Général)**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :

   - **Tunnel Interface (Interface de tunnel)** : tunnel.41
   - **Type** : clé automatique
   - **IKE Gateway (Passerelle IKE)** : sélectionnez la passerelle IKE définie ci-dessus
   - **Profil crypto IPSec** : sélectionnez la passerelle IKE définie ci-dessus

   La configuration de l'homologue VPN B est la suivante :

   - **Tunnel Interface (Interface de tunnel)** : tunnel.40
   - **Type** : clé automatique
   - **IKE Gateway (Passerelle IKE)** : sélectionnez la passerelle IKE définie ci-dessus
   - **Profil crypto IPSec** : sélectionnez la passerelle IKE définie ci-dessus
3. Sélectionnez **Afficher les options avancées**, puis **Surveillance des tunnels** et spécifiez une adresse IP de destination à laquelle envoyer une requête ping pour vérifier la connexion.
4. Pour définir l'action en cas d'échec de la connexion, reportez-vous à la section Définition d'un profil de surveillance de tunnel.

**STEP 7 |** Créez des politiques pour autoriser le trafic entre les sites (sous-réseaux).

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
2. Créez des règles pour autoriser le trafic provenant d'adresses IP source et de destination spécifiées entre la zone non approuvée et la zone vpn-tun.

**STEP 8 |** Vérifiez les itinéraires et les éléments adjacents OSPF à partir de la CLI.

Vérifiez que les deux pare-feu peuvent se voir comme voisins, ainsi que toutes les informations d'état. Vérifiez également l'adresse IP de l'interface de tunnel de l'homologue VPN et l'ID du routeur OSPF. Utilisez les commandes CLI suivantes sur chaque homologue VPN :

- **show routing protocol ospf neighbor**

```
admin@FW-A> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.140
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.140
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no

admin@FW-B> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.141
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.141
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```

- **show routing route type ospf**

```
admin@FW-A> show routing route type ospf

flags: A:active, ?:loose, C:connect, H:host, S:static, ~:internal, R:rip, O:ospf, B:bgp,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2


VIRTUAL ROUTER: vr1 (id 1)
  ==========
destination             nexthop             metric flags      age   interface          next-AS
2.1.1.0/24              0.0.0.0                 10   Oi       6760  tunnel.41
172.16.101.0/24         0.0.0.0                 10   Oi       6854  ethernet1/1
192.168.1.0/24          2.1.1.140               20 A Oo       6754  tunnel.40
total routes shown: 3
    admin@FW-B> show routing route type ospf

    flags: A:active, C:connect, H:host, S:static, R:rip, O:ospf,
           Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2


    VIRTUAL ROUTER: vr1 (id 1)
      ==========
    destination             nexthop             metric flags      age   interface
    2.1.1.0/24              0.0.0.0                 10   Oi       20033 tunnel.40
    172.16.101.0/24         2.1.1.141               20   AOo      6896  tunnel.40
    192.168.1.0/24          0.0.0.0                 10   Oi       8058  ethernet1/15
    total routes shown: 3
```

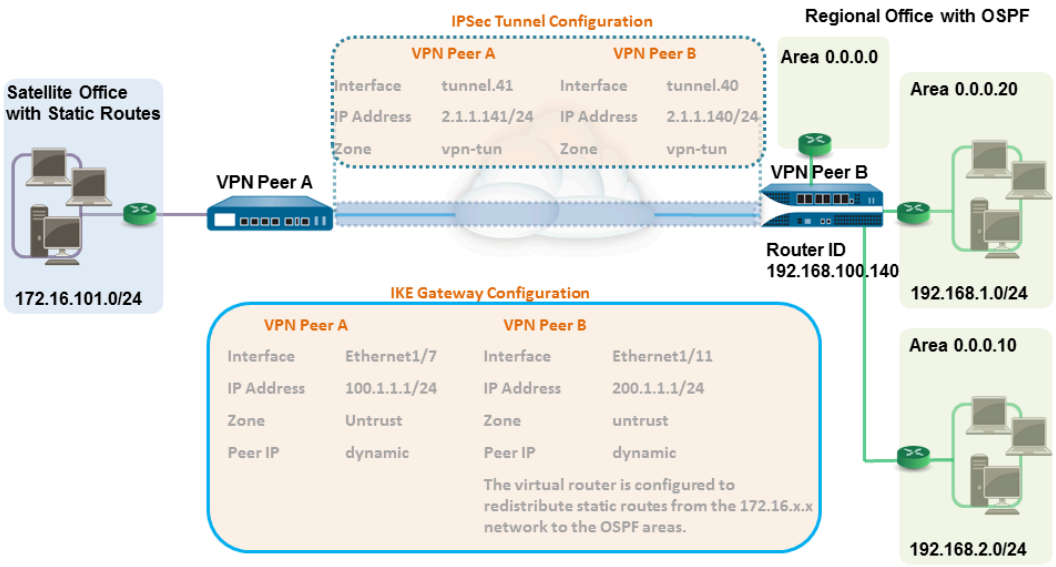
**STEP 9 |** Test de la connexion du VPN.

Reportez-vous aux sections Configuration de la surveillance des tunnels et Affichage de l'état des tunnels.

# VPN de site à site avec routage statique et dynamique

Dans cet exemple, un site utilise des itinéraires statiques et l'autre utilise OSPF. Lorsque le protocole de routage n'est pas identique sur les deux sites, l'interface de tunnel sur chaque pare-feu doit être configurée avec une adresse IP statique. Ensuite, pour permettre l'échange des informations de routage, le pare-feu qui participe au processus de routage statique et dynamique doit être configuré avec un profil de redistribution. La configuration du profil de redistribution permet au routeur virtuel de redistribuer et de filtrer les itinéraires entre les protocoles (itinéraires statiques, itinéraires connectés et hôtes) du système statique autonome au système OSPF autonome. Sans ce profil de redistribution, chaque protocole fonctionne de manière autonome et n'échange aucune information d'itinéraire avec les autres protocoles exécutés sur le même routeur virtuel.

Dans cet exemple, le bureau satellite dispose d'itinéraires statiques et tout le trafic destiné au réseau 192.168.x.x est acheminé vers l'interface tunnel.41. Le routeur virtuel sur l'homologue VPN B participe au processus de routage statique et dynamique ; il est configuré avec un profil de redistribution afin de propager (exporter) les itinéraires statiques sur le système OSPF autonome.



**STEP 1 |** Configurez les interfaces de couche 3 sur chaque pare-feu.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** et choisissez l'interface que vous souhaitez configurer pour le réseau privé virtuel.
2. Sélectionnez **Layer3 (Couche 3)** comme **Interface Type (Type de liaison)**.
3. Dans l'onglet **Config (Configuration)**, sélectionnez la **Security Zone (Zone de sécurité)** à laquelle appartient l'interface :
   - L'interface doit être accessible depuis une zone en dehors de votre réseau approuvé. Envisagez de créer une zone VPN dédiée pour améliorer la visibilité et le contrôle de votre trafic VPN.
   - Si vous n'avez pas encore créé de zone, sélectionnez **New Zone (Nouvelle zone)** dans la **Security Zone (Zone de sécurité)**, donnez un **Name (Nom)** à la zone et cliquez sur **OK (OK)**.
4. Sélectionnez le **Virtual Router (Routeur virtuel)** à utiliser.
5. Pour assigner une adresse IP à l'interface, cliquez sur l'onglet **IPv4**, puis sur **Add (Ajouter)** dans la section IP et saisissez l'adresse IP, ainsi que le masque réseau à assigner à l'interface, par exemple : 192.168.210.26/24.
6. Pour enregistrer la configuration de l'interface, cliquez sur **OK**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :

   - **Interface** : ethernet1/7
   - **Security Zone (Zone de sécurité)** : non approuvée
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** (IPv4) : 100.1.1.1/24

   La configuration de l'homologue VPN B est la suivante :

   - **Interface** : ethernet1/11
   - **Security Zone (Zone de sécurité)** : non approuvée
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** (IPv4) : 200.1.1.1/24

**STEP 2 |** Configurez les profils crypto (profils crypto IKE pour la phase 1 et profil crypto IPSec pour la phase 2).

Effectuez cette tâche sur les deux homologues et assurez-vous de définir des valeurs identiques.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Crypto (Crypto IKE)**. Dans cet exemple, le profil par défaut est utilisé.
2. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IPSec Crypto (Crypto IPSec)**. Dans cet exemple, le profil par défaut est utilisé.

**STEP 3 |** Configurez la passerelle IKE.

Grâce aux clés prépartagées, pour renforcer l'authentification lors de la configuration du tunnel IKE de phase 1, vous pouvez configurer les attributs d'identification locale et de

l'homologue, ainsi qu'une valeur correspondante mise en correspondance dans le processus de négociation IKE.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IKE Gateway (Passerelle IKE)**.
2. Cliquez sur **Add (Ajouter)**, puis configurez les options dans l'onglet **General (Général)**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :

   - **Interface** : ethernet1/7
   - **Local IP Address (Adresse IP locale)** : 100.1.1.1/24
   - **Type d'adresse IP de l'homologue** : dynamique
   - **Clés prépartagées** : saisissez une valeur
   - **Identification locale** : sélectionnez **Nom de domaine complet (nom d'hôte)** et saisissez la valeur pour l'homologue VPN A.
   - **Identification de l'homologue** : sélectionnez **Nom de domaine complet (nom d'hôte)** et saisissez la valeur pour l'homologue VPN B.

   La configuration de l'homologue VPN B est la suivante :

   - **Interface** : ethernet1/11
   - **Local IP Address** (Adresse IP locale) : 200.1.1.1/24
   - **Type d'adresse IP de l'homologue** : dynamique
   - **Clés prépartagées** : saisissez la même valeur que sur l'homologue A
   - **Identification locale** : sélectionnez **Nom de domaine complet (nom d'hôte)** et saisissez la valeur pour l'homologue VPN B.
   - **Identification de l'homologue** : sélectionnez **Nom de domaine complet (nom d'hôte)** et saisissez la valeur pour l'homologue VPN A.
3. Sélectionnez le profil crypto IKE créé précédemment à utiliser pour la phase 1 du protocole IKE.

**STEP 4 |** Créez une interface de tunnel et associez-la à un routeur virtuel et une zone de sécurité.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Tunnel** et cliquez sur **Add (Ajouter)**.
2. Dans le champ **Nom de l'interface**, spécifiez un suffixe numérique, tel que **.41**.
3. Dans l'onglet **Config (Configuration)**, développez la liste **Security Zone (Zone de sécurité)** pour définir la zone de la manière suivante :
   - Pour utiliser votre zone approuvée comme point de terminaison du tunnel, sélectionnez la zone.
   - (Recommandé) Pour créer une zone séparée pour la terminaison du tunnel VPN, cliquez sur **New Zone (Nouvelle zone)**. Dans la boîte de dialogue, donnez un **Name (Nom)** à la nouvelle zone (par exemple, ***vpn-tun***), puis cliquez sur **OK**.
4. Sélectionnez le **Virtual Router (Routeur virtuel)**.
5. Affectez une adresse IP à l'interface de tunnel, sélectionnez l'onglet **IPv4** ou **IPv6** puis cliquez sur **Ajouter** dans la section IP et saisissez l'adresse IP, ainsi que le préfixe/masque réseau à affecter à l'interface, par exemple, 172.19.9.2/24.

   Cette adresse IP sera utilisée pour acheminer le trafic vers le tunnel et Surveiller l'état du tunnel.
6. Pour enregistrer la configuration de l'interface, cliquez sur **OK**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :
   - **Interface** : tunnel.41
   - **Zone de sécurité** : vpn_tun
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** (IPv4) : 2.1.1.141/24

   La configuration de l'homologue VPN B est la suivante :
   - **Interface** : tunnel.42
   - **Zone de sécurité** : vpn_tun
   - **Virtual Router (Routeur virtuel)** : par défaut
   - **IPv4** (IPv4) : 2.1.1.140/24

**STEP 5 |** Spécifiez l'interface qui acheminera le trafic vers une destination sur le réseau 192.168.x.x.

1. Sélectionnez le routeur virtuel sur l'homologue VPN A.
2. Sélectionnez **Static Routes (Itinéraires statiques)**, puis cliquez sur **Add (Ajouter)** pour ajouter tunnel.41 comme **Interface** pour acheminer le trafic vers une **Destination** sur le réseau 192.168.x.x.

**STEP 6 |** Définissez l'itinéraire statique et la configuration OSPF sur le routeur virtuel, puis associez les zones OSPF aux interfaces appropriées sur le pare-feu.

1. Sur l'homologue VPN B, sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, puis choisissez le routeur par défaut ou ajoutez-en un nouveau.
2. Sélectionnez **Static Routes (Itinéraires statiques)** et cliquez sur **Add (Ajouter)** pour ajouter l'adresse IP comme saut suivant du trafic sur le réseau 172.168.x.x.

   Affectez la mesure d'itinéraire souhaitée ; plus la valeur est faible, plus la priorité de sélection de l'itinéraire dans la table de transfert est élevée.
3. Sélectionnez **OSPF** (pour IPv4) ou **OSPFv3** (pour IPv6), puis **Enable (Activer)**.
4. Dans cet exemple, la configuration OSPF de l'homologue VPN B est la suivante :
   - Router ID (ID de routeur) : 192.168.100.140
   - Area ID (ID de zone) : 0.0.0.0 qui est affecté à l'interface Ethernet1/12 avec le type de liaison Diffusion
   - Area ID (ID de zone) : 0.0.0.10 qui est affecté à l'interface Ethernet1/1 avec le type de liaison Diffusion
   - Area ID (ID de zone) : 0.0.0.20 qui est affecté à l'interface Ethernet1/15 avec le type de liaison Diffusion

**STEP 7 |** Créez un profil de redistribution pour injecter les itinéraires statiques dans le système OSPF autonome.

1. Créez un profil de redistribution sur l'homologue VPN B.
   1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, puis choisissez le routeur utilisé ci-dessus.
   2. Sélectionnez **Redistribution Profiles (Profils de redistribution)** et cliquez sur **Add (Ajouter)**.
   3. Donnez un nom au profil, puis sélectionnez **Redistribution** et affectez-lui une valeur de **priorité**. Si vous avez configuré plusieurs profils, le profil dont la valeur de priorité est la plus faible est d'abord mis en correspondance.
   4. Définissez le **Source Type (Type de source)** comme **static (statique)** et cliquez sur **OK**. L'itinéraire statique que vous avez défini à l'étape 6 sera utilisé pour la redistribution.
2. Injectez les itinéraires statiques dans le système OSPF.
   1. Sélectionnez **OSPF** > **Export Rules (Exporter les règles)** (pour IPv4) ou **OSPFv3** > **Export Rules (Exporter les règles)** (pour IPv6).
   2. Cliquez sur **Ajouter**, puis sélectionnez le profil de redistribution que vous venez de créer.
   3. Déterminez la manière dont les itinéraires externes sont injectés dans le système OSPF. L'option par défaut, **Ext2**, calcule le coût total de l'itinéraire uniquement à l'aide des mesures externes. Pour utiliser des mesures OSPF internes et externes, sélectionnez **Ext1**.
   4. Affectez une **Metric (Mesure)** (valeur de coût) aux itinéraires injectés dans le système OSPF. Cette option vous permet de modifier la mesure de l'itinéraire lorsqu'il est injecté dans le système OSPF.
   5. Cliquez sur **OK**.

**STEP 8 |** Configurez le tunnel IPSec.

1. Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)**.
2. Cliquez sur **Add (Ajouter)**, puis configurez les options dans l'onglet **General (Général)**.

   Dans cet exemple, la configuration de l'homologue VPN A est la suivante :

   - **Tunnel Interface (Interface de tunnel)** : tunnel.41
   - **Type** : clé automatique
   - **IKE Gateway (Passerelle IKE)** : sélectionnez la passerelle IKE définie ci-dessus
   - **Profil crypto IPSec** : sélectionnez la passerelle IKE définie ci-dessus

   La configuration de l'homologue VPN B est la suivante :

   - **Tunnel Interface (Interface de tunnel)** : tunnel.40
   - **Type** : clé automatique
   - **IKE Gateway (Passerelle IKE)** : sélectionnez la passerelle IKE définie ci-dessus
   - **Profil crypto IPSec** : sélectionnez la passerelle IKE définie ci-dessus
3. Sélectionnez **Afficher les options avancées**, puis **Surveillance des tunnels** et spécifiez une adresse IP de destination à laquelle envoyer une requête ping pour vérifier la connexion.
4. Pour définir l'action en cas d'échec de la connexion, reportez-vous à la section Définition d'un profil de surveillance de tunnel.

**STEP 9 |** Créez des politiques pour autoriser le trafic entre les sites (sous-réseaux).

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
2. Créez des règles pour autoriser le trafic provenant d'adresses IP source et de destination spécifiées entre la zone non approuvée et la zone vpn-tun.

**STEP 10 |** Vérifiez les itinéraires et les éléments adjacents OSPF à partir de la CLI.

Vérifiez que les deux pare-feu peuvent se voir comme voisins, ainsi que toutes les informations d'état. Vérifiez également l'adresse IP de l'interface de tunnel de l'homologue VPN et l'ID du routeur OSPF. Utilisez les commandes CLI suivantes sur chaque homologue VPN :

- **show routing protocol ospf neighbor**

```
admin@FW-A> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.140
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.140
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no

admin@FW-B> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.141
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.141
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```

- **show routing route**

Voici un exemple de résultat sur chaque homologue VPN :

```
VPN PeerA

destination             next hop        metric  flags   age     interface       next-AS
192.168.1.0/24          2.1.1.141       20      A S             tunnel.41
192.168.2.0/24          2.1.1.141       20      A S             tunnel.41
172.16.101.0/24         0.0.0.0         1       A H             ethernet1/1
2.1.1.140/24            2.1.1.141       20      A S             tunnel.41

VPN PeerB

destination             next hop        metric  flags   age     interface       next-AS
192.168.1.0/24          0.0.0.0         10      A Oo            ethernet1/1
192.168.2.0/24          0.0.0.0         10      A Oo            ethernet1/15
172.16.101.0/24         2.1.1.140       20      A H             tunnel.40
2.1.1.141/24            2.1.1.140       10      A C             tunnel.40
```

**STEP 11 |** Test de la connexion du VPN.

Reportez-vous aux sections Configuration de la surveillance des tunnels et Affichage de l'état des tunnels.

# VPN à grande échelle (LSVPN)

La fonctionnalité Large Scale VPN (VPN à grande échelle ; LSVPN) GlobalProtect sur le pare-feu de dernière génération Palo Alto Networks simplifie le déploiement des VPN en étoile traditionnels, vous permettant ainsi de déployer rapidement des réseaux d'entreprise dans plusieurs filiales avec une configuration minime sur les ***satellites*** distants. Cette solution utilise des certificats pour l'authentification du pare-feu et IPSec pour la sécurisation des données.

LSVPN permet d'obtenir des VPN site à site entre des pare-feu Palo Alto Networks. Pour configurer un VPN site à site entre un pare-feu Palo Alto Networks et un autre périphérique, reportez-vous à la section VPNs

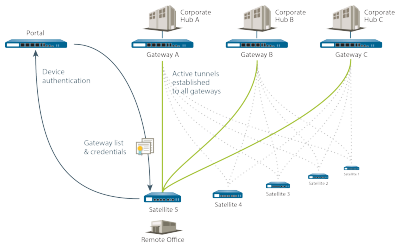
Les rubriques suivantes décrivent les composants du LSVPN et comment les configurer afin d'activer des services de VPN site à site entre des pare-feu Palo Alto Networks :

# Présentation du LSVPN

GlobalProtect propose une infrastructure complète de gestion de l'accès sécurisé aux ressources de l'entreprise à partir de sites distants. L'infrastructure inclut les composants suivants :

- **Portail GlobalProtect** : fournit les fonctions de gestion de l'infrastructure de votre LSVPN GlobalProtect. Chaque satellite prenant part au LSVPN GlobalProtect reçoit des informations de configuration du portail, notamment des informations de configuration permettant aux satellites (les branches) de se connecter aux passerelles (le cœur). Vous configurez le portail sur une interface d'un quelconque pare-feu de dernière génération Palo Alto Networks.
- **Passerelles GlobalProtect** : un pare-feu Palo Alto Networks incluant l'extrémité du tunnel pour les connexions satellites. Les ressources auxquelles les satellites accèdent sont protégées par une politique de sécurité sur la passerelle. Le portail et la passerelle ne doivent pas nécessairement être distincts, un même pare-feu peut servir à la fois de portail et de passerelle.
- **Satellite GlobalProtect** : un pare-feu Palo Alto Networks sur un site distant formant des tunnels IPSec avec la ou les passerelles dans votre ou vos filiales d'entreprise afin de sécuriser l'accès aux ressources centralisées. La configuration sur le pare-feu satellite est minime, vous permettant ainsi de faire évoluer rapidement et facilement votre VPN à mesure que vous ajoutez de nouveaux sites.

Le diagramme suivant illustre comment les composants du LSVPN GlobalProtect fonctionnent ensemble.



# Création d'interfaces et de zones pour le LSVPN

Vous devez configurer les interfaces et zones suivantes pour votre infrastructure LSVPN :

- **Portail GlobalProtect** : nécessite une interface de Couche 3 à laquelle les satellites GlobalProtect se connectent. Si le portail et la passerelle se trouvent sur le même pare-feu, ils peuvent utiliser la même interface. Le portail doit se trouver dans une zone accessible depuis vos filiales.
- **Passerelles GlobalProtect** : nécessitent trois interfaces : une interface de couche 3 dans la zone accessible aux satellites distants, une interface interne dans la zone approuvée qui est connectée aux ressources protégées, et une interface de tunnel logique pour la terminaison des tunnels VPN à partir des satellites. Contrairement à d'autres solutions VPN DE site à site, la passerelle GlobalProtect ne nécessite qu'une seule interface de tunnel, qu'elle utilisera pour les connexions de tunnel avec tous vos satellites distants (point-à-multipoint). Si vous envisagez d'utiliser le routage dynamique, vous devez affecter une adresse IP à l'interface de tunnel. GlobalProtect prend en charge l'adressage IPv6 et IPv4 pour l'Interface de tunnel.
- **Satellites GlobalProtect** : nécessitent une seule interface de tunnel pour l'établissement d'un VPN avec les passerelles distantes (jusqu'à 25 passerelles maximum). Si vous envisagez d'utiliser le routage dynamique, vous devez affecter une adresse IP à l'interface de tunnel. GlobalProtect prend en charge l'adressage IPv6 et IPv4 pour l'Interface de tunnel.

Pour plus d'informations sur les portails, passerelles et satellites, reportez-vous à la section Présentation du LSVPN.

**STEP 1 |** Configurez une interface de couche 3.

Le portail, et chaque passerelle et satellite, nécessitent tous une interface de couche 3 pour activer le trafic à acheminer entre les sites.

Si la passerelle et le portail se trouvent sur le même pare-feu, vous pouvez utiliser une seule interface pour les deux composants.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)** et choisissez l'interface que vous voulez configurer pour le LSVPN GlobalProtect.
2. Sélectionnez **Layer3 (Couche 3)** dans la liste déroulante **Interface Type (Type d'interface)**.
3. Dans l'onglet **Config (Configuration)**, sélectionnez la **Security Zone (Zone de sécurité)** à laquelle appartient l'interface :
   - L'interface doit être accessible depuis une zone en dehors de votre réseau approuvé. Envisagez de créer une zone VPN dédiée pour améliorer la visibilité et le contrôle de votre trafic VPN.
   - Si vous n'avez pas encore créé de zone, sélectionnez **New Zone (Nouvelle zone)** dans la liste déroulante **Security Zone (Zone de sécurité)**, donnez un **Name (Nom)** à la zone et cliquez sur **OK (OK)**.
4. Sélectionnez le **Virtual Router (Routeur virtuel)** à utiliser.
5. Affectez une adresse IP à l'interface :
   - Pour une adresse IPv4, sélectionnez **IPv4** et **Add (Ajouter)** l'adresse IP et le masque de réseau à affecter à l'interface, par exemple 203.0.11.100/24.
   - Pour une adresse IPv6, sélectionnez **IPv6**, **Enable IPv6 on the interface (Activez IPv6 sur l'interface)**, et **Add (Ajoutez)** l'adresse IP et le masque réseau à affecter à l'interface, par exemple 2001:1890:12f2:11::10.1.8.160/80.
6. Pour enregistrer la configuration de l'interface, cliquez sur **OK**.

**STEP 2 |** Sur le ou les pare-feu hébergeant la ou les passerelles GlobalProtect, configurez l'interface de tunnel logique qui terminera les tunnels VPN établis par les satellites GlobalProtect.

*Les adresses IP ne sont pas requises sur l'interface de tunnel, sauf si vous envisagez d'utiliser le routage dynamique. L'affectation d'une adresse IP à l'interface de tunnel peut toutefois être utile pour le dépannage de problèmes de connectivité.*

*Veillez à activer User-ID dans la zone dans laquelle les tunnels VPN se terminent.*

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Tunnel** et cliquez sur **Add (Ajouter)**.
2. Dans le champ **Interface Name (Nom de l'interface)**, spécifiez un suffixe numérique, tel que **.2**.
3. Dans l'onglet **Config (Configuration)**, développez la liste déroulante **Security Zone (Zone de sécurité)** pour définir la zone de la manière suivante :
   - Pour utiliser votre zone approuvée comme point de terminaison du tunnel, sélectionnez la zone dans la liste déroulante.
   - (Recommandé) Pour créer une zone séparée pour la terminaison du tunnel VPN, cliquez sur **New Zone (Nouvelle zone)**. Dans la boîte de dialogue Zone, donnez un

**Name (Nom)** à la nouvelle zone (par exemple, *lsvpn-tun*), cochez la case **Enable User Identification (Activer l'identification des utilisateurs)**, puis cliquez sur **OK (OK)**.

4. Sélectionnez le **Virtual Router (Routeur virtuel)**.
5. (Facultatif) Pour attribuer une adresse IP à l'interface du tunnel :
   - Pour une adresse IPv4, sélectionnez **IPv4** et **Add (Ajouter)** l'adresse IP et le masque de réseau à affecter à l'interface, par exemple 203.0.11.100/24.
   - Pour une adresse IPv6, sélectionnez **IPv6**, **Enable IPv6 on the interface (Activez IPv6 sur l'interface)**, et **Add (Ajoutez)** l'adresse IP et le masque réseau à affecter à l'interface, par exemple 2001:1890:12f2:11::10.1.8.160/80.
6. Pour enregistrer la configuration de l'interface, cliquez sur **OK**.

**STEP 3 |** Si vous avez créé une zone distincte pour le point de terminaison du tunnel de connexions VPN, créez une politique de sécurité afin d'autoriser le flux de trafic entre la zone VPN et votre zone de confiance.

Par exemple, une règle de politique autorise le trafic entre la zone ***lsvpn-tun*** et la zone ***L3-Trust***.

**STEP 4 |** Validez vos modifications.

Cliquez sur **Commit (Valider)**.

# Activation de SSL entre des composants du LSVPN GlobalProtect

Toutes les interactions entre les composants GlobalProtect se produisent sur une connexion SSL/TLS. Vous devez donc générer et/ou installer les certificats nécessaires avant de configurer chaque composant afin de pouvoir faire référence au ou aux certificats et/ou profils de certificat appropriés lors de la configuration de chaque composant. Les sections suivantes décrivent les méthodes de déploiement de certificat prises en charge, les descriptions et les directives relatives aux divers certificats GlobalProtect, et fournissent des instructions sur la génération et le déploiement des certificats nécessaires :

- À propos du déploiement de certificats
- Déploiement de certificats de serveur sur les composants du LSVPN GlobalProtect
- Déploiement des certificats client vers les satellites GlobalProtect à l'aide de SCEP

## À propos du déploiement de certificats

Deux approches de base de déploiement des certificats pour le LSVPN GlobalProtect sont possibles :

- **Certificate Authority (autorité de certification - CA) d'entreprise** : si vous disposez déjà de votre propre autorité de certification d'entreprise, vous pouvez utiliser la CA interne pour générer un certificat CA intermédiaire afin de permettre au portail GlobalProtect de générer des certificats vers les passerelles et satellites GlobalProtect. Vous pouvez également configurer le portail GlobalProtect pour qu'il agisse en tant que client Simple Certificate Enrollment Protocol (protocole de recrutement de certificat simple ; SCEP) pour générer des certificats client aux satellites GlobalProtect.
- **Certificats auto-signés** : vous pouvez générer un certificat CA racine auto-signé sur le pare-feu et l'utiliser pour générer des certificats de serveur du portail, des passerelles et des satellites. Lors de l'utilisation de certificats CA racine auto-signés, il est recommandé de créer un certificat CA racine auto-signé sur le portail et de l'utiliser pour générer des certificats de serveur pour les passerelles et les satellites. La clé privée utilisée pour la signature du certificat reste ainsi sur le portail.

## Déploiement de certificats de serveur sur les composants du LSVPN GlobalProtect

Les composants du LSVPN GlobalProtect utilisent SSL/TLS pour s'authentifier mutuellement. Avant de déployer le LSVPN, vous devez affecter un profil de service SSL/TLS au portail et à chaque passerelle. Le profil spécifie le certificat de serveur et les versions TLS autorisées pour la communication avec les satellites. Vous n'avez pas besoin de créer de profils de service SSL/TLS pour les satellites, car le portail génère un certificat de serveur pour chaque satellite lors de la première connexion, dans le cadre du processus d'enregistrement du satellite.

De plus, vous devez importer le certificat de Certificate Authority (autorité de certification ; CA) racine utilisé pour générer les certificats de serveur sur chaque pare-feu que vous envisagez d'héberger comme passerelle ou satellite. Enfin, sur chaque passerelle et satellite prenant part au LSVPN, vous devez configurer un profil de certificat qui leur permettra d'établir une connexion SSL/TLS utilisant l'authentification mutuelle.

Le flux de travail suivant illustre les étapes de déploiement de certificats SSL sur les composants du LSVPN GlobalProtect :

**STEP 1 |** Sur le pare-feu hébergeant le portail GlobalProtect, créez le certificat CA racine pour la signature des certificats des composants GlobalProtect.

Création d'un certificat CA racine auto-signé.

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, puis cliquez sur **Generate (Générer)**.
2. Saisissez un **Certificate Name (Nom de certificat)**, tel que **LSVPN_CA**.
3. Ne sélectionnez pas de valeur dans le champ **Signed By (Signé par)** (ceci indique qu'il est auto-signé).
4. Cochez la case **Certificate Authority (Autorité de certification)**, puis cliquez sur **OK (OK)** pour générer le certificat.

**STEP 2 |** Créez des profils de service SSL/TLS pour le portail et les passerelles GlobalProtect.

Vous devez affecter au portail et à chaque passerelle un profil de service SSL/TLS qui fait référence à un certificat de serveur auto-signé unique.

*Il est recommandé de générer tous les certificats requis sur le portail, afin de ne pas devoir exporter le certificat de signature (avec la clé privée).*

*Si le portail et la passerelle GlobalProtect se trouvent sur la même interface de pare-feu, vous pouvez utiliser le même certificat de serveur pour les deux composants.*

1. Utilisez le CA racine sur le portail pour générer un certificat pour chaque passerelle que vous déploierez :
   1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, puis cliquez sur **Generate (Générer)**.
   2. Saisissez un **Certificate Name (Nom de certificat)**.
   3. Dans le champ **Common Name (Nom commun)**, saisissez le FQDN (recommandé) ou l'adresse IP de l'interface sur laquelle vous envisagez de configurer la passerelle.
   4. Dans le champ **Signed By (Signé par)**, sélectionnez le certificat **LSVPN_CA** que vous venez de créer.
   5. Dans la section Certificate Attributes (Attributs du certificat), cliquez sur **Add (Ajouter)** et définissez les attributs afin de différencier de manière unique la passerelle. Si vous ajoutez un attribut **Host Name (Nom d'hôte)** (qui renseigne le champ SAN du certificat),

il doit correspondre exactement à la valeur que vous avez définie pour le **Common Name (Nom commun)**.

6. **Generate (Générez)** le certificat.

2. Configuration d'un profil de service SSL/TLS pour le portail et chaque passerelle :
   1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion de certificats)** > **SSL/TLS Service Profile (Profil de service SSL/TLS)** et cliquez sur **Add (Ajouter)**.
   2. Saisissez un **Name (Nom)** pour identifier le profil et sélectionnez le **Certificate (Certificat)** de serveur que vous venez de créer pour le portail ou la passerelle.
   3. Définissez la plage de versions TLS (**Min Version (Version min.)** à **Max Version (Version max.)**) autorisée pour la communication avec les satellites, puis cliquez sur **OK (OK)**.

**STEP 3 |** Déployez les certificats de serveur auto-signés sur les passerelles.

***Meilleures pratiques :***

- Exportez les certificats de serveur auto-signés générés par la CA racine du portail et importez-les sur les passerelles.
- Veillez à générer un certificat de serveur unique pour chaque passerelle.
- Le champ Common Name (nom commun - CN) et, le cas échéant, le champ Subject Alternative Name (autre nom de l'objet -SAN) doivent correspondre exactement à l'adresse IP ou au Fully Qualified Domain Name (nom de domaine complet - FQDN) de l'interface sur laquelle vous configurez la passerelle.

1. Sur le portail, sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, sélectionnez le certificat de passerelle que vous souhaitez déployer, puis cliquez sur **Export (Exporter)**.
2. Sélectionnez **Encrypted Private Key and Certificate (PKCS12) (Clé privée et certificat cryptés (PKCS12))** dans la liste déroulante **File Format (Format de fichier)**.
3. Saisissez (et confirmez) une **Passphrase (Phrase secrète)** pour crypter la clé privée associée au certificat, puis cliquez sur **OK (OK)** pour télécharger le fichier PKCS12 sur votre ordinateur.
4. Sur la passerelle, sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, puis cliquez sur **Import (Importer)**.
5. Saisissez un **Certificate Name (Nom de certificat)**.
6. Saisissez le chemin et nommez le **Certificate File (Fichier du certificat)** que vous venez de télécharger du portail, ou cliquez sur **Browse (Parcourir)** pour trouver le fichier.
7. Sélectionnez **Encrypted Private Key and Certificate (PKCS12) (Clé privée cryptée et certificat (PKCS12))** comme **File Format (Format du fichier)**.
8. Saisissez le chemin et nommez le fichier PKCS12 dans le champ **Key File (Fichier de clé)** ou cliquez sur **Browse (Parcourir)** pour le trouver.
9. Saisissez et confirmez la **Passphrase (Phrase secrète)** que vous avez utilisée pour coder la clé privée lorsque vous l'avez exportée depuis le portail, puis cliquez sur **OK (OK)** pour importer le certificat et la clé.

**STEP 4 |** Importez le certificat CA racine utilisé pour générer des certificats de serveur pour les composants du LSVPN.

Vous devez importer le certificat CA racine sur toutes les passerelles et tous les satellites. Pour des raisons de sécurité, veillez à n'exporter que le certificat, et non la clé privée associée.

1. Téléchargez le certificat CA racine du portail.
    1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**.
    2. Sélectionnez le certificat CA racine utilisé pour générer des certificats de serveur pour les composants du LSVPN, puis cliquez sur **Export (Exporter)**.
    3. Sélectionnez **Base64 Encoded Certificate (PEM) (Certificat codé en base-64 (PEM))** dans la liste déroulante **File Format (Format de fichier)**, puis cliquez sur **OK (OK)** pour télécharger le certificat. (N'exportez pas la clé privée.)
2. Sur les pare-feu hébergeant les passerelles et les satellites, importez le certificat CA racine.
    1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, puis cliquez sur **Import (Importer)**.
    2. Saisissez un **Certificate Name (Nom de certificat)** qui identifie le certificat comme étant votre certificat CA client.
    3. **Browse (Accédez)** au **Certificate File (Fichier du certificat)** que vous avez téléchargé du CA.
    4. Sélectionnez **Base64 Encoded Certificate (PEM)** (Certificat codé en base-64 (PEM)) comme **File Format (Format du fichier)**, puis cliquez sur **OK**.
    5. Sélectionnez le certificat que vous venez d'importer dans l'onglet **Device Certificates (Certificats de périphérique)** pour l'ouvrir.
    6. Sélectionnez **Trusted Root CA (CA racine de confiance)**, puis cliquez sur **OK**.
    7. **Commit (Validez)** les modifications.

**STEP 5 |** Créez un profil de certificat.

Le portail LSVPN GlobalProtect et chaque passerelle nécessitent un profil de certificat qui spécifie le certificat à utiliser pour authentifier les satellites.

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion de Certificat)** > **Certificate Profile (Profil de certificats)**, cliquez sur **Add (Ajouter)** et entrez un **Name (Nom)** de profil.
2. Vérifiez que le **Username Field (Champ Nom d'utilisateur)** est défini sur **None (Aucun)**.
3. Dans le champ **CA Certificates (Certificats CA)**, cliquez sur **Add (Ajouter)**, sélectionnez le certificat CA racine de confiance que vous avez importé à l'étape précédente.
4. (Recommandé) Activez l'utilisation de CRL et/ou d'OCSP pour permettre la vérification de l'état du certificat.
5. Cliquez sur **OK** pour enregistrer le profil.

**STEP 6 |** Validez vos modifications.

Cliquez sur **Commit (Valider)**.

# Déploiement des certificats client vers les satellites GlobalProtect à l'aide de SCEP

Pour déployer des certificats client vers les satellites, vous pouvez également configurer votre portail GlobalProtect pour qu'il agisse en tant que client Simple Certificate Enrollment Protocol (Protocole de recrutement de certificat simple ; SCEP) d'un serveur SCEP de la PKI de votre entreprise. L'opération SCEP est dynamique du fait que la PKI de l'entreprise génère un certificat à la demande du portail et l'envoie au portail.

Lorsque le périphérique satellite demande une connexion au portail ou à la passerelle, il inclut son numéro de série à la demande de connexion. Le portail envoie un CSR au serveur SCEP à l'aide des paramètres du profil SCEP et inclut automatiquement le numéro de série du périphérique dans le champ sujet du certificat client. Après avoir reçu le certificat client de la PKI de l'entreprise, le portail déploie, de façon transparente, le certificat client vers le périphérique satellite. Le périphérique satellite présente alors le certificat client au portail ou à la passerelle à des fins d'authentification.

**STEP 1 |** Créez un profil SCEP.

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **SCEP (SCEP)**, puis **Add (Ajouter)** un nouveau profil.
2. Saisissez un **Name (Nom)** pour identifier le profil.
3. S'il s'agit du profil d'un pare-feu pouvant prendre en charge de multiples systèmes virtuels, sélectionnez un système virtuel ou sélectionnez l'option **Shared (Partagé)** en tant que **Location (Emplacement)** où le profil est disponible.

**STEP 2 |** (Facultatif) Pour rendre la génération de certificats basée sur SCEP plus sécurisée, configurez un mécanisme de réponse au défi SCEP entre l'ICP et le portail pour chaque demande de certificat.

Après avoir configuré ce mécanisme, son fonctionnement est invisible et aucune autre intervention de votre part n'est nécessaire.

Pour vous conformer à la U.S. Federal Information Processing Standard (norme de traitement de l'information fédérale ; FIPS), utilisez un **SCEP Challenge (Mécanisme de recrutement SCEP) Dynamic (Dynamique)** et précisez une Server URL (URL du serveur) qui utilise HTTPS (reportez-vous à l'étape 7).

Sélectionnez l'une des options suivantes :

- **None (Aucune)** (par défaut) : le serveur SCEP n'envoie pas de demande d'authentification au portail avant de générer un certificat.
- **Fixed (Fixe)** : obtenez le mot de passe du mécanisme de recrutement auprès du serveur SCEP (par exemple, **`http://10.200.101.1/CertSrv/mscep_admin/`**) dans l'infrastructure PKI, puis copiez ou saisissez le mot de passe dans le champ Password (Mot de passe).
- **Dynamic (Dynamique)** : saisissez la **Server URL (URL du serveur)** SCEP où le client du portail envoie ces informations d'authentification (par exemple, **`http://10.200.101.1/CertSrv/mscep_admin/`**), ainsi qu'un nom d'utilisateur et un OTP que vous choisissez. Le nom d'utilisateur et le mot de passe peuvent être les informations d'authentification de l'administrateur de la PKI.

**STEP 3 |** Spécifiez les paramètres de connexion entre le serveur SCEP et le portail pour permettre au portail de demander et de recevoir des certificats clients.

Pour identifier le satellite, le portail inclut automatiquement le numéro de série du périphérique dans la demande CSR qu'il envoie au serveur SCEP. Étant donné qu'une valeur doit être indiquée dans le champ **Subject (Sujet)** du profil SCEP, vous pouvez laisser le jeton **$USERNAME** par défaut, même si la valeur n'est pas utilisée dans les certificats client des LSVPN.

1. Configurez la **Server URL (URL du serveur)** que le portail utilise pour atteindre le serveur SCEP dans la PKI (par exemple, **`http://10.200.101.1/certsrv/mscep/`**).
2. Saisissez une chaîne (jusqu'à 255 caractères de longueur) dans le champ **CA-IDENT Name (Nom AC-IDENT)** pour identifier le serveur SCEP.
3. Sélectionnez le **Subject Alternative Name Type (Type de nom alternatif de sujet)** :
   - **RFC 822 Name (Nom RFC 822)** : saisissez le nom de la messagerie dans l'objet du certificat ou l'extension alternative du nom de l'objet.
   - **DNS Name (Nom DNS)** : saisissez le nom DNS utilisé pour évaluer les certificats.
   - **Uniform Resource Identifier (Identificateur de ressource uniforme)** : saisissez le nom de la ressource à partir de laquelle le client obtient le certificat.
   - **None (Aucun)** : ne spécifiez pas d'attributs pour le certificat.

**STEP 4 |** (Facultatif) Configurez les paramètres cryptographiques du certificat.

- Sélectionnez la longueur de la clé (**Number of Bits (Nombre de bits)**) pour le certificat. Si le pare-feu est en mode FIPS-CC et que l'algorithme de génération de clés est RSA. Les clés RSA doivent être de 2.048 bits ou plus.
- Sélectionnez **Digest for CSR (Résumé du CSR)**, qui indique l'algorithme de résumé de la Certificate Signing Request (demande de signature de certificat ; CSR) : SHA1, SHA256, SHA384 ou SHA512.

**STEP 5 |** (Facultatif) Configurez les utilisations autorisées du certificat, soit pour la signature ou le chiffrement.

- Pour utiliser ce certificat pour la signature, activez la case à cocher **Use as digital signature (Utiliser comme signature numérique)**. Cela permet au point de terminaison d'utiliser la clé privée dans le certificat pour valider une signature numérique.
- Pour utiliser ce certificat pour le chiffrement, activez la case à cocher **Use for key encipherment (Utiliser pour le chiffrement des clés)**. Sélectionnez cette option pour configurer le terminal client afin d'utiliser la clé privée dans le certificat dans le but de crypter les données échangées par le biais de la connexion HTTPS établie avec les certificats générés par le serveur SCEP.

**STEP 6 |** (Facultatif) Pour veiller à ce que le portail se connecte au bon serveur SCEP, saisissez le **CA Certificate Fingerprint (Empreinte du certificat de l'autorité de certification)**. Vous pouvez obtenir cette empreinte auprès de l'interface du serveur SCEP dans le champ « Empreinte numérique ».

1. Entrez l'URL de l'interface utilisateur du serveur SCEP (par exemple, **`http://<hostname or IP>/CertSrv/mscep_admin/`**).
2. Copiez l'empreinte numérique et saisissez-la dans le champ **CA Certificate Fingerprint (Empreinte du certificat de l'autorité de certification)**.

**STEP 7 |** Activer l'authentification SSL mutuelle entre le serveur SCEP et le portail GlobalProtect. C'est nécessaire pour se conformer à la norme FIPS (Federal Information Processing Standard) des États-Unis.

*(L'opération FIPS-CC est indiquée sur la page de connexion du pare-feu et dans la barre d'état du pare-feu.)*

Sélectionnez le **CA Certificate (Certificat CA)** racine du serveur SCEP. Vous pouvez activer l'authentification SSL mutuelle entre le serveur SCEP et le portail GlobalProtect en sélectionnant **Client Certificate (Certificat client)**.

**STEP 8 |** Enregistrez et validez la configuration.

1. Cliquez sur **OK** pour enregistrer les paramètres puis fermez la boîte de dialogue SCEP.
2. **Commit (Validez)** la configuration.

Le portail tente de demander un certificat CA à l'aide des paramètres du profil SCEP et l'enregistre sur le pare-feu hébergeant le portail. En cas de succès, le certificat CA est affiché dans **Device (Périphérique)** > **Certificate Management (Gestion de certificat)** > **Certificates (Certificats)**.

**STEP 9 |** (Facultatif) Si, après avoir enregistré le profil SCEP, le portail ne parvient pas à obtenir le certificat, vous pouvez générer manuellement une demande de signature de certificat (CSR) à partir du portail.

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphériques)**, puis cliquez sur **Generate (Générer)**.
2. Saisissez un **Certificate Name (Nom de certificat)**. Ce nom ne peut contenir d'espaces.
3. Sélectionnez le **SCEP Profile (Profil SCEP)** qui doit servir à l'envoi d'une CSR à la PKI de votre entreprise.
4. Cliquez sur **OK** pour soumettre la demande et générer le certificat.

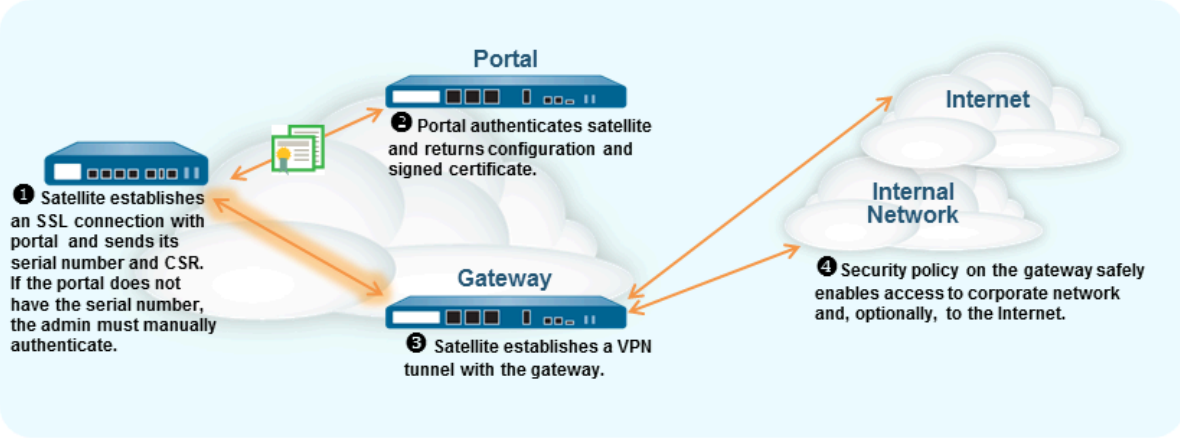
 

# Configuration du portail pour l'authentification de satellites

Pour pouvoir s'enregistrer sur le LSVPN, chaque satellite doit établir une connexion SSL/TLS avec le portail. Une fois la connexion établie, le portail authentifie le satellite pour s'assurer qu'il est autorisé à rejoindre le LSVPN. Une fois l'authentification du satellite réussie, le portail génère un certificat du serveur pour le satellite et transmet la configuration du LSVPN en spécifiant les passerelles auxquelles le satellite peut se connecter et le certificat CA racine requis pour établir une connexion SSL avec les passerelles.

Deux méthodes d'authentification du satellite sur le portail lors de sa première connexion sont possibles :

- **Numéro de série** : vous pouvez configurer le portail avec le numéro de série des pare-feu satellites autorisés à rejoindre le LSVPN. Lors de la première connexion du satellite au portail, le satellite fournit son numéro de série au portail et, si la configuration du portail inclut ce numéro de série, le satellite est alors correctement authentifié. Vous ajoutez les numéros de série des satellites autorisés lors de la configuration du portail. Reportez-vous à la section Configuration du portail.
- **Nom d'utilisateur et mot de passe** : si vous mettez en service vos satellites sans saisir manuellement les numéros de série des satellites dans la configuration du portail, vous pouvez demander à l'administrateur du satellite une authentification lors de la première connexion au portail. Même si le portail recherche toujours le numéro de série lors de la première requête du satellite, s'il ne parvient pas à identifier le numéro de série, l'administrateur du satellite doit fournir un nom d'utilisateur et un mot de passe pour l'authentification sur le portail. Étant donné que le portail revient toujours à ce type d'authentification, vous devez créer un profil d'authentification afin de valider la configuration du portail. Pour cela, vous devez configurer un profil d'authentification lors de la configuration du LSVPN du portail, même si vous envisagez d'authentifier les satellites à l'aide du numéro de série.




Le flux de travail suivant décrit la configuration du portail afin d'authentifier des satellites auprès d'un service d'authentification existant. Le LSVPN GlobalProtect prend en charge l'authentification externe à l'aide d'une base de données locale, de LDAP (Active Directory inclus), Kerberos, TACACS+ ou RADIUS.

**STEP 1 |** (Authentification externe uniquement) Créez un profil de serveur sur le portail.

Le profil de serveur définit comment le pare-feu se connecte à un service d'authentification externe afin de valider les informations d'identification d'authentification saisies par l'administrateur du satellite.

*Si vous utilisez une authentification locale, ignorez cette étape et ajoutez un utilisateur local pour l'administrateur du satellite, reportez-vous à la section* Ajoutez le compte utilisateur à la base de données locale.

Configurez un profil de serveur pour le type de service d'authentification :

- Ajoutez un profil de serveur RADIUS.

*Vous pouvez vous servir de RADIUS pour l'intégrer à un service d'*Authentification multifacteur**.**

- Ajoutez un profil de serveur TACACS+.
- Ajoutez un profil de serveur d'IDP en SAML.
- Ajoutez un profil de serveur Kerberos.
- Ajoutez un profil de serveur LDAP. Si vous utilisez LDAP pour vous connecter à Active Directory (AD), créez un profil de serveur LDAP distinct pour chaque domaine AD.

**STEP 2 |** Configurez un profil d'authentification.

Le profil d'authentification définit le profil de serveur à utiliser pour authentifier les satellites.

1. Sélectionnez **Device (Périphérique)** > **Authentication Profile (Profil d'authentification)**, puis cliquez sur **Add (Ajouter)**.
2. Donnez un **Name (Nom)** au profil, puis sélectionnez le **Type (Type)** d'authentification. Si le **Type (Type)** est un service externe, sélectionnez le **Server Profile (Profil de serveur)** que vous avez créé à l'étape précédente. Si vous avez ajouté un utilisateur local, définissez le **Type (Type)** sur **Local Database (Base de données locale)**.
3. Cliquez sur **OK**, puis sur **Commit (Valider)**.

# Configuration de passerelles GlobalProtect pour le LSVPN

Étant donné que la configuration de GlobalProtect transmise par le portail aux satellites inclut la liste des passerelles auxquelles le satellite peut se connecter, il convient de configurer les passerelles avant de configurer le portail.

Avant de configurer la passerelle GlobalProtect, vous devez avoir effectué les tâches suivantes :

- Création d'interfaces et de zones pour le LSVPNsur l'interface sur laquelle vous configurerez chaque passerelle. Vous devez configurer l'interface physique et l'interface de tunnel virtuelle.
- Activation de SSL entre des composants du LSVPN GlobalProtect en configurant les certificats du serveur de passerelle, les profils de service SSL/TLS et le profil de certificat requis pour établir une connexion SSL/TLS mutuelle des satellites GlobalProtect à la passerelle.

Configurez chaque passerelle GlobalProtect pour prendre part au LSVPN comme suit :

**STEP 1 |** Ajoutez une passerelle.

1. Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Gateways (Passerelle)**et cliquez sur **Add (Ajouter)**.
2. Dans l'écran **General (Général)**, donnez un **Name (Nom)** à la passerelle. Le nom de passerelle ne doit pas contenir d'espace et, selon la procédure recommandée, il doit inclure l'emplacement ou d'autres informations descriptives qui permettront aux utilisateurs et autres administrateurs d'identifier la passerelle.
3. (Facultatif) Sélectionnez le système virtuel auquel cette passerelle appartient dans le champ **Location (Emplacement)**.

**STEP 2 |** Spécifiez les informations réseau qui permettent aux périphériques satellites de se connecter à la passerelle.

Si vous n'avez pas créé l'interface réseau de la passerelle, reportez-vous à la section Création d'interfaces et de zones pour le LSVPN pour obtenir des instructions.

1. Sélectionnez l'**Interface (Interface)** que les satellites utiliseront comme accès d'entrée à la passerelle.
2. Spécifiez le **IP Address Type (Type d'adresse IP)** et la **IP address (Adresse IP)** pour l'accès à la passerelle :
   - L'adresse IP peut être de type **IPv4 (IPv4)** (uniquement), **IPv6 (IPv6)** (uniquement) ou **IPv4 and IPv6 (IPv4 et IPv6)**. Utilisez **IPv4 and IPv6 (IPv4 et IPv6)** si votre réseau prend en charge les configurations en double pile, où IPv4 et IPv6 fonctionnent en même temps.
   - L'adresse IP doit être compatible avec le type d'adresse IP. Par exemple, **`172.16.1/0`** pour les adresses IPv4 ou **`21DA:D3:0:2F3B`** pour les adresses IPv6. Pour les configurations en double pile, saisissez une adresse IPv4 ainsi qu'une adresse IPv6.
3. Cliquez sur **OK** pour enregistrer les modifications.

**STEP 3 |** Précisez la façon dont la passerelle authentifie les satellites qui tentent d'établir des tunnels. Si vous n'avez pas déjà créé de profil de service SSL/TLS pour la passerelle, reportez-vous à la section Déploiement de certificats de serveur sur les composants du LSVPN GlobalProtect.

Si vous n'avez pas encore configuré les profils d'authentification ou les profils de certificat, reportez-vous à la section Configuration du portail pour l'authentification de satellites pour obtenir les instructions.

Si vous n'avez pas déjà configuré le profil de certificat, reportez-vous à la section Activation de SSL entre des composants du LSVPN GlobalProtect pour obtenir des instructions.

Dans la boîte de dialogue GlobalProtect Gateway Configuration (Configuration de la passerelle GlobalProtect), sélectionnez Authentication (Authentification), puis configurez l'un des éléments suivants :

- Pour sécuriser la communication entre la passerelle et les satellites, sélectionnez le **SSL/TLS Service Profile (Profile de service SSL/TLS)** de la passerelle.
- Pour préciser le profil d'authentification à utiliser pour authentifier les satellites, **Add (Ajouter)** une Client Authentication (authentification de client). Puis, entrez un **Name (Nom)** pour identifier la configuration et sélectionnez **OS (système d'exploitation)**. Choisissez **Satellite (Satellite)** pour appliquer la configuration à l'ensemble des satellites, et précisez le **Authentication Profile (Profil d'authentification)** à utiliser pour authentifier le satellite. Vous pouvez également sélectionner un **Certificate Profile (Profil de certificat)** que la passerelle utilisera pour authentifier des périphériques satellites tentant d'établir des tunnels.

**STEP 4 |** Configurez les paramètres du tunnel et activez la tunnellisation.

1. Dans la boîte de dialogue GlobalProtect Gateway Configuration (Configuration de la passerelle GlobalProtect), sélectionnez **Satellite (Satellite)** > **Tunnel Settings (Paramètres du tunnel)**.
2. Cochez la case **Tunnel Configuration (Configuration du tunnel)** pour activer la tunnellisation.
3. Sélectionnez la **Tunnel Interface (Interface de tunnel)** que vous avez définie pour mettre fin aux tunnels VPN établis par les satellites GlobalProtect lorsque vous avez effectué la tâche liée à la Création d'interfaces et de zones pour le LSVPN.
4. (Facultatif) Si vous souhaitez conserver les informations de Type of Service (type de service ; ToS) dans les paquets encapsulés, sélectionnez **Copy TOS (Copier l'en-tête ToS)**.

   *Les paquets IPSec pourraient arriver dans le désordre si vous copiez l'en-tête ToS et qu'il y a plusieurs sessions dans le tunnel (chacune d'entre elles possédant une valeur de ToS différente),*

**STEP 5 |** (Facultatif) Activez la surveillance des tunnels.

La surveillance des tunnels permet aux satellites de surveiller leur connexion de tunnel de passerelle, leur permettant ainsi de basculer vers une passerelle de secours en cas d'échec de connexion. Le basculement vers une autre passerelle est le seul type de surveillance du tunnel pris en charge avec le LSVPN.

1. Cochez la case **Tunnel Monitoring (Surveillance du tunnel)**.
2. Spécifiez la **Destination IP Address** (Adresse IP de destination) que les satellites doivent utiliser pour déterminer si la passerelle est active. Vous pouvez indiquer une adresse **IPv4**

**(IPv4)** et une adresse **IPv6 (IPv6)**, ou les deux. Si vous avez configuré une adresse IP pour l'interface de tunnel, vous pouvez également ne pas renseigner ce champ. La surveillance des tunnels utilisera alors l'interface de tunnel pour déterminer si la connexion est active.

3. Sélectionnez **Failover (Basculement)** dans la liste déroulante **Tunnel Monitor Profile (Profil de surveillance du tunnel)** (c'est le seul profil de surveillance du tunnel pris en charge pour le LSVPN).

**STEP 6 |** Sélectionnez le profil crypto IPSec à utiliser lors de l'établissement de connexions de tunnel.

Le profil précise le type de chiffrement IPSec et la méthode d'authentification pour sécuriser les données qui passeront par le tunnel. Les deux extrémités du tunnel d'un LSVPN étant des pare-feu approuvés au sein de votre entreprise, vous pouvez généralement utiliser le profil par défaut (prédéfini) qui utilise le protocole IPSec ESP, le groupe DH 2, le chiffrement AES-128-CVC et l'authentification SHA-1.

Dans la liste déroulante **IPSec Crypto Profile (Profil crypto IPSec)**, sélectionnez **default (par défaut)** pour utiliser le profil prédéfini, ou choisissez **New IPSec Crypto Profile (Nouveau profil crypto IPSec)** pour définir un nouveau profil. Pour obtenir plus d'informations sur les options d'authentification et de chiffrement, reportez-vous à la section Définition de profils crypto IPSec.

**STEP 7 |** Configurez les paramètres réseau pour affecter les satellites lors de l'établissement du tunnel IPSec.

*Vous pouvez également configurer le satellite afin qu'il transmette les paramètres DNS à ses clients locaux en configurant un serveur DHCP sur le pare-feu hébergeant le satellite. Dans cette configuration, le satellite transmettra aux clients DHCP les paramètres DNS qu'il reçoit de la passerelle.*

1. Dans la boîte de dialogue GlobalProtect Gateway Configuration (Configuration de la passerelle GlobalProtect), sélectionnez **Satellite (Satellite)** > **Network Settings (Paramètres réseau)**.
2. (Facultatif) Si des clients locaux du satellite doivent résoudre des FQDN sur le réseau d'entreprise, configurez la passerelle pour qu'elle transmette des paramètres DNS aux satellites de l'une des manières suivantes :
   - Si la passerelle inclut une interface configurée en tant que client DHCP, vous pouvez définir la **Inheritance Source (Source de l'héritage)** sur l'interface et attribuer les mêmes paramètres que ceux reçus par le client DHCP aux satellites GlobalProtect. Vous pouvez aussi hériter des suffixes DNS de la même source.

- Définissez manuellement les paramètres **Primary DNS (DNS principal)**, **Secondary DNS (DNS secondaire)** et **DNS Suffix (Suffixe DNS)** à transmettre aux satellites.

3. Pour spécifier le paramètre **IP Pool (Pool d'adresses IP)** à affecter à l'interface de tunnel sur les satellites lors de l'établissement du VPN, cliquez sur **Add (Ajouter)**, puis indiquez la ou les plages d'adresses IP à utiliser.
4. Pour définir les sous-réseaux de destination pour le routage via le tunnel, cliquez sur **Add (Ajouter)** dans la section **Access Route (Itinéraire d'accès)**, puis saisissez les itinéraires de la manière suivante :

   - Si vous souhaitez acheminer l'ensemble du trafic provenant des satellites via le tunnel, ne renseignez pas ce champ.

     *Dans ce cas, tout le trafic excepté le trafic destiné au sous-réseau local sera tunnellisé vers la passerelle.*

   - Pour n'acheminer qu'un trafic donné via la passerelle (***split tunneling***), spécifiez les sous-réseaux de destination qui doivent être tunnellisés. Dans ce cas, le satellite acheminera le trafic non destiné à un itinéraire d'accès spécifié selon sa propre table de routage. Par exemple, vous pouvez choisir de ne tunnelliser que le trafic destiné à votre réseau d'entreprise et d'utiliser le satellite local pour autoriser l'accès à Internet en toute sécurité.
   - Si vous souhaitez autoriser le routage entre des satellites, saisissez l'itinéraire récapitulatif du réseau protégé par chaque satellite.

**STEP 8 |** (Facultatif) Définissez les itinéraires (le cas échéant) que la passerelle acceptera des satellites.

Par défaut, la passerelle n'ajoutera aucune publication d'itinéraires de satellites à sa table de routage. Si vous ne souhaitez pas que la passerelle accepte des itinéraires des satellites, vous pouvez ignorer cette étape.

1. Pour autoriser la passerelle à accepter des itinéraires publiés par des satellites, sélectionnez **Satellite (Satellite)** > **Route Filter (Filtre d'itinéraire)**.
2. Cochez la case **Accept published routes (Accepter les itinéraires publiés)**.
3. Pour filtrer les itinéraires publiés par les satellites à ajouter à la table de routage de la passerelle, cliquez sur **Add (Ajouter)**, puis définissez les sous-réseaux à inclure. Par exemple, si tous les satellites sont configurés avec le sous-réseau 192.168.x.0/24 côté LAN, configurez l'itinéraire autorisé 192.168.0.0/16 pour que la passerelle n'accepte les itinéraires de satellites que s'ils se trouvent dans le sous-réseau 192.168.0.0/16.

**STEP 9 |** Enregistrez la configuration de la passerelle.

1. Cliquez sur **OK** pour enregistrer les paramètres puis fermez la boîte de dialogue GlobalProtect Gateway Configuration (Configuration de la passerelle GlobalProtect).
2. **Commit (Validez)** la configuration.

# Configuration du portail GlobalProtect pour le LSVPN

Le portail GlobalProtect fournit les fonctions de gestion de votre LSVPN GlobalProtect. Chaque système satellite qui fait partie du LSVPN reçoit des informations de configuration du portail, notamment des informations sur les passerelles disponibles, ainsi que le certificat dont il a besoin pour se connecter aux passerelles.

Les sections suivantes décrivent les procédures de configuration du portail :

- Tâches LSVPN préalables à la configuration du portail GlobalProtect
- Configuration du portail
- Définition des configurations de satellites

## Tâches LSVPN préalables à la configuration du portail GlobalProtect

Avant de configurer le portail GlobalProtect, vous devez avoir effectué les tâches suivantes :

- Création d'interfaces et de zones pour le LSVPN sur l'interface sur laquelle vous configurerez le portail.
- Activation de SSL entre des composants du LSVPN GlobalProtect en créant un profil de service SSL/TLS pour le certificat de serveur du portail, en générant des certificats de serveur de passerelle et en configurant le portail pour générer des certificats de serveur pour les satellites GlobalProtect.
- Configuration du portail pour l'authentification de satellites en définissant un profil d'authentification que le portail utilisera pour authentifier les satellites si le numéro de série n'est pas disponible.
- Configuration de passerelles GlobalProtect pour le LSVPN.

## Configuration du portail

Après avoir exécuté les tâches préalables à la configuration LSVPN du portail GlobalProtect, configurez le portail GlobalProtect de la manière suivante :

**STEP 1 |** Ajoutez le portail.

1. Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)** et cliquez sur **Add (Ajouter)**.
2. Dans l'onglet **General (Général)**, donnez un **Name (Nom)** au portail. .Le nom du portail ne doit pas contenir d'espaces.
3. (Facultatif) Sélectionnez le système virtuel auquel ce portail appartient dans le champ **Location (Emplacement)**.

**STEP 2 |** Spécifiez les informations sur le réseau permettant aux satellites de se connecter au portail.

Si vous n'avez pas encore créé d'interface réseau pour la passerelle, pour obtenir les instructions, consultez la section Création d'interfaces et de zones pour le LSVPN.

1. Sélectionnez l'**Interface (Interface)** que les satellites utiliseront comme accès d'entrée au portail.
2. Sélectionnez le **IP Address Type (Type d'adresse IP)** et la **IP address (Adresse IP)** pour l'accès du satellite au portail :
   - L'adresse IP peut être de type **IPv4 (IPv4)** (pour le trafic IPv4 uniquement), **IPv6 (IPv6)** (pour le trafic IPv6 uniquement) ou **IPv4 and IPv6 (IPv4 et IPv6)**. Utilisez **IPv4 and IPv6 (IPv4 et IPv6)** si votre réseau prend en charge les configurations en double pile, où IPv4 et IPv6 fonctionnent en même temps.
   - L'adresse IP doit être compatible avec le type d'adresse IP. Par exemple, **`172.16.1/0`** pour les adresses IPv4 ou **`21DA:D3:0:2F3B`** pour les adresses IPv6. Pour les configurations en double pile, saisissez une adresse IPv4 ainsi qu'une adresse IPv6.
3. Cliquez sur **OK** pour enregistrer les modifications.

**STEP 3 |** Indiquez un SSL/TLS Service Profile (Profil de service SSL/TLS) à utiliser pour permettre au satellite d'établir une connexion SSL/TLS au portail.

Si vous n'avez pas créé de profil de service SSL/TLS pour le portail et émis des certificats de passerelle, consultez la section Déploiement de certificats de serveur sur les composants du LSVPN GlobalProtect.

1. Dans la boîte de dialogue GlobalProtect Portal Configuration (Configuration du portail GlobalProtect), sélectionnez **Authentication (Authentification)**.
2. Sélectionnez le **SSL/TLS Service Profile (Profil de service SSL/TLS)**.

**STEP 4 |** Précisez un profil d'authentification et un profil de certificat facultatif pour authentifier les satellites.

> ***Si le portail ne parvient pas à valider les numéros de série des satellites qui se connectent, il a recours au profil d'authentification. Par conséquent, avant de pouvoir enregistrer la configuration du portail (en cliquant sur OK (OK)), vous devez*** configurer un profil d'authentification**.**

**Add (Ajoutez)** une Client Authentication (Authentification de client), puis saisissez un **Name (Nom)** pour identifier la configuration, sélectionnez **OS (Système d'exploitation)** : Choisissez **Satellite (Satellite)** pour appliquer la configuration à l'ensemble des satellites, et précisez le **Authentication Profile (Profil d'authentification)** à utiliser pour authentifier le périphérique satellite. Vous pouvez également préciser un **Certificate Profile (Profil de certificat)** que le portail utilisera pour authentifier des périphériques satellites.

**STEP 5 |** Continuez en définissant les configurations à transmettre aux satellites, ou, si vous avez déjà créé les configurations de satellites, enregistrez la configuration du portail.

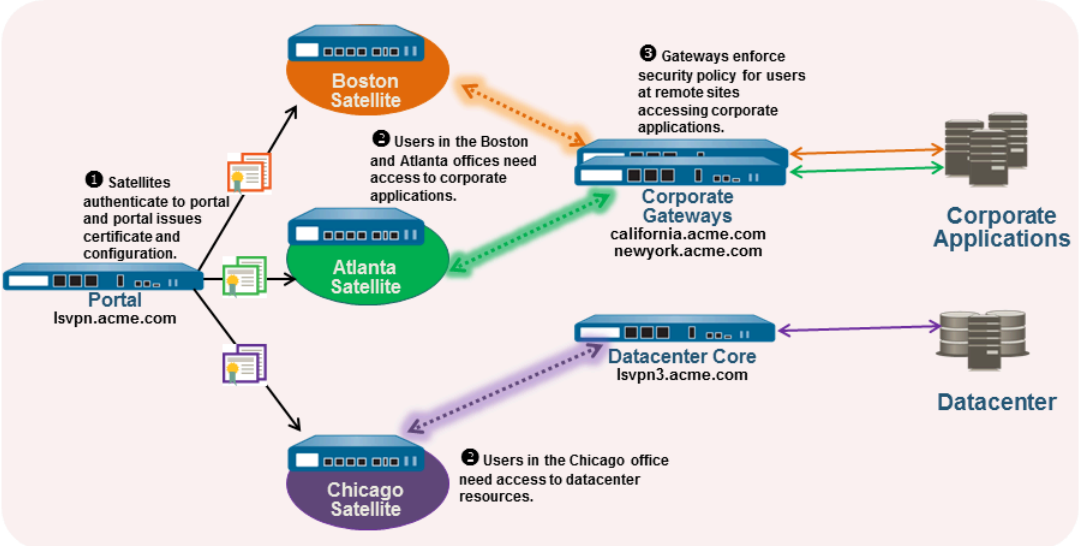
Cliquez sur **OK (OK)** pour enregistrer la configuration du portail ou continuez avec la section Définition des configurations de satellites.

# Définition des configurations de satellites

Lorsqu'un satellite GlobalProtect se connecte et s'authentifie avec succès auprès du portail GlobalProtect, ce dernier envoie une configuration de satellite qui indique les passerelles auxquelles le satellite peut se connecter. Si tous vos satellites utiliseront les mêmes configurations de passerelle et de certificat, vous pouvez créer une seule configuration de satellite à envoyer à tous les satellites une fois l'authentification réussie. Toutefois, si vous avez besoin de configurations de satellites différentes (par exemple, si vous souhaitez qu'un groupe de satellites se connecte à une passerelle et qu'un autre groupe de satellites se connecte à une autre passerelle), vous pouvez créer une configuration de satellite distincte pour chacun. Le portail utilise ensuite le nom d'utilisateur/de groupe d'inscription ou le numéro de série du satellite pour déterminer la configuration de satellite à déployer. Comme avec l'évaluation des règles de sécurité, le portail recherche une correspondance en commençant par le début de la liste. Lorsqu'il trouve une correspondance, il fournit la configuration correspondante au satellite.

Par exemple, la figure suivante illustre un réseau dans lequel certaines filiales nécessitent un accès VPN aux applications d'entreprise protégées par vos pare-feu périphériques et où un autre site requiert un accès VPN au centre de données.




Utilisez la procédure suivante pour créer une ou plusieurs configurations de satellites.

**STEP 1 |** Ajoutez une configuration de satellite.

La configuration de satellite spécifie les paramètres de configuration du LSVPN GlobalProtect à déployer sur les satellites qui se connectent. Vous devez définir au moins une configuration de satellite.

1. Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)**, choisissez la configuration de portail à laquelle vous souhaitez ajouter une configuration de satellite, puis cliquez sur l'onglet **Satellite (Satellite)**.
2. Dans la section Satellite (Satellite), cliquez sur **Add (Ajouter)**.
3. Saisissez un **Name (Nom)** pour la configuration.

   Si vous envisagez de créer plusieurs configurations, veillez à ce que le nom que vous définissez pour chacune soit suffisamment explicite pour vous permettre de les distinguer.
4. Pour modifier la fréquence à laquelle un satellite devrait vérifier la disponibilité des mises à jour de configuration du portail, indiquez une valeur dans le champ **Configuration Refresh Interval (hours) (Intervalle d'actualisation de la configuration (heures))** (plage comprise entre 1 et 48 ; valeur par défaut : 24).

**STEP 2 |** Indiquez les satellites sur lesquels déployer cette configuration.

Le portail utilise les paramètres **Enrollment User/User Group (Utilisateur/groupe d'utilisateurs d'inscription)** et/ou les numéros de série des **Devices (Périphériques)** pour faire correspondre un satellite et une configuration. Si vous disposez de plusieurs configurations, veillez donc à les classer de manière appropriée. Dès que le portail trouve une correspondance, il fournit la configuration. Ainsi, les configurations plus spécifiques doivent précéder les configurations plus générales. Reportez-vous à l'étape 5 pour obtenir des instructions sur le classement de la liste des configurations de satellites.

Spécifiez les critères de correspondance de configuration de satellite comme suit :

- Pour limiter cette configuration aux satellites dotés de numéros de série spécifiques, sélectionnez l'onglet **Devices (Périphériques)**, cliquez sur **Add (Ajouter)**, puis saisissez le numéro de série (vous ne devez pas saisir le nom d'hôte du satellite, celui-ci sera automatiquement ajouté lors de la connexion du satellite). Répétez cette étape pour chaque satellite qui doit recevoir cette configuration.
- Sélectionnez l'onglet **Enrollment User/User Group (Utilisateur/groupe d'utilisateurs d'inscription)**, cliquez sur **Add (Ajouter)**, puis sélectionnez l'utilisateur ou le groupe qui doit recevoir cette configuration. Les satellites ne correspondant pas au numéro de série devront s'authentifier en tant qu'utilisateur spécifié ici (utilisateur individuel ou membre de groupe).

*Avant de pouvoir restreindre la configuration à des groupes spécifiques, vous devez* mapper les utilisateurs à des groupes.

**STEP 3 |** Spécifiez les passerelles avec lesquelles les satellites dotés de cette configuration peuvent établir des tunnels VPN.

> *Les itinéraires publiés par la passerelle sont installés sur le satellite en tant qu'itinéraires statiques. La mesure de l'itinéraire statique correspond à 10 fois la priorité de routage. Si vous disposez de plusieurs passerelles, veillez à définir également la priorité d'itinéraire pour s'assurer que les itinéraires publiés par les passerelles de secours incluent des mesures supérieures aux mêmes itinéraires publiés par les passerelles principales. Par exemple, si vous définissez la priorité de routage de la passerelle principale et de la passerelle de secours sur 1 et 10, respectivement, le satellite utilisera la mesure 10 pour la passerelle principale et 100 pour la passerelle de secours.*

1. Dans l'onglet **Gateways (Passerelles)**, cliquez sur **Add (Ajouter)**.
2. Donnez un **Name (Nom)** descriptif à la passerelle. Le nom que vous saisissez ici doit correspondre au nom que vous avez défini lors de la configuration de la passerelle, et doit être suffisamment explicite pour pouvoir identifier l'emplacement de la passerelle.
3. Dans le champ **Gateways (Passerelles)**, saisissez le nom de domaine complet, FQDN, ou l'adresse IP de l'interface sur laquelle la passerelle est configurée. L'adresse que vous spécifiez doit correspondre exactement au nom commun (NC) dans le certificat de serveur de passerelle.
4. (Facultatif) Si vous ajoutez deux passerelles ou plus à la configuration, la **Routing Priority (Priorité de routage)** aide le satellite à choisir la passerelle préférée. Saisissez une valeur comprise entre 1 et 25, une valeur inférieure représentant une priorité supérieure (à savoir, la passerelle à laquelle le satellite se connectera si toutes les passerelles sont disponibles). Le satellite multipliera la priorité de routage par 10 pour déterminer la mesure de routage.

**STEP 4 |** Enregistrez la configuration de satellite.

1. Cliquez sur **OK (OK)** pour enregistrer la configuration du satellite.
2. Si vous souhaitez ajouter une autre configuration de satellite, répétez les étapes précédentes.

**STEP 5 |** Organisez les configurations de satellites de sorte que la configuration appropriée soit déployée sur chaque satellite.

- Pour remonter une configuration de satellite dans la liste de configurations, sélectionnez la configuration, puis cliquez sur **Move Up (Déplacer vers le haut)**.
- Pour descendre une configuration de satellite dans la liste de configurations, sélectionnez la configuration, puis cliquez sur **Move Down (Déplacer vers le bas)**.

**STEP 6 |** Spécifiez les certificats nécessaires pour permettre aux satellites de prendre part au LSVPN.

1. Dans le champ **Trusted Root CA (CA racine de confiance)**, cliquez sur **Add (Ajouter)**, puis sélectionnez le certificat CA utilisé pour générer les certificats serveur de passerelle. Le portail déploie le certificat CA racine que vous ajoutez ici sur tous les satellites lors de la configuration afin de permettre au satellite d'établir une connexion SSL avec les passerelles. Il est recommandé que toutes vos passerelles utilisent le même émetteur.
2. Sélectionnez la méthode de distribution du **Client Certificate (Certificat de client)** :
   - **Pour stocker les certificats de client sur le portail** : sélectionnez **Local (Local)** et, à partir de la liste déroulante **Issuing Certificate (Publication de certificat)**,

sélectionnez le certificat CA racine que le portail utilisera pour générer des certificats de client aux satellites une fois ces derniers authentifiés avec succès.

*Si le certificat CA racine utilisé pour générer vos certificats de serveur de passerelle ne se trouve pas sur le portail, vous pouvez cliquer sur **Import (Importer)** pour l'importer maintenant. Reportez-vous à la section* Activation de SSL entre des composants du LSVPN GlobalProtect *pour obtenir plus de détails sur l'importation d'un certificat AC racine.*

- **Pour permettre au portail d'agir en tant que client SCEP pour demander et générer des certificats de client de façon dynamique** : sélectionnez **SCEP (SCEP)**, puis sélectionnez le profil **SCEP (SCEP)** utilisé pour générer les CSR envoyées à votre serveur SCEP.

*Si vous n'avez pas encore configuré le portail pour qu'il agisse en tant que client SCE, vous pouvez ajouter un **New (Nouveau)** profil SCEP maintenant. Reportez-vous à la section* Déploiement des certificats client vers les satellites GlobalProtect à l'aide de SCEP *pour obtenir plus de précisions.*

**STEP 7 |** Enregistrez la configuration du portail.

1. Cliquez sur **OK** pour enregistrer les paramètres puis fermez la boîte de dialogue Passerelles GlobalProtect.
2. **Commit (Validez)** vos modifications.

# Préparation du satellite pour l'association au LSVPN

Pour pouvoir prendre part au LSVPN, le satellite a besoin d'une configuration minime. La configuration requise étant minime, vous pouvez pré-configurer les satellites avant de les envoyer pour installation dans vos filiales.

**STEP 1 |** Configure a Layer 3 Interface (Configurez une interface de couche 3).

Il s'agit de l'interface physique que le satellite utilisera pour se connecter au portail et à la passerelle. Cette interface doit se trouver dans une zone autorisant un accès en dehors du réseau approuvé local. Il est recommandé de créer une zone dédiée pour les connexions VPN dans un souci de visibilité et de contrôle du trafic destiné aux passerelles d'entreprise.

**STEP 2 |** Configurez l'interface de tunnel logique qui sera utilisée par le tunnel pour établir des tunnels VPN avec les passerelles GlobalProtect.

***Les adresses IP ne sont pas requises sur l'interface de tunnel, sauf si vous envisagez d'utiliser le routage dynamique. L'affectation d'une adresse IP à l'interface de tunnel peut toutefois être utile pour le dépannage de problèmes de connectivité.***

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Tunnel** et cliquez sur **Add (Ajouter)**.
2. Dans le champ **Interface Name (Nom de l'interface)**, spécifiez un suffixe numérique, tel que **.2**.
3. Dans l'onglet **Config (Configuration)**, développez la liste déroulante **Security Zone (Zone de sécurité)**, puis sélectionnez une zone existante ou créez une zone distincte pour le trafic de tunnel VPN en cliquant sur **New Zone (Nouvelle zone)** et en donnant un **Name (Nom)** à la nouvelle zone (par exemple, ***lsvpnsat***).
4. Dans la liste déroulante **Virtual Router (Routeur virtuel)**, sélectionnez **default (Par défaut)**.
5. (Facultatif) Pour attribuer une adresse IP à l'interface du tunnel :
   - Pour une adresse IPv4, sélectionnez **IPv4** et **Add (Ajouter)** l'adresse IP et le masque de réseau à affecter à l'interface, par exemple 203.0.11.100/24.
   - Pour une adresse IPv6, sélectionnez **IPv6**, **Enable IPv6 on the interface (Activez IPv6 sur l'interface)**, et **Add (Ajoutez)** l'adresse IP et le masque réseau à affecter à l'interface, par exemple 2001:1890:12f2:11::10.1.8.160/80.
6. Pour enregistrer la configuration de l'interface, cliquez sur **OK**.

**STEP 3 |** Si vous avez généré le certificat de serveur du portail à l'aide d'une CA racine non approuvée par les satellites (si vous avez utilisé des certificats auto-signés par exemple), importez le certificat CA racine utilisé pour générer le certificat de serveur du portail.

Le certificat CA racine est nécessaire pour permettre au satellite d'établir la première connexion avec le portail afin d'obtenir la configuration du LSVPN.

1. Téléchargez le certificat CA utilisé pour générer les certificats de serveur de portail. Si vous utilisez des certificats auto-signés, exportez le certificat CA racine depuis le portail comme suit :
   1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**.
   2. Sélectionnez le certificat CA, puis cliquez sur **Export (Exporter)**.
   3. Sélectionnez **Base64 Encoded Certificate (PEM) (Certificat codé en base-64 (PEM))** dans la liste déroulante **File Format (Format de fichier)**, puis cliquez sur **OK (OK)** pour télécharger le certificat. (Vous n'avez pas besoin d'exporter la clé privée.)
2. Importez le certificat AC que vous venez d'exporter sur chaque satellite comme suit.
   1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, puis cliquez sur **Import (Importer)**.
   2. Saisissez un **Certificate Name (Nom de certificat)** qui identifie le certificat comme étant votre certificat CA client.
   3. **Browse (Accédez)** au **Certificate File (Fichier du certificat)** que vous avez téléchargé du CA.
   4. Sélectionnez **Base64 Encoded Certificate (PEM)** (Certificat codé en base-64 (PEM)) comme **File Format (Format du fichier)**, puis cliquez sur **OK**.
   5. Sélectionnez le certificat que vous venez d'importer dans l'onglet **Device Certificates (Certificats de périphérique)** pour l'ouvrir.
   6. Sélectionnez **Trusted Root CA (CA racine de confiance)**, puis cliquez sur **OK**.

**STEP 4 |** Procédez à la configuration du tunnel IPSec.

1. Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)**, puis cliquez sur **Add (Ajouter)**.
2. Dans l'onglet **General (Général)**, donnez un **Name (Nom)** descriptif à la configuration IPSec.
3. Sélectionnez la **Tunnel Interface (Interface de tunnel)** que vous avez créée pour le satellite.
4. Sélectionnez **GlobalProtect Satellite (Satellite GlobalProtect)** comme **Type (Type)**.
5. Saisissez l'adresse IP ou le FQDN du portail pour le paramètre **Portal Address (Adresse du portail)**.
6. Sélectionnez l'**Interface (Interface)** de couche 3 que vous avez configurée pour le satellite.
7. Sélectionnez la **IP Address (Adresse IP)** à utiliser sur l'interface sélectionnée. Vous pouvez sélectionner une adresse **IPv4 (IPv4)**, une adresse **IPv6 (IPv6)**, ou les deux. Précisez si

vous souhaitez **IPv6 preferred for portal registration (privilégié l'adresse IPv6 pour l'enregistrement au portail)**.

**STEP 5 |** (Facultatif) Configurez le satellite pour qu'il publie des itinéraires locaux sur la passerelle.

La transmission d'itinéraires à la passerelle autorise le trafic vers les sous-réseaux locaux vers le satellite via la passerelle. Cependant, vous devez également configurer la passerelle pour qu'elle accepte les itinéraires, comme décrit en détail à la section Configuration de passerelles GlobalProtect pour le LSVPN.

1. Pour autoriser le satellite à transmettre des itinéraires à la passerelle, dans l'onglet **Advanced (Avancé)**, sélectionnez **Publish all static and connected routes to Gateway (Publier tous les itinéraires statiques et connectés sur la passerelle)**.

   Si vous cochez cette case, le pare-feu transfère tous les itinéraires statiques et connectés depuis le satellite vers la passerelle. Toutefois, pour empêcher la création de boucles de routage, le pare-feu applique certains filtres d'itinéraires, tels que les suivants :

   - Itinéraires par défaut
   - Itinéraires au sein d'un routeur virtuel autre que celui associé à l'interface de tunnel
   - Itinéraires utilisant l'interface de tunnel
   - Itinéraires utilisant l'interface physique associée à l'interface de tunnel virtuelle
2. (Facultatif) Si vous ne souhaitez envoyer que des itinéraires de sous-réseaux spécifiques, et non tous les itinéraires, cliquez sur **Add (Ajouter)** dans la section Subnet (Sous-réseau), puis spécifiez les itinéraires de sous-réseau à publier.

**STEP 6 |** Enregistrez la configuration de satellite.

1. Cliquez sur **OK** pour enregistrer les paramètres de tunnel IPSec.
2. Cliquez sur **Commit (Valider)**.

**STEP 7 |** Si nécessaire, fournissez les informations d'identification pour permettre au satellite de s'authentifier sur le portail.

Cette étape n'est requise que si le portail n'a pas trouvé un numéro de série correspondant dans sa configuration ou si le numéro de série ne fonctionne pas. Dans ce cas, le satellite ne pourra pas établir le tunnel avec la ou les passerelles.

1. Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)**, puis cliquez sur le lien **Gateway Info (Informations sur la passerelle)** dans la colonne d'État de la configuration du tunnel que vous avez créée pour le LSVPN.
2. Cliquez sur le lien **enter credentials (Saisir les informations d'identification)** dans le champ **Portal Status (État du portail)**, puis saisissez le nom d'utilisateur et le mot de passe requis pour authentifier le satellite sur le portail.

   Une fois le satellite authentifié avec succès sur le portail, il reçoit son certificat signé et sa configuration, qu'il utilisera pour se connecter à la ou aux passerelles. Le tunnel doit alors être établi et l'**État** passe à **Actif**.

# Vérification de la configuration du LSVPN

Une fois le portail, les passerelles et les satellites configurés, vérifiez que les satellites peuvent se connecter au portail et à la passerelle, et établissez des tunnels VPN avec la ou les passerelles.

**STEP 1 |** Vérifiez la connectivité du satellite avec le portail.

Dans le pare-feu hébergeant le portail, vérifiez que les satellites peuvent se connecter en sélectionnant **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portal (Portail)** et en cliquant sur **Satellite Info (Infos sur le satellite)** dans la colonne Infos de l'entrée de configuration du portail.

**STEP 2 |** Vérifiez la connectivité du satellite avec la ou les passerelles.

Sur chaque pare-feu hébergeant une passerelle, vérifiez que les satellites peuvent établir des tunnels VPN en sélectionnant **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Gateways (Passerelles)** puis cliquez sur **Satellite Info (Infos sur le satellite)**, dans la colonne Infos de l'entrée de configuration de la passerelle. Les satellites ayant établi avec succès des tunnels avec la passerelle s'affichent dans l'onglet **Active Satellites (Satellites actifs)**.

**STEP 3 |** Vérifiez l'état du tunnel LSVPN sur le satellite.

Sur chaque pare-feu hébergeant un satellite, vérifiez l'état du tunnel en sélectionnant **Network (Réseau)** > **IPSec Tunnels (Tunnels IPsec)** et vérifiez l'état actif indiqué par une icône verte.

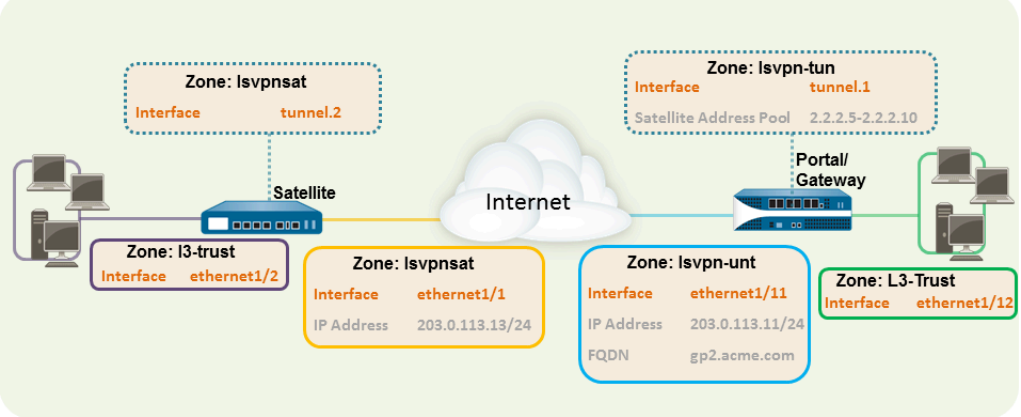
# Configurations rapides du LSVPN

Les sections suivantes fournissent des instructions détaillées sur la configuration de certains déploiements communs du LSVPN GlobalProtect :

- Configuration du LSVPN de base avec routage statique
- Configuration LSVPN avancée avec routage dynamique
- Configuration LSVPN avancée avec iBGP

## Configuration du LSVPN de base avec routage statique

Cette configuration rapide indique la méthode la plus rapide de mise en route et d'exécution avec le LSVPN. Dans cet exemple, un seul pare-feu situé au siège social est configuré à la fois en tant que portail et passerelle. Les satellites peuvent être déployés rapidement et facilement avec une configuration minime pour une meilleure évolutivité.




Le flux de travail suivant indique les étapes de cette configuration de base :

**STEP 1 |** Configurez une interface de couche 3.

Dans cet exemple, l'interface de Couche 3 sur le portail/la passerelle nécessite la configuration suivante :

- **Interface** : ethernet1/11
- **Security Zone (Zone de sécurité)** : lsvpn-tun
- **IPv4 (IPv4)** : 203.0.113.11/24

**STEP 2 |** Sur le ou les pare-feu hébergeant la ou les passerelles GlobalProtect, configurez l'interface de tunnel logique qui terminera les tunnels VPN établis par les satellites GlobalProtect.

*Pour activer la visibilité des utilisateurs et des groupes se connectant sur le VPN, activez User-ID dans la zone où se terminent les tunnels VPN.*

Dans cet exemple, l'interface de tunnel sur le portail/la passerelle nécessite la configuration suivante :

- **Interface** : tunnel.1
- **Security Zone (Zone de sécurité)** : lsvpn-tun

**STEP 3 |** Créez la règle de politique de sécurité pour autoriser le flux de trafic dans la zone VPN où se termine le tunnel (lsvpn-tun) et dans la zone approuvée où se trouvent les applications d'entreprise (L3-Trust).

Reportez-vous à la section Création d'une règle de politique de sécurité.

**STEP 4 |** Affectez un profil de service SSL/TLS au portail/à la passerelle. Le profil doit faire référence à un certificat de serveur auto-signé.

Le nom du certificat doit correspondre au FQDN ou à l'adresse IP de l'interface de Couche 3 créée pour le portail/la passerelle.

1. Sur le pare-feu hébergeant le portail GlobalProtect, créez le certificat CA racine pour la signature des certificats des composants GlobalProtect. Dans cet exemple, le certificat CA racine, **`lsvpn-CA`**, sera utilisé pour générer le certificat de serveur de ce portail/cette passerelle. Le portail utilisera également ce certificat CA racine pour signer les CSR provenant des satellites.
2. Créez des profils de service SSL/TLS pour le portail et les passerelles GlobalProtect.

   Comme le portail et la passerelle se trouvent sur la même interface dans cet exemple, ils peuvent partager un profil de service SSL/TLS qui utilise le même certificat de serveur. Dans cet exemple, le profil est nommé **`lsvpnserver`**.

**STEP 5 |** Créez un profil de certificat.

Dans cet exemple, le profil de certificat **`lsvpn-profile`** fait référence au certificat CA racine **`lsvpn-CA`**. La passerelle utilisera ce profil de certificat pour authentifier les satellites tentant d'établir des tunnels VPN.

**STEP 6 |** Configurez un profil d'authentification que le portail utilisera si le numéro de série du satellite n'est pas disponible.

1. Créez un type de profil de serveur sur le portail.
   - Ajoutez un profil de serveur RADIUS.

     *Vous pouvez vous servir de RADIUS pour l'intégrer à un service d'*Authentification multifacteur**.**
   - Ajoutez un profil de serveur TACACS+.
   - Ajoutez un profil de serveur d'IDP en SAML.
   - Ajoutez un profil de serveur Kerberos.
   - Ajoutez un profil de serveur LDAP. Si vous utilisez LDAP pour vous connecter à Active Directory (AD), créez un profil de serveur LDAP distinct pour chaque domaine AD.
2. Configurez un profil d'authentification. Dans cet exemple, le profil **`lsvpn-sat`** est utilisé pour authentifier des satellites.

**STEP 7 |** Configuration de passerelles GlobalProtect pour le LSVPN.

Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Gateways (Passerelles)** et **Add (Ajoutez)** une configuration. Cet exemple nécessite la configuration de passerelle suivante :

- **Interface** : ethernet1/11
- **IP Address (Adresse IP)** : 203.0.113.11/24
- **SSL/TLS Server Profile (Profil de serveur SSL/TLS)** : lsvpnserver
- **Certificate Profile (Profil de certificat)** : lsvpn-profile
- **Tunnel Interface (Interface de tunnel)** : tunnel.1
- **Primary DNS/Secondary DNS (DNS principal/DNS secondaire)** : 4.2.2.1/4.2.2.2
- **IP Pool (Pool d'adresses IP)** : 2.2.2.111-2.2.2.120
- **Access Route (Itinéraire d'accès)** : 10.2.10.0/24

**STEP 8 |** Configuration du portail.

Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portal (Portail)** et **Add (Ajoutez)** une configuration. Cet exemple nécessite la configuration de portail suivante :

- **Interface** : ethernet1/11
- **IP Address (Adresse IP)** : 203.0.113.11/24
- **SSL/TLS Server Profile (Profil de serveur SSL/TLS)** : lsvpnserver
- **Authentication Profile (Profil d'authentification)** : lsvpn-sat

**STEP 9 |** Définition des configurations de satellites.

Dans l'onglet **Satellite (Satellite)** de la configuration de portail, puis cliquez sur **Add (Ajouter)** pour ajouter une configuration de satellite et une CA racine de confiance, puis spécifiez la CA que

le portail utilisera pour générer des certificats pour les satellites. Dans cet exemple, les paramètres requis sont les suivants :

- **Gateway (Passerelle)** : 203.0.113.11
- **Issuing Certificate (Publication du certificat)** : lsvpn-CA
- **Trusted Root CA (Autorité de certification racine de confiance)** : lsvpn-CA

**STEP 10 |** Préparation du satellite pour l'association au LSVPN.

La configuration de satellite dans cet exemple nécessite les paramètres suivants :

Configuration de l'interface

- Interface de couche 3 : ethernet1/1, 203.0.113.13/24
- Interface de tunnel : tunnel.2
- Zone : lsvpnsat

Certificat CA racine du portail

- lsvpn-CA

Configuration du tunnel IPSec

- **Tunnel Interface (Interface de tunnel)** : tunnel.2
- **Portal Address (Adresse du portail)** : 203.0.113.11
- **Interface** : ethernet1/1
- **Local IP Address (Adresse IP locale)** : 203.0.113.13/24
- **Publish all static and connected routes to Gateway (Publier tous les itinéraires statiques et connectés sur la passerelle)** : activé

## Configuration LSVPN avancée avec routage dynamique

Dans les déploiements de LSVPN de plus grande envergure comprenant plusieurs passerelles et de nombreux satellites, consacrer un peu plus de temps lors de la configuration initiale afin de configurer le routage dynamique permet de simplifier la maintenance des configurations de passerelles, car les itinéraires d'accès seront mis à jour de manière dynamique. L'exemple de configuration suivant illustre comment étendre la configuration LSVPN de base pour configurer OSPF comme protocole de routage dynamique.

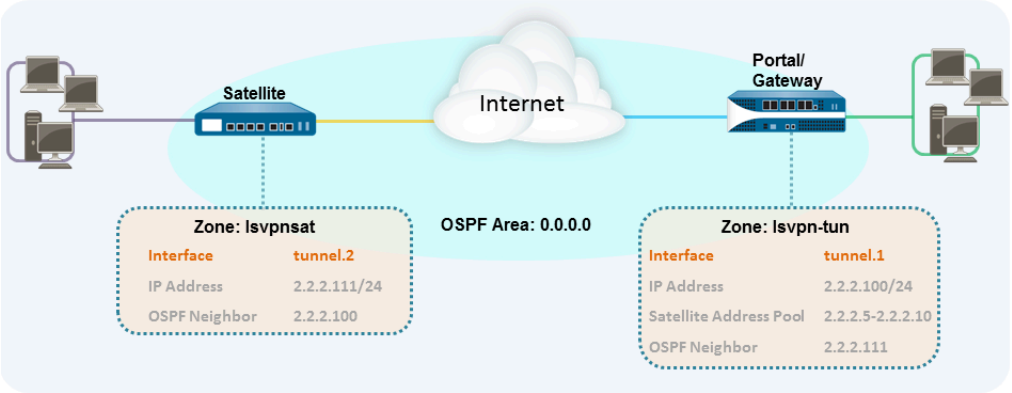
La configuration d'un LSVPN afin d'utiliser OSPF pour le routage dynamique implique les étapes supplémentaires suivantes sur les passerelles et les satellites :

- Affectation manuelle d'adresses IP afin de tunnelliser les interfaces sur toutes les passerelles et tous les satellites.
- Configuration d'OSPF point-à-multipoint (P2MP) sur le routeur virtuel de toutes les passerelles et de tous les satellites. De plus, dans le cadre de la configuration d'OSPF sur chaque passerelle, vous devez définir manuellement l'adresse IP de tunnel de chaque satellite en tant que voisin OSPF. De même, sur chaque satellite, vous devez définir manuellement l'adresse IP de tunnel de chaque passerelle en tant que voisin OSPF.

Bien que le routage dynamique implique une configuration supplémentaire lors de la configuration initiale du LSVPN, il réduit les tâches de maintenance liées à la mise à jour des itinéraires en cas de changement de topologie sur votre réseau.

La figure suivante illustre une configuration de LSVPN avec routage dynamique. Cet exemple illustre comment configurer OSPF comme protocole de routage dynamique pour le VPN.




Pour la configuration de base d'un LSVPN, suivez les étapes de la section Configuration du LSVPN de base avec routage statique. Vous pouvez ensuite suivre les étapes du flux de travail suivant afin d'étendre la configuration pour utiliser le routage dynamique au lieu du routage statique.

**STEP 1 |** Ajoutez une adresse IP à la configuration de l'interface de tunnel sur chaque passerelle et chaque satellite.

Suivez les étapes ci-dessous sur chaque passerelle et chaque satellite :

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Tunnel (Tunnel)**, puis sélectionnez la configuration tunnel que vous avez créée pour le LSVPN afin d'ouvrir la boîte de dialogue Interface de tunnel.

   Si vous n'avez pas déjà créé l'interface de tunnel, reportez-vous à l'étape 2 de la section Create Interfaces and Zones for the LSVPN (Création d'interfaces et de zones pour le LSVPN).
2. Dans l'onglet **IPv4 (IPv4)**, cliquez sur **Add (Ajouter)**, puis saisissez une adresse IP et un masque de sous-réseau. Par exemple, pour ajouter une adresse IP pour l'interface de tunnel de la passerelle, saisissez 2.2.2.100/24.
3. Cliquez sur **OK** pour enregistrer la configuration.

**STEP 2 |** Configurez le protocole de routage dynamique sur la passerelle.

Pour configurer OSPF sur la passerelle :

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et choisissez le routeur virtuel associé à vos interfaces VPN.
2. Dans l'onglet **Zones (Zones)**, cliquez sur **Add (Ajouter)** pour créer la zone principale ou, si elle est déjà configurée, cliquez sur l'ID de zone pour la modifier.
3. Si vous créez une nouvelle zone, saisissez un **Area ID (ID de zone)** dans l'onglet **Type (Type)**.
4. Dans l'onglet **Interface (Interface)**, cliquez sur **Add (Ajouter)** et sélectionnez l'**Interface (Interface)** de tunnel que vous avez créée pour le LSVPN.
5. Sélectionnez **p2mp (p2mp)** comme **Link Type (Type de lien)**.
6. Cliquez sur **Add (Ajouter)** dans la section Neighbors (Voisins), puis saisissez l'adresse IP de l'interface de tunnel de chaque satellite, par exemple, 2.2.2.111.
7. Cliquez deux fois sur **OK ( OK)** pour enregistrer la configuration du routeur virtuel, puis **Commit (Validez)** les modifications sur la passerelle.
8. Répétez cette étape chaque fois que vous ajoutez un nouveau satellite au LSVPN.

**STEP 3 |** Configurez le protocole de routage dynamique sur le satellite.

Pour configurer OSPF sur le satellite :

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et choisissez le routeur virtuel associé à vos interfaces VPN.
2. Dans l'onglet **Zones (Zones)**, cliquez sur **Add (Ajouter)** pour créer la zone principale ou, si elle est déjà configurée, cliquez sur l'ID de zone pour la modifier.
3. Si vous créez une nouvelle zone, saisissez un **Area ID (ID de zone)** dans l'onglet **Type (Type)**.
4. Dans l'onglet **Interface (Interface)**, cliquez sur **Add (Ajouter)** et sélectionnez l'**Interface (Interface)** de tunnel que vous avez créée pour le LSVPN.
5. Sélectionnez **p2mp (p2mp)** comme **Link Type (Type de lien)**.
6. Cliquez sur **Add (Ajouter)** dans la section Voisins, puis saisissez l'adresse IP de l'interface de tunnel de chaque passerelle GlobalProtect, par exemple, 2.2.2.100.
7. Cliquez deux fois sur **OK ( OK)** pour enregistrer la configuration du routeur virtuel, puis **Commit (Validez)** les modifications sur la passerelle.
8. Répétez cette étape chaque fois que vous ajoutez une nouvelle passerelle.

**STEP 4 |** Vérifiez que les passerelles et les satellites peuvent former des adjacences de routeur.

- Sur chaque satellite et chaque passerelle, vérifiez que des adjacences homologues sont formées et que des entrées de table de routage ont été créées pour les homologues (à savoir que les satellites comprennent des itinéraires vers les passerelles et vice versa). Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, puis cliquez sur le lien **More Runtime Stats (Plus de statistiques d'exécution)** du routeur virtuel utilisé pour le LSVPN. Dans l'onglet Routage, vérifiez que l'homologue du LSVPN comporte un itinéraire.
- Dans l'onglet **OSPF (OSPF)** > **Interface (Interface)**, vérifiez que le **Type (Type)** est **p2mp (p2mp)**.

- Dans l'onglet **OSPF (OSPF)** > **Neighbor (Voisin)**, vérifiez que les pare-feu hébergeant vos passerelles ont établi des adjacences de routeur avec les pare-feu hébergeant vos satellites, et vice versa. Vérifiez également que le **Status (État)** est **Full (Complet)** qui signifie que des adjacences complètes ont été établies.

## Configuration LSVPN avancée avec iBGP

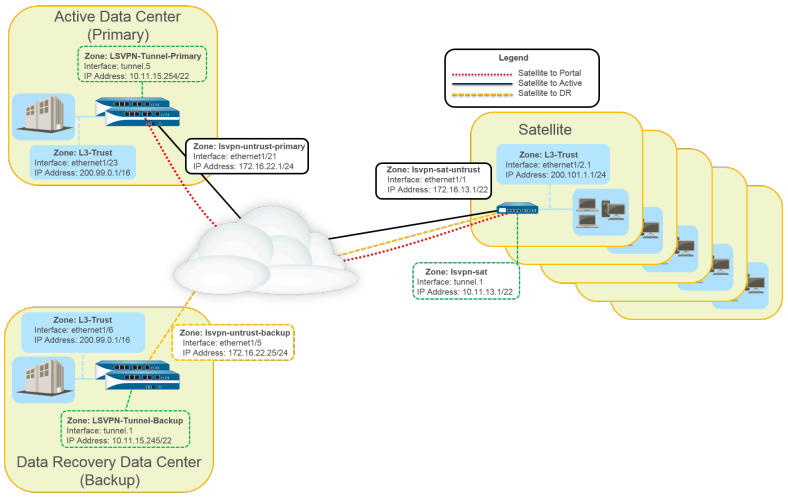
Ce cas pratique illustre la manière dont le LSVPN GlobalProtect relie en toute sécurité des succursales distantes à des centres de données principaux et de reprise après sinistre qui hébergent des applications critiques pour les utilisateurs et la manière dont le internal border gateway protocol (protocole de passerelle frontière interne ; iBGP) facilite le déploiement et la maintenance. Grâce à cette méthode, vous pouvez lier un maximum de 500 bureaux satellites à une seule passerelle.

BGP est un protocole d'acheminement dynamique hautement extensible qui convient parfaitement aux déploiements en étoile, comme LSVPN. En tant que protocole d'acheminement dynamique, il élimine considérablement la surcharge associée aux itinéraires d'accès (itinéraires statiques) en facilitant le déploiement des pare-feu satellites supplémentaires. Compte tenu de ses fonctions et capacités de filtrage des itinéraires (p. ex., plusieurs minuteurs réglables, atténuation d'itinéraires et actualisation des itinéraires), le protocole BGP peut accepter un plus grand nombre de préfixes d'itinéraires avec une plus grande stabilité que les autres protocoles d'acheminement, comme RIP et OSPF. Dans le cas de iBGP, un groupe d'homologues, qui se compose de tous les satellites et de toutes les passerelles du déploiement LSVPN, établit des adjacences sur les points d'extrémité du tunnel. Le protocole prend alors implicitement le contrôle de publications d'itinéraire, des mises à jour et de la convergence.

Dans cet exemple de configuration, une paire HA active/passive de pare-feu PA-5200 est déployée dans le centre de données principal (actif) et fait office de portail et de passerelle principale. Le centre de données de reprise après sinistre dispose de deux pare-feu PA-5200 dans une paire HA active/passive faisant office de passerelle LSVPN de secours. Le portail et les passerelles desservent 500 pare-feu PA-220 déployés en tant que satellites LSVPN dans les filiales.

Les deux centres de données publient des itinéraires, qui possèdent toutefois des mesures différentes. Par conséquent, les satellites privilégient les itinéraires du centre de données actif et les installent. Cependant, les itinéraires de secours sont également présents dans la Routing Information Base (base d'informations de routage ; RIB). En cas d'échec du centre de données actif, les itinéraires publiés par ce dernier sont supprimés et remplacés par des itinéraires du centre de données de reprise après sinistre. Le délai de basculement dépend des délais iBGP que vous avez sélectionnés et de la convergence du routage associée à iBGP.




Le flux de travail suivant indique les étapes à suivre pour configurer ce déploiement :

**STEP 1 |** Création d'interfaces et de zones pour le LSVPN.

Portail et passerelle principale :

- **Zone** : LSVPN-Untrust-Primary
- Interface : ethernet1/21
- Abandon d'IPv4 : 172.16.22.1/24
- **Zone** : l3-trust
- **Interface** : ethernet1/23
- **IPv4** : 200.99.0.1/16

Passerelle de secours :

- **Zone** : LSVPN-Untrust-Primary
- **Interface** : ethernet1/5
- **IPv4** : 172.16.22.25/24
- **Zone** : l3-trust
- **Interface** : ethernet1/6
- **IPv4** : 200.99.0.1/16

Satellite :

- **Zone** : LSVPN-Sat-Untrust
- **Interface** : ethernet1/1
- **IPv4** : 172.16.13.1/22
- **Zone** : l3-trust
- **Interface** : ethernet1/2.1
- **IPv4** : 200.101.1.1/24

*Configurez les zones, les interfaces et les adresses IP sur chaque satellite. L'interface et l'adresse IP locale varieront d'un satellite à l'autre. Cette interface est utilisée pour la connexion VPN au portail et à la passerelle.*

**STEP 2 |** Sur le ou les pare-feu hébergeant la ou les passerelles GlobalProtect, configurez l'interface de tunnel logique qui terminera les tunnels VPN établis par les satellites GlobalProtect.

**Passerelle principale** :

- **Interface** : tunnel.5
- **IPv4** : 10.11.15.254/22
- **Zone** : LSVPN-Tunnel-Primary

**Passerelle de secours** :

- **Interface** : tunnel.1
- **IPv4** : 10.11.15.245/22
- **Zone** : LSVPN-Tunnel-Backup

**STEP 3 |** Activation de SSL entre des composants du LSVPN GlobalProtect.

La passerelle utilise la Certificate Authority (autorité de certification ; CA) racine autosignée pour délivrer des certificats pour les satellites du LSVPN GlobalProtect. Puisqu'un pare-feu héberge la passerelle principale et le portail, un seul certificat est utilisé pour l'authentification aux satellites. La même CA est utilisée pour générer un certificat pour la passerelle de secours. La CA génère des certificats qui sont transmis aux satellites à partir du portail, puis utilisés par les satellites pour s'authentifier auprès des passerelles.

Vous devez également générer un certificat à partir de la même CA pour la passerelle de secours, ce qui lui permet de s'authentifier auprès des satellites.

1. Sur le pare-feu hébergeant le portail GlobalProtect, créez le certificat CA racine pour la signature des certificats des composants GlobalProtect. Dans cet exemple, le certificat CA racine s'appelle CA-cert.
2. Créez des profils de service SSL/TLS pour le portail et les passerelles GlobalProtect. Puisque le portail et la passerelle principale GlobalProtect se trouvent sur la même interface de pare-feu, vous pouvez utiliser le même certificat de serveur pour les deux composants.
   - **Certificat CA racine** : CA-Cert
   - **Nom du certificat** : LSVPN-Scale
3. Déployez les certificats de serveur auto-signés sur les passerelles.
4. Importez le certificat CA racine utilisé pour générer des certificats de serveur pour les composants du LSVPN.
5. Créez un profil de certificat.
6. Reprenez les étapes 2 à 5 sur la passerelle de secours en configurant les paramètres suivants :
   - **Certificat CA racine** : CA-cert
   - **Nom du certificat** : LSVPN-back-GW-cert

**STEP 4 |** Configuration de passerelles GlobalProtect pour le LSVPN.

1. Sélectionnez**Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Gateways (Passerelle)**et cliquez sur**Add (Ajouter)**.
2. À l'onglet**General (Général)**, donnez le nom**LSVPN-Scale** à la passerelle principale.
3. Sous**Network Settings (Paramètres réseau)**, sélectionnez**ethernet1/21** en tant qu'interface de la passerelle principale et saisissez**172.16.22.1/24** en tant qu'adresse IP.
4. À l'onglet**Authentication (Authentification)**, sélectionnez le certificat LSVPN-Scale créé à l'étape3.
5. Sélectionnez**Satellite (Satellite)** > **Tunnel Settings (Paramètres du tunnel)** et sélectionnez**Tunnel Configuration (Configuration du tunnel)**. Définissez la**Tunnel Interface (Interface du tunnel)** sur tunnel.5. Tous les satellites de ce cas pratiques se connectent à une seule passerelle ; une seule configuration de satellite s'avère donc nécessaire. Les satellites sont mis en correspondance selon leur numéro de série ; aucun satellite ne doit s'authentifier en tant qu'utilisateur.
6. Sous**Satellite (Satellite)** > **Network Settings (Paramètres réseau)**, définissez le pool d'adresses IP à affecter à l'interface de tunnel sur le satellite une fois la connexion VPN

établie. Puisque ce cas pratique repose sur un acheminement dynamique, le paramètre relatif aux itinéraires d'accès demeure vide.

7. Reprenez les étapes 1 à 5 sur la passerelle de secours en configurant les paramètres suivants :
   - **Name (Nom)** : LSVPN-backup
   - **Interface de la passerelle** : ethernet1/5
   - **Adresse IP de la passerelle** : 172.16.22.25/24
   - **Certificat serveur** : LSVPN-backup-GW-cert
   - **Interface de tunnel** : tunnel.1

**STEP 5 |** Configurez le protocole iBGP sur les passerelles principale et de secours et ajoutez un profil de redistribution pour autoriser les satellites à injecter des itinéraires locaux sur les passerelles.

Chaque bureau satellite gère son propre réseau et son propre pare-feu. Ainsi, le profil de redistribution nommé ToAllSat est configuré de sorte à redistribuer les itinéraires locaux vers la passerelle GlobalProtect.

1. Sélectionnez**Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, puis**Add (Ajoutez)** un routeur virtuel.
2. Sous**Router Settings (Paramètres du routeur)**, ajoutez le**Name (Nom)** et l'**Interface (Interface)** du routeur virtuel.
3. Sous**Redistribution Profile (Profil de redistribution)**, sélectionnez**Add (Ajouter)**.
   1. Nommez le profil de redistribution**`ToAllSat`** et définissez la**Priority (Priorité)** sur 1.
   2. Définissez la redistribution sur**Redist (Redistribution)**.
   3. **Add (Ajoutez)**`ethernet1/23` à partir de la liste déroulante Interface (Interface).
   4. Cliquez sur**OK**.
4. Pour configurer le protocole BGP, sélectionnez**BGP (BGP)** sur le routeur virtuel.
   1. Sous**BGP (BGP)** > **General (Général)**, sélectionnez**Enable (Activer)**.
   2. Saisissez l'adresse IP de la passerelle en tant que**Router ID (ID de routeur)** `172.16.22.1`) et`1000` en tant que**AS Number (Numéro de l'AS)**.
   3. Dans la section Options (Options), sélectionnez**Install Route (Installer l'itinéraire)**.
   4. Sous**BGP (BGP)** > **Peer Group (Groupe d'homologues)**, cliquez sur**Add (Ajouter)** pour ajouter un groupe d'homologues comprenant tous les satellites qui se connecteront à la passerelle.
   5. Sous**BGP (BGP)** > **Redist Rules (Règles de redistribution)**,**Add (Ajoutez)** le profil de redistribution**`ToAllSat`** que vous avez précédemment créé.
5. Cliquez sur**OK**.
6. Reprenez les étapes 1 à 5 sur la passerelle de secours en utilisant**`ethernet1/6`** pour le profil de redistribution.

**STEP 6 |** Préparation du satellite pour l'association au LSVPN.

La configuration illustrée est un exemple d'un satellite unique.

Répétez cette configuration chaque fois que vous ajoutez un nouveau satellite au déploiement LSVPN.

1. Configurez une interface de tunnel comme point de terminaison de la connexion VPN aux passerelles.
2. Définissez le type de tunnel IPSec sur satellite GlobalProtect et saisissez l'adresse IP du portail GlobalProtect.
3. Sélectionnez**Network (Réseau)** > **Virtual Routers (Routeurs virtuels)**, puis**Add (Ajoutez)** un routeur virtuel.
4. Sous**Router Settings (Paramètres du routeur)**, ajoutez le**Name (Nom)** et l'**Interface (Interface)** du routeur virtuel.
5. Sélectionnez**Virtual Router (Routeur virtuel)** > **Redistribution Profile (Profil de redistribution)**, puis**Add (Ajoutez)** un profil comportant les paramètres suivants.
   1. Nommez le profil de redistribution**`ToLSVPNGW`** et définissez la**Priority (Priorité)** sur 1.
   2. **Add (Ajoutez)** une**Interface (Interface)****`ethernet1/2.1`**.
   3. Cliquez sur**OK**.
6. Sélectionnez**BGP (BGP)** > **General (Général)**,**Enable (Activez)** le protocole BGP et configurez-le comme suit :
   1. Saisissez l'adresse IP de la passerelle en tant que**Router ID (ID de routeur)** **`172.16.22.1`**) et**`1000`** en tant que**AS Number (Numéro de l'AS)**.
   2. Dans la section Options (Options), sélectionnez**Install Route (Installer l'itinéraire)**.
   3. Sous**BGP (BGP)** > **Peer Group (Groupe d'homologues)**,**Add (Ajoutez)** un groupe d'homologues comprenant tous les satellites qui se connecteront à la passerelle.
   4. Sous**BGP (BGP)** > **Redist Rules (Règles de redistribution)**,**Add (Ajoutez)** le profil de redistribution**`ToLSVPNGW`** que vous avez précédemment créé.
7. Cliquez sur**OK**.

**STEP 7 |** Configuration du portail GlobalProtect pour le LSVPN.

Les deux centres de données publient leurs itinéraires, mais avec des priorités de routage différentes, pour veiller à ce que le centre de données actif soit la passerelle privilégiée.

1. Sélectionnez**Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)** et cliquez sur**Add (Ajouter)**.
2. Sous**General (Général)**, saisissez**`LSVPN-Portal`** en tant que nom de portail.
3. Sous**Network Settings (Paramètres réseau)**, sélectionnez**`ethernet1/21`** en tant qu**Interface (Interface)** et sélectionnez**`172.16.22.1/24`** en tant qu**IP Address (Adresse IP)**.
4. À l'onglet**Authentication (Authentification)**, sélectionnez le profil SSL/TLS de la passerelle principale**`LSVPN-Scale`** que vous avez précédemment créé dans le menu déroulant**SSL/TLS Service Profile (Profil de service SSL/TLS)**.
5. À l'onglet**Satellite (Satellite)**,**Add (Ajoutez)** un satellite et**Name (Nommez)**-le**`sat-config-1`**.
6. Définissez la**Configuration Refresh Interval (Configuration de l'intervalle d'actualisation)** sur**`12`**.
7. Sous**GlobalProtect Satellite (Satellite GlobalProtect)** > **Devices (Périphériques)**, ajoutez le numéro de série et le nom d'hôte de chaque périphérique satellite du LSVPN.
8. Sous**GlobalProtect Satellite (Satellite GlobalProtect)** > **Gateways (Passerelles)**, ajoutez le nom et l'adresse IP de chaque passerelle. Définissez la priorité de routage de la passerelle principale sur 1 et celle de la passerelle de secours sur 10 pour veiller à ce que le centre de données actif soit la passerelle privilégiée.

**STEP 8 |** Vérification de la configuration du LSVPN.

**STEP 9 |** Facultatif) Ajoutez un nouveau site au déploiement LSVPN.

1. Sélectionnez**Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)** > **GlobalProtect Portal (Portail GlobalProtect)** > **Satellite Configuration (Congiguration du satellite)** > **GlobalProtect Satellite (Satellite GlobalProtect)** > **Devices (Périphériques)** pour ajouter le numéro de série du nouveau satellite au portail GlobalProtect.
2. Configurez le tunnel IPSec sur le satellite avec l'adresse IP du portail GlobalProtect.
3. Sélectionnez**Network (Réseau)** > **Virtual Router (Routeur virtuel)** > **BGP (BGP)** > **Peer Group (Groupe d'homologues)** pour ajouter le satellite à la configuration du groupe d'homologues BGP sur chaque passerelle.
4. Sélectionnez**Network (Réseau)** > **Virtual Router (Routeur virtuel)** > **BGP (BGP)** > **Peer Group (Groupe d'homologues)** pour ajouter les passerelles à la configuration du groupe d'homologues BGP sur le nouveau satellite.

# Politique

Les stratégies vous permettent d'appliquer des règles et d'agir. Les différents types de règles de politique que vous pouvez créer sur le pare-feu sont : sécurité, NAT, qualité de service (QoS), transfert basé sur une politique (PBF), décryptage, contrôle prioritaire sur l'application, authentification, déni de service (DoS) et protection de zone. Toutes ces différentes politiques œuvrent ensemble pour autoriser, refuser, définir la priorité, transférer, crypter, décrypter, faire des exceptions, authentifier un accès et réinitialiser les connexions, si nécessaire, pour sécuriser votre réseau. Les rubriques suivantes décrivent l'utilisation des politiques :

# Types de politique

Le pare-feu de dernière génération Palo Alto Networks prend en charge différents types de politique qui fonctionnent conjointement pour activer en toute sécurité les applications sur votre réseau.

Pour tous les types de politiques, lorsque vous Application de la description, de l'étiquette ou du commentaire d'audit d'une règle de politique, vous pouvez utiliser l'archive des commentaires d'audit pour consulter les modifications apportées à une règle de politique au fil du temps. L'archive, qui comprend l'historique des commentaires d'audit et les journaux de configuration, vous permet de comparer les versions de configuration et d'examiner la personne qui les a créées ou modifiées et pourquoi.

| Type de politique | Description |
|---|---|
| Sécurité | Détermine si une session doit être bloquée ou autorisée en fonction des attributs du trafic comme la zone de sécurité source et de destination, l'adresse IP source et de destination, l'application, l'utilisateur et le service. Pour de plus amples détails, reportez-vous à la section Politique de sécurité. |
| NAT | Indique au pare-feu les paquets devant être traduits et la manière dont la traduction doit être effectuée. Le pare-feu prend en charge la traduction de l'adresse et/ou du port source et la traduction de l'adresse et/ou du port de destination. Pour plus d'informations, reportez-vous à NAT. |
| QoS | Identifie le trafic nécessitant un traitement QoS (traitement préférentiel ou à bande passante limitée) à l'aide d'un ou plusieurs paramètres définis et de leur affectation à une classe. Pour plus d'informations, reportez-vous à la section Qualité de service. |
| Policy-Based Forwarding (transfert basé sur une politique - PBF) | Identifie le trafic qui doit utiliser une autre interface de sortie que celle qui serait normalement utilisée en fonction de la table de routage. Pour plus détails, reportez-vous à la section Transfert basé sur une politique. |
| Déchiffrement | Identifie le trafic crypté à des fins de visibilité, contrôle et sécurité granulaire. Pour plus d'informations, reportez-vous à la section Déchiffrement . |
| Contrôle prioritaire sur l'application | Identifie les sessions que vous ne souhaitez pas voir traitées par le moteur App-ID, qui est une inspection de la Couche 7. Le trafic correspondant à une politique de contrôle prioritaire sur l'application force le pare-feu à gérer la session comme un pare-feu à inspection d'état régulière de la Couche 4. Pour plus d'informations, reportez-vous à la section Gestion des applications personnalisées ou inconnues. |

| Type de politique | Description |
| --- | --- |
| Authentification | Identifie le trafic qui exige que les utilisateurs s'authentifient. Pour de plus amples détails, reportez-vous à la section Politique d'authentification. |
| Protection DoS | Identifie les attaques de déni de service (DoS) et prend des mesures de protection en cas de correspondance des règles. Pour plus d'informations, reportez-vous à la section Profil de protection DoS. |

# Politique de Sécurité

La politique de sécurité protège les actifs du réseau des menaces et des défaillances et permet d'optimiser l'allocation des ressources du réseau afin d'améliorer la productivité et l'efficacité des processus métier. Sur un pare-feu Palo Alto Networks, les règles de politique de sécurité individuelles déterminent si une session doit être bloquée ou autorisée en fonction des attributs du trafic comme la zone de sécurité source et de destination, l'adresse IP source et de destination, l'application, l'utilisateur et le service.

***Pour s'assurer que les utilisateurs finaux s'authentifient lorsqu'ils essaient d'accéder à vos ressources réseau, le pare-feu évalue la*** Politique d'Authentification ***avant la politique de Sécurité.***

Tout le trafic passant par le pare-feu est mis en correspondance avec une session et chaque session avec une règle de politique de sécurité. Lorsqu'une correspondance de session se produit, le pare-feu applique la règle de politique de sécurité correspondante au trafic bidirectionnel (du client vers le serveur et du serveur vers le client) dans cette session. Pour le trafic qui ne correspond à aucune règle définie, les règles par défaut s'appliquent. Les règles par défaut, qui s'affichent en bas de la base des règles de sécurité, sont prédéfinies pour autoriser l'ensemble du trafic intra-zone (au sein d'une zone) et refuser le trafic inter-zone (entre les zones). Bien que ces règles fassent partie de la configuration prédéfinie et soient en lecture seule par défaut, vous pouvez les forcer afin de modifier un nombre limité de paramètres, notamment les étiquettes, l'action (autoriser ou bloquer), les paramètres des journaux et les profils de sécurité.

Les règles de politique de sécurité sont évaluées de gauche à droite et de haut en bas. Une correspondance est établie entre un paquet et la première règle répondant aux critères définis et, après avoir déclenché une correspondance, les règles suivantes ne sont pas évaluées. Par conséquent, les règles les plus spécifiques doivent précéder les plus génériques afin d'appliquer les meilleurs critères de correspondance. Le trafic correspondant à une règle génère une entrée de journal à la fin de la session dans le journal de trafic si vous activez la journalisation pour cette règle. Les options de journalisation sont configurables pour chaque règle et la journalisation peut, par exemple, être configurée en début de session au lieu ou en plus d'être configurée en fin de session.

Après qu'un administrateur configure une règle, vous pouvez consulter l'Affichage de l'utilisation de la règle de politique pour déterminer quand et combien de fois le trafic correspond à la règle de politique de sécurité dans le but d'en déterminer l'efficacité. Au fur et à mesure de l'évolution de votre base de règle, les informations sur les changements et les audits sont perdus, sauf si vous les avez archivées lors de la création ou de la modification de la règle. Vous pouvez Application de la description, de l'étiquette ou du commentaire d'audit d'une règle de politique pour veiller à ce que tous les administrateurs saisissent des commentaires d'audit afin de pouvoir afficher l'archive des commentaires d'audit et passer en revue les commentaires et l'historique du journal de configuration et pour pouvoir comparer les versions de configuration d'une règle sélectionnée. Ensemble, vous avez maintenant une visibilité et un contrôle accrus de la base de règles.

- Composants d'une règle de politique de sécurité
- Actions de la politique de sécurité
- Création d'une règle de politique de sécurité

# Composants d'une règle de politique de sécurité

La formulation d'une règle de politique de sécurité permet de combiner les champs obligatoires et facultatifs détaillés dans le tableau suivant :

| Obligatoi Facultati | Champ | Description |
|---|---|---|
| requis | **Name (Nom)** | Une étiquette (63 caractères maximum) qui identifie la règle. |
| | **UUID** | Le Universally Unique Identifier (identifiant unique universel ; UUID) est une chaîne distincte de 32 caractères qui identifie de manière permanente les règles pour que vous puissiez suivre une règle, peu importe les changements qui y sont apportés, comme le nom. |
| | **Type de règle** | Indique si la règle s'applique au trafic dans une zone, entre des zones ou aux deux :<br>• **universal (universel)** (par défaut) : applique la règle à l'ensemble du trafic inter-zone et intra-zone correspondant dans les zones source et de destination indiquées. Par exemple, si vous créez une règle universelle pour les zones source A et B et de destination A et B, la règle s'applique à l'ensemble du trafic dans la zone A, dans la zone B, ainsi que de la zone A à la zone B et de la zone B à la zone A.<br>• **intrazone (intra-zone)** : applique la règle à l'ensemble du trafic correspondant dans les zones source indiquées (vous ne pouvez pas indiquer de zone de destination pour les règles intra-zone). Par exemple, si vous définissez la zone source sur A et B, la règle s'applique à l'ensemble du trafic dans les zones A et B, mais pas entre les zones A et B.<br>• **interzone (inter-zone)** : applique la règle à l'ensemble du trafic correspondant entre les zones source et de destination indiquées. Par exemple, si vous définissez la zone source sur A, B et C, et la zone de destination sur A et B, la règle s'applique à l'ensemble du trafic de la zone A à la zone B, de la zone B à la zone A, de la zone C à la zone A, de la zone C à la zone B, mais pas au trafic dans les zones A, B et C. |
| | **Source Zone (Zone source)** | Zone d'où provient le trafic. |
| | **Destination Zone (Zone de destination)** | Zone dans laquelle se termine le trafic. Si vous utilisez la traduction NAT, veillez à toujours faire référence à la zone post-NAT. |
| | **Application** | Application que vous voulez contrôler. Le pare-feu utilise App-ID, la technologie de classification du trafic, pour identifier le trafic sur votre réseau. App-ID permet de contrôler les applications et |

| Obligatoi Facultati | Champ | Description |
|---|---|---|
| | | la visibilité afin de créer des politiques de sécurité qui bloquent des applications inconnues, tout en activant, en inspectant et en modelant celles étant autorisées. |
| | **Action (Action)** | Indique une action ***Autoriser*** ou ***Refuser*** pour le trafic en fonction des critères que vous avez définis dans la règle. Lorsque vous configurez le pare-feu pour qu'il refuse le trafic, il réinitialise la connexion ou effectue un abandon silencieux des paquets. Afin de procurer une expérience utilisateur plus agréable, vous pouvez configurer des options granulaires pour refuser le trafic plutôt que d'abandonner silencieusement des paquets, ce qui peut entraîner l'interruption de certaines applications, qui peuvent sembler non réactives pour l'utilisateur. Pour de plus amples détails, reportez-vous à la section Actions de la politique de sécurité. |
| En option | **Étiquette** | Mot clé ou phrase vous permettant de filtrer les règles de sécurité, ce qui se révèle utile lorsque vous avez défini de nombreuses règles et que vous voulez ensuite passer en revue celles étiquetées avec un mot clé, par exemple : ***applications approuvées par les TI*** ou ***applications à risque élevé***. |
| | **Description** | Champ de texte allant jusqu'à 1024 caractères qui permet de décrire la règle. |
| | **Source Address (Adresse source)** | Définir les adresses IP des hôtes, les sous-réseaux, les objets d'adresse (de type masque de réseau IP, plage d'adresses IP, FQDN ou masque générique IP), les groupes d'adresses ou l'application selon le pays. Si vous utilisez la traduction NAT, veillez à toujours faire référence aux adresses IP d'origine dans le paquet (c'est-à-dire, les adresses IP pré-NAT). |
| | **Adresse de destination** | Emplacement ou destination du paquet. Définir les adresses IP, les sous-réseaux, les objets d'adresse (de type masque de réseau IP, plage d'adresses IP, FQDN ou masque générique IP), les groupes d'adresses ou l'application selon le pay. Si vous utilisez la traduction NAT, veillez à toujours faire référence aux adresses IP d'origine dans le paquet (c'est-à-dire, les adresses IP pré-NAT). |
| | **Utilisateur** | Utilisateur ou groupe d'utilisateurs auquel/auxquels s'applique la politique. User-ID doit être activé dans la zone. Pour ce faire, consultez la section Présentation de User-ID. |
| | **URL Category (Catégorie d'URL)** | L'utilisation de la catégorie d'URL comme critère de correspondance vous permet de personnaliser des profils de sécurité (antivirus, antispyware, blocage des fichiers, filtrage des données et déni de service) en fonction de la catégorie d'URL. Par exemple, vous pouvez empêcher le téléchargement/chargement d'un fichier .exe |

| Obligatoi Facultati | Champ | Description |
|---|---|---|
| | | à des catégories d'URL présentant les risques les plus élevés tout en l'autorisant aux autres catégories. Cette fonctionnalité vous permet également d'associer des calendriers à des catégories d'URL spécifiques (autorisation des sites Web pendant le déjeuner et en dehors des heures de travail) de signaler certaines catégories d'URL dotées d'une qualité de service et de sélectionner différents profils de transfert des journaux en fonction de la catégorie d'URL.<br><br>Bien que vous puissiez manuellement configurer les catégories d'URL sur votre pare-feu, pour profiter pleinement des mises à jour de catégorisation des URL dynamiques disponibles sur les pare-feu Palo Alto Networks, vous devez acquérir une licence de filtrage des URL.<br><br>*Pour bloquer ou autoriser le trafic selon la catégorie d'URL, vous devez appliquer un profil de filtrage des URL aux règles de politique de sécurité. Définissez la catégorie d'URL sur Indifférent, puis associez un profil de filtrage des URL à la politique de sécurité. Reportez-vous à la section* Configuration d'une politique de sécurité de base *pour plus d'informations sur l'utilisation des profils par défaut dans votre politique de sécurité.* |
| | **Service (Service)** | Vous permet de sélectionner un port de couche 4 (TCP ou UDP) pour l'application. Vous pouvez choisir ***Any (Indifférent)***, indiquer un port ou utiliser le port ***application-defaut (Par défaut de l'application)*** pour pouvoir utiliser le port standard de l'application. Par exemple, pour les applications disposant de numéros de port bien connus tels que DNS, l'option ***application-default (Par défaut de l'application)*** correspond au trafic DNS uniquement sur le port TCP 53. Vous pouvez également ajouter une application personnalisée et définir les ports que l'application peut utiliser.<br><br>*Pour les règles d'autorisation du trafic entrant (par exemple, de la zone non approuvée à la zone approuvée), l'utilisation de l'option Par défaut de l'application empêche l'exécution d'applications sur des ports ou protocoles inhabituels. Par défaut de l'application est l'option par défaut ; alors que le pare-feu vérifie toujours les applications sur tous les ports, dans cette configuration, les applications sont autorisées uniquement sur leurs ports/protocoles standard.* |

| Obligatoi Facultati | Champ | Description |
|---|---|---|
| | **Profils de sécurité** | Fournissent une protection supplémentaire contre les menaces, les vulnérabilités et les fuites de données. Les profils de sécurité sont uniquement évalués pour les règles dotées d'une action ***Autoriser***. |
| | **HIP Profile (Profil HIP)** (pour GlobalProtect) | Vous permet d'identifier les clients dotés d'un profil d'informations sur l'hôte (HIP) et d'appliquer les privilèges d'accès. |
| | **Options (Options)** | Vous permettent de définir la journalisation de la session, de consigner les paramètres de transfert, de modifier les marquages de qualité de service (QoS) des paquets correspondant à la règle, mais aussi de planifier le moment (jour et heure) où la règle de sécurité doit être effective. |

## Actions de la politique de sécurité

Pour le trafic correspondant aux attributs définis dans une politique de sécurité, vous pouvez appliquer les actions suivantes :

| Action (Action) | Description |
|---|---|
| **Allow (Autoriser)** (par défaut) | Autorise le trafic. |
| **Refuser** | Bloque le trafic et applique l'***action Refuser*** définie par défaut pour l'application refusée. Pour afficher l'action Refuser définie par défaut pour une application, consultez les détails de l'application dans **Objects (Objets)** > **Applications** ou vérifiez les détails de l'application dans Applipedia. |
| **Chutes** | Abandonne silencieusement le trafic ; dans le cas d'une application, cette action applique un contrôle prioritaire sur l'action Refuser par défaut. Aucune réinitialisation TCP n'est envoyée à l'hôte/application.<br><br>Pour les interfaces de Couche 3, pour envoyer, de façon facultative, une réponse ICMP inaccessible au client, définissez l'action : **Drop (Abandonner)** et cochez la case **Send ICMP Unreachable (Envoyer ICMP inaccessible)**. Lorsque cette option est activée, le pare-feu envoie le code ICMP qui indique que ***la communication avec la destination est interdite de manière administrative***—ICMPv4 : Type 3, Code 13 ; ICMPv6 : Type 1, Code 1. |
| **Réinitialiser le client** | Envoie une réinitialisation TCP au périphérique côté client. |

| Action (Action) | Description |
|---|---|
| **Réinitialiser le serveur** | Envoie une réinitialisation TCP au périphérique côté serveur. |
| **Réinitialiser les deux** | Envoie une réinitialisation TCP aux périphériques côté client et côté serveur. |

*Une réinitialisation n'est envoyée que lorsque la session est formée. Le pare-feu n'enverra pas de réinitialisation si la session est bloquée avant qu'une connexion en trois étapes ne soit effectuée.*

Dans le cas d'une session TCP pour laquelle une action Réinitialiser est configurée, le pare-feu n'envoie pas de réponse ICMP inaccessible.

Dans le cas d'une session UDP pour laquelle une action Abandonner ou Réinitialiser est configurée, si la case **ICMP Unreachable (ICMP inaccessible)** est cochée, le pare-feu envoie un message ICMP au client.

## Création d'une règle de politique de sécurité

**STEP 1 |** (Facultatif) Supprimez la règle de politique de sécurité par défaut.

Par défaut, le pare-feu inclut une règle de sécurité nommée ***règle1*** qui autorise tout trafic issu d'une zone de confiance vers une zone non approuvée. Vous pouvez supprimer cette règle ou la modifier afin qu'elle reflète votre convention de dénomination de zone.

**STEP 2 |** Ajoutez une règle.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis **Add (Ajoutez)** une nouvelle règle.
2. Dans l'onglet **General (Général)**, donnez un **Name (Nom)** descriptif à la règle.
3. Sélectionnez un **Rule Type (Type de règle)**.

**STEP 3 |** Définissez les critères de correspondance des champs sources du paquet.

1. Dans l'onglet **Source (Source)**, sélectionnez une **Source Zone (Zone source)**.
2. Précisez une **Source IP Address (Adresse IP source)** ou laissez la valeur définie sur **Any (Indifférent)**.

   *Si vous décidez de **Negate (Refuser)** une région comme **Source address (Adresse source)**, assurez-vous que toutes les régions qui contiennent des adresses IP privées sont ajoutées à la **Source Address (Adresse source)** afin d'éviter toute perte de connectivité entre ces adresses IP privées.*
3. Précisez un **User (Utilisateur)** source ou laissez la valeur définie sur **Any (Indifférent)**.

**STEP 4 |** Définissez les critères de correspondance des champs de destination du paquet.

1. Dans l'onglet **Destination (Destination)**, définissez la **Destination Zone (Zone de destination)**.
2. Précisez une **Destination IP Address (Adresse IP de destination)** ou laissez la valeur définie sur **Any (Indifférent)**.

*Si vous décidez de **Negate (Refuser)** une région comme **Destination address (Adresse de destination)**, assurez-vous que toutes les régions qui contiennent des adresses IP privées sont ajoutées à la **Destination Address (Adresse de destination)** afin d'éviter toute perte de connectivité entre ces adresses IP privées.*

*Il est recommandé d'utiliser des objets d'adresse comme **Destination Address (Adresse de destination)** pour autoriser l'accès uniquement à des serveurs ou des groupes de serveurs donnés, particulièrement pour des services fréquemment exploités, tels que DNS et SMTP. En restreignant les utilisateurs à des adresses de serveurs de destination, vous pouvez prévenir l'exfiltration de données et empêcher le trafic de commande et de contrôle d'établir une communication grâce à des techniques comme la tunnellisation DNS.*

**STEP 5 |** Précisez l'application que la règle autorisera ou interdira.

*Il est recommandé de toujours utiliser des règles de politique de sécurité basées sur des applications plutôt que des règles basées sur le port et de toujours définir le Service sur Par défaut de l'application, à moins que vous utilisiez une liste de ports plus restrictifs que les ports standard d'une application.*

1. À l'onglet **Applications (Applications)**, **Add (Ajoutez)** l'**Application (Application)** que vous souhaitez autoriser en toute sécurité. Vous pouvez sélectionner plusieurs applications ou vous pouvez utiliser des groupes d'applications ou des filtres d'applications.
2. À l'onglet **Service/URL Category (Service/Catégorie d'URL)**, laissez le service défini sur **application-default (par défaut de l'application)** pour garantir que les applications que la règle autorise ne soient autorisées que sur leurs ports standard.

**STEP 6 |** (Facultatif) Précisez une catégorie d'URL en tant que critère de correspondance de la règle.

Dans l'onglet **Service/URL Category (Service/Catégorie d'URL)**, sélectionnez la **URL Category (Catégorie d'URL)**.

Si vous sélectionnez une catégorie d'URL, seul le trafic WEB sera mis en correspondance avec la règle et seulement si le trafic est destiné à la catégorie précisée.

**STEP 7 |** Définissez l'action que le pare-feu doit prendre relativement au trafic qui correspond à la règle.

Dans l'onglet **Actions (Actions)**, sélectionnez une **Action (Action)**. Pour obtenir une description de chaque action, reportez-vous à la section Actions de la politique de sécurité.

**STEP 8 |** Configurez les paramètres des journaux

- Par défaut, la règle est définie sur **Log at Session End (Journaliser en fin de session)**. Vous pouvez désactiver ce paramètre si vous ne souhaitez pas que des journaux soient générés

lorsque du trafic est mis en correspondance avec cette règle ou vous pouvez sélectionner **Log at Session Start (Journaliser en début de session)** pour obtenir des journaux plus détaillés.

- Sélectionnez un profil de **Log Forwarding (Transfert des journaux)**.

*Il est recommandé de ne pas cocher la case **Disable Server Response Inspection (Désactiver l'inspection de la réponse du serveur)** (DSRI). Si vous cochez cette option, le pare-feu ne pourra pas inspecter les paquets transmis du serveur au client. Pour une sécurité optimale, le pare-feu doit inspecter les flux du client au serveur ainsi que les flux du serveur au client pour détecter et prévenir les menaces.*

**STEP 9 |** Associez des profils de sécurité pour permettre au pare-feu d'analyser tout le trafic autorisé afin d'y déceler des menaces.

*Assurez-vous de créer des profils de sécurité exemples qui protègent votre réseau contre les menaces connues et inconnues.*

À l'onglet **Actions (Actions)**, sélectionnez **Profiles (Profils)** dans la liste déroulante **Profile Type (Type de profil)**, puis sélectionnez les profils de sécurité individuels à associer à la règle.

Vous pouvez également sélectionner **Group (Groupe)** dans la liste déroulante **Profile Type (Type de profil)** et sélectionner un **Group Profile (Profil de groupe)** de sécurité à associer.

**STEP 10 |** Cliquez sur **Commit (Valider)** pour enregistrer la règle de politique dans la configuration active du pare-feu.

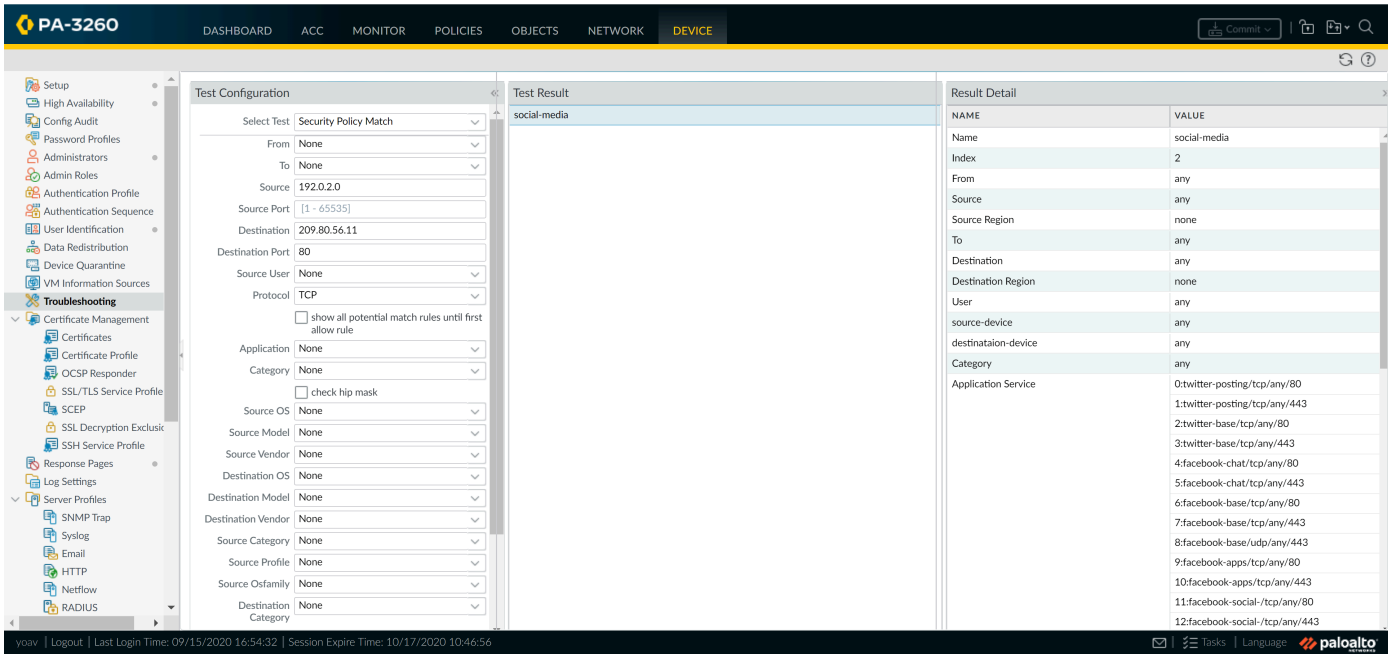
 

**STEP 11 |** Pour vérifier que vous avez correctement paramétré vos politiques de sécurité de base, testez si vos règles de politique de sécurité sont en cours d'évaluation et déterminez la règle de politique de sécurité qui s'applique à un flux de trafic.

La sortie affiche la meilleure règle correspondant à l'adresse IP source et de destination indiquée dans la commande de la CLI.

Par exemple, pour vérifier la règle de politique qui sera appliquée à un serveur du centre de données avec l'adresse IP 208.90.56.11 lorsqu'il accédera au serveur Microsoft Update :

1. Sélectionnez **Device (Périphérique)** > **Troubleshooting (Résolution des problèmes)**, puis sélectionnez **Security Policy Match (Correspondance de la politique de sécurité)** dans la liste déroulante Select Test (Sélectionner le test).
2. Saisissez les adresses IP source et de destination.
3. Saisissez le protocole.
4. **Execute (Exécutez)** le test de correspondance de la politique de sécurité.




**STEP 12 |** Après avoir attendu suffisamment longtemps pour permettre au trafic de traverser le pare-feu, affichez l'utilisation de la règle de politique pour surveiller l'état d'utilisation de la règle de politique et déterminer son efficacité.

# Objets de politique

Un ***objet de politique*** est un objet unique ou une unité collective regroupant des identités discrètes, comme des adresses IP, des URL, des applications ou des utilisateurs. Les objets de politiques étant une unité collective, vous pouvez référencer un objet dans une politique de sécurité au lieu de sélectionner manuellement plusieurs objets en même temps. En général, lors de la création d'un objet de politique, vous regroupez les objets nécessitant des autorisations similaires dans une politique. Par exemple : si votre organisation utilise un ensemble d'adresses IP du serveur pour authentifier les utilisateurs, vous pouvez regrouper l'ensemble de ces adresses en tant qu'objet de politique ***groupe d'adresses*** et faire référence au groupe d'adresses dans la politique de sécurité. En regroupant des objets, vous pouvez significativement réduire vos frais administratifs en créant des politiques.

***Si vous devez exporter des sections spécifiques de la configuration à des fins d'examen interne ou d'audit, vous pouvez procéder à l'***Exportation des données du tableau de configuration ***en tant que fichier PDF ou CSV.***

Vous pouvez créer les objets de politique suivants sur le pare-feu :

| Objet de politique | Description |
|---|---|
| Adresse/Groupe d'adresses, région | Vous permettent de regrouper des adresses sources ou de destination spécifiques nécessitant l'application d'une politique identique. L'objet adresse peut inclure une adresse IPv4 ou IPv6 (IP unique, plage, sous-réseau), une adresse IP générique (adresse IPv4/masque réseau générique) ou le FQDN. Une région peut également être définie par les coordonnées de latitude et de longitude ou vous pouvez sélectionner un pays et définir une adresse IP ou une plage d'adresses IP. Vous pouvez ensuite regrouper une collection d'objets adresse pour créer un objet groupe d'adresses.<br><br>Vous pouvez également utiliser des groupes d'adresses dynamiques pour mettre dynamiquement à jour des adresses IP dans des environnements où les adresses IP hôtes changent fréquemment.<br><br>***Les listes dynamiques externes prédéfinis (EDL) sur le pare-feu comptent dans le nombre maximum d'objets d'adresse qu'un modèle de pare-feu prend en charge.*** |
| Utilisateur/Groupe d'utilisateurs | Vous permet de créer une liste d'utilisateurs à partir de la base de données locale ou d'une base de données externe et de les regrouper. |
| Groupe d'applications et filtre d'applications | Un filtre d'applications vous permet de filtrer dynamiquement des applications. Vous pouvez filtrer et enregistrer un groupe d'applications en utilisant les attributs définis dans la base de données de l'application sur le pare-feu. Par exemple, vous pouvez procéder à la Création d'un filtre d'application selon un ou plusieurs attributs (catégorie, sous-catégorie, technologie, risque, caractéristiques). Grâce à |

| Objet de politique | Description |
| --- | --- |
| | un filtre d'applications, lors de la mise à jour du contenu, toute nouvelle application correspondant à vos critères de filtrage sera automatiquement ajoutée à votre filtre d'application enregistré.<br><br>Un groupe d'applications vous permet de créer un groupe statique d'applications spécifiques que vous voulez regrouper pour un groupe d'utilisateurs ou un service particulier, ou pour atteindre un objectif donné de la politique. Reportez-vous à la section Création d'un groupe d'applications. |
| Service/Groupes de services | Vous permettent de spécifier les ports sources et de destination, ainsi que le protocole qu'un service peut utiliser. Le pare-feu contient deux services prédéfinis (service-http et service-https) qui utilisent les ports TCP 80 et 8080 pour HTTP et le port TCP 443 pour HTTPS. Toutefois, vous pouvez créer n'importe quel service personnalisé sur n'importe quel port TCP/UDP de votre choix afin de limiter l'utilisation de l'application à des ports spécifiques (en d'autres termes, vous pouvez définir le port par défaut de l'application).<br><br>*Pour afficher les ports standard utilisés par une application, sous **Objects (Objets)** > **Applications**, recherchez l'application et cliquez sur le lien. Un bref descriptif s'affiche.* |

# Profils de sécurité

Alors que les règles de politique de sécurité vous permettent d'autoriser ou de bloquer le trafic sur votre réseau, les profils de sécurité servent à définir une règle ***autoriser mais analyser*** qui analyse les applications autorisées afin d'identifier les menaces, telles que les virus, les logiciels malveillants, les logiciels espions et les attaques DDOS. Lorsque le trafic correspond à la règle d'autorisation définie dans la politique de sécurité, le(s) profil(s) de sécurité qui est/sont associé(s) à la règle est/sont appliqué(s) à d'autres règles d'inspection du contenu, comme des analyses d'antivirus et un filtrage des données.

***Les profils de sécurité ne sont pas utilisés dans les critères de correspondance d'un flux de trafic. Un profil de sécurité est appliqué pour analyser le trafic après qu'une application ou une catégorie a été autorisée par la politique de sécurité.***

Le pare-feu fournit par défaut des profils de sécurité que vous pouvez directement utiliser pour commencer à protéger votre réseau des menaces. Reportez-vous à la section Configuration d'une politique de sécurité de base pour plus d'informations sur l'utilisation des profils par défaut dans votre politique de sécurité. Lorsque vous commencez à mieux comprendre les besoins en sécurité de votre réseau, reportez-vous à la section Création de profils de sécurité exemplaires pour la passerelle Internet pour en apprendre davantage sur la création de profils personnalisés.

***Pour connaître les recommandations relatives aux meilleures pratiques en matière de profils de sécurité, reportez-vous à la section*** Création de profils de sécurité exemplaires pour la passerelle Internet.

Vous pouvez ajouter des profils de sécurité généralement appliqués ensemble pour Créer un groupe de profils de sécurité ; cet ensemble de profils peut être traité comme une unité et ajouté à des politiques de sécurité en une seule étape (ou inclus par défaut dans des politiques de sécurité), si vous choisissez de configurer un groupe de profils de sécurité par défaut).

| Type de profil | Description |
|---|---|
| Profils antivirus | Les profils antivirus assurent une protection contre les virus, les vers et les chevaux de Troie, ainsi que contre le téléchargement de logiciels espions. À l'aide d'un moteur de prévention des logiciels malveillants basé sur les flux, qui inspecte le trafic dès la réception du premier paquet, la solution antivirus de Palo Alto Networks peut offrir aux clients une protection sans que les performances du pare-feu soient significativement altérées. Ce profil recherche une grande variété de logiciels malveillants dans les exécutables et les fichiers PDF, de virus HTML et JavaScript ; elle permet également l'analyse des fichiers compressés et des schémas de codage de données. Si vous avez activé le Décryptage sur le pare-feu, le profil permet également de rechercher du contenu décrypté.<br><br>Le profil par défaut inspecte tous les décodeurs de protocole répertoriés pour les virus, et génère des alertes pour les protocoles SMTP, IMAP et POP3, tout en bloquant les protocoles FTP, HTTP et SMB. Vous |

| Type de profil | Description |
|---|---|
| | pouvez configurer l'action pour un décodeur ou une signature antivirus et préciser la façon dont le pare-feu doit répondre à une menace :<br>• **Default (Par défaut)** : une action par défaut est définie en interne pour chacune des signatures de menace et signatures antispyware qui sont définies par Palo Alto Networks. L'action par défaut est généralement une alerte ou une réinitialisation des deux. L'action par défaut est indiquée entre parenthèses dans la signature de menace ou antivirus, par exemple, par défaut (alerte).<br>• **Allow (Autoriser)** - Autorisation du trafic de l'application.<br>  *L'action **Allow (Autoriser)** ne génère pas de registres associés aux signatures ou aux profils.*<br>• **Alert (Alerte)** - Génération d'une alerte pour chaque flux de trafic de l'application. L'alerte est sauvegardée dans le journal des menaces.<br>• **Drop (Abandonner)** - Abandon du trafic de l'application.<br>• **Reset Client (Réinitialiser le client)** - Pour le protocole TCP, la connexion côté client est réinitialisée. Pour le protocole UDP, la connexion est abandonnée.<br>• **Reset Server (Réinitialiser le serveur)** - Pour le protocole TCP, la connexion côté serveur est réinitialisée. Pour le protocole UDP, la connexion est abandonnée.<br>• **Reset Both (Réinitialiser les deux)** - Pour le protocole TCP, la connexion est réinitialisée sur le client et le serveur. Pour le protocole UDP, la connexion est abandonnée.<br>Il est possible d'utiliser des profils personnalisés pour limiter les inspections antivirus sur le trafic entre des zones de sécurité de confiance ou au contraire les renforcer sur le trafic provenant de zones non sécurisées comme Internet, ainsi que sur le trafic vers des destinations hautement sensibles comme des batteries de serveurs.<br>Le système WildFire de Palo Alto Networks fournit également des signatures pour les menaces persistantes qui sont plus évasives et qui n'ont pas été encore découvertes par les autres solutions antivirus. Lorsque les menaces sont découvertes par WildFire, les signatures sont rapidement créées, puis intégrées dans les signatures antivirus standard pouvant être téléchargées quotidiennement par les abonnés Prévention des menaces (téléchargement sub-horaire pour les abonnés WildFire). |
| Profils antispyware | Les profils antispyware bloquent les tentatives de communications phone-home ou de signalement sur les serveurs (C2) de commande et de contrôle externes par les logiciels espions sur les hôtes compromis. Ils vous permettent permet de détecter le trafic malveillant provenant de clients infectés et quittant le réseau. Vous pouvez appliquer divers niveaux de protection entre les zones. Par exemple, vous pouvez créer des profils antispyware personnalisés qui réduisent l'inspection entre |

| Type de profil | Description |
| --- | --- |
| | les zones autorisées, tout en optimisant l'inspection du trafic reçu d'une zone non autorisée, telle que les zones ayant accès à Internet. Lorsque le pare-feu est géré par un serveur de gestion Panorama, le ThreatID est mappé avec la menace personnalisée correspondante sur le pare-feu pour permettre au pare-feu de générer un journal des menaces rempli avec le ThreatID personnalisé configuré.<br><br>Vous pouvez définir vos propres profils antispyware personnalisés, ou choisir l'un des profils prédéfinis suivants lors de l'application de l'antispyware à une règle de politique de sécurité :<br><br>• **Par défaut** : utilise l'action par défaut pour chaque signature, comme spécifié par Palo Alto Networks, lors de la création d'une signature.<br>• **Strict** : remplace l'action par défaut des menaces dont le niveau de gravité est critique, élevé et moyen par l'action de blocage, quelle que soit l'action définie dans le fichier de signature. Ce profil utilise toujours l'action par défaut pour les signatures de niveaux de gravité bas et informations.<br><br>Lorsque le pare-feu détecte une menace, vous pouvez configurer les actions suivantes dans le profil antispyware :<br><br>• **Par défaut** : une action par défaut est définie en interne pour chacune des signatures de menace et signatures antispyware qui sont définies par Palo Alto Networks. L'action par défaut est généralement une alerte ou une réinitialisation des deux. L'action par défaut est indiquée entre parenthèses dans la signature de menace ou antivirus, par exemple, par défaut (alerte).<br>• **Allow (Autoriser)** - Autorisation du trafic de l'application.<br><br>  *L'action **Allow (Autoriser)** ne génère pas de registres associés aux signatures ou aux profils.*<br><br>• **Alert (Alerte)** - Génération d'une alerte pour chaque flux de trafic de l'application. L'alerte est sauvegardée dans le journal des menaces.<br>• **Drop (Abandonner)** - Abandon du trafic de l'application.<br>• **Reset Client (Réinitialiser le client)** - Pour le protocole TCP, la connexion côté client est réinitialisée. Pour le protocole UDP, la connexion est abandonnée.<br>• **Reset Server (Réinitialiser le serveur)** - Pour le protocole TCP, la connexion côté serveur est réinitialisée. Pour le protocole UDP, la connexion est abandonnée. |

| Type de profil | Description |
|---|---|
| | • **Reset Both (Réinitialiser les deux)** - Pour le protocole TCP, la connexion est réinitialisée sur le client et le serveur. Pour le protocole UDP, la connexion est abandonnée.<br><br>*Dans certains cas, lorsque l'action du profil est définie sur **reset-both (réinitialiser les deux)**, le journal de menaces associées peut afficher l'action en tant que **reset-server (réinitialiser le serveur)**. Cela se produit lorsque le pare-feu détecte une menace au début d'une session et présente au client la page de blocage 503. Parce que la page de blocage interdit la connexion, le côté client n'a pas à être réinitialisé et seule la connexion côté serveur est réinitialisée.*<br><br>• **Block IP (Bloquer l'adresse IP)** - Cette action bloque le trafic d'une source ou d'une paire source-destination. Elle est configurable pendant une durée déterminée.<br><br>De plus, vous pouvez activer l'action Mise en entonnoir DNS dans les profils antispyware, pour permettre au pare-feu de falsifier une réponse à une requête DNS d'un domaine malveillant connu, entraînant alors la résolution du nom de domaine malveillant en une adresse IP que vous aurez définie. Cette fonction permet d'identifier les hôtes infectés sur le réseau protégé utilisant le trafic DNS. Les hôtes infectés pourront ensuite être facilement identifiés dans les journaux de trafic et de menaces, car tout hôte tentant de se connecter à l'adresse IP entonnoir est probablement infecté par des logiciels malveillants.<br><br>Les profils Antispyware et Protection contre les vulnérabilités sont configurés de la même manière. |
| Profils de protection contre les vulnérabilités | Les profils de protection contre les vulnérabilités bloquent les tentatives d'exploitation des failles du système ou d'accès non autorisé aux systèmes. Les profils antispyware permettent d'identifier les hôtes infectés lorsque le trafic quitte le réseau, tandis que les profils de protection contre les vulnérabilités protègent contre les menaces entrant dans le réseau. Par exemple, les profils de protection contre les vulnérabilités assurent la protection contre le dépassement de capacité de la mémoire tampon, l'exécution non autorisée de code et d'autres tentatives d'exploitation des vulnérabilités du système. Le profil Protection contre les vulnérabilités protège les clients et les serveurs contre l'ensemble des menaces connues de niveaux de gravité critique, élevé et moyen. Vous pouvez également créer des exceptions qui vous permettent de modifier la réponse à une signature spécifique. Lorsque le pare-feu est géré par un serveur de gestion Panorama, le ThreatID est mappé avec la menace personnalisée correspondante sur le pare-feu pour permettre au pare-feu de générer un journal des menaces rempli avec le ThreatID personnalisé configuré. |

| Type de profil | Description |
|---|---|
| | Lorsque le pare-feu détecte une menace, vous pouvez configurer les actions suivantes dans le profil antispyware :<br>• **Par défaut** : une action par défaut est définie en interne pour chacune des signatures de menace et signatures antispyware qui sont définies par Palo Alto Networks. L'action par défaut est généralement une alerte ou une réinitialisation des deux. L'action par défaut est indiquée entre parenthèses dans la signature de menace ou antivirus, par exemple, par défaut (alerte).<br>• **Allow (Autoriser)** - Autorisation du trafic de l'application.<br>  *L'action **Allow (Autoriser)** ne génère pas de registres associés aux signatures ou aux profils.*<br>• **Alert (Alerte)** - Génération d'une alerte pour chaque flux de trafic de l'application. L'alerte est sauvegardée dans le journal des menaces.<br>• **Drop (Abandonner)** - Abandon du trafic de l'application.<br>• **Reset Client (Réinitialiser le client)** - Pour le protocole TCP, la connexion côté client est réinitialisée. Pour le protocole UDP, la connexion est abandonnée.<br>• **Reset Server (Réinitialiser le serveur)** - Pour le protocole TCP, la connexion côté serveur est réinitialisée. Pour le protocole UDP, la connexion est abandonnée.<br>• **Reset Both (Réinitialiser les deux)** - Pour le protocole TCP, la connexion est réinitialisée sur le client et le serveur. Pour le protocole UDP, la connexion est abandonnée.<br>  *Dans certains cas, lorsque l'action du profil est définie sur **reset-both (réinitialiser les deux)**, le journal de menaces associées peut afficher l'action en tant que **reset-server (réinitialiser le serveur)**. Cela se produit lorsque le pare-feu détecte une menace au début d'une session et présente au client la page de blocage 503. Parce que la page de blocage interdit la connexion, le côté client n'a pas à être réinitialisé et seule la connexion côté serveur est réinitialisée.*<br>• **Block IP (Bloquer l'adresse IP)** - Cette action bloque le trafic d'une source ou d'une paire source-destination. Elle est configurable pendant une durée déterminée. |
| Profils de filtrage des URL | Les profils de filtrage des URL vous permettent de surveiller et de contrôler la manière dont les utilisateurs accèdent au Web via les protocoles HTTP et HTTPS. Le pare-feu est livré avec un profil par défaut qui est configuré pour bloquer des sites Web tels que les sites renfermant des logiciels malveillants, les sites de hameçonnage et les sites pour adultes connus. Vous pouvez utiliser le profil par défaut dans une politique de sécurité, le cloner pour l'utiliser comme point de |

| Type de profil | Description |
|---|---|
| | départ pour créer de nouveaux profils de filtrage des URL ou ajouter un nouveau profil d'URL qui autorisera l'ensemble des catégories afin d'obtenir une visibilité du trafic sur votre réseau. Vous pouvez ensuite personnaliser les profils d'URL récemment ajoutés et ajouter des listes de sites Web spécifiques à bloquer ou à autoriser en permanence, ce qui permet un contrôle plus granulaire des catégories d'URL. |
| Profils de filtrage des données | Les profils de filtrage des données permettent d'empêcher que les informations confidentielles, telles que les numéros de carte de crédit ou de sécurité sociale, quittent un réseau protégé. Ils vous permettent également de filtrer des mots-clés, tels qu'un nom de projet confidentiel ou le mot « confidentiel ». Il est important de focaliser votre profil sur les types de fichiers souhaités afin de réduire les faux positifs. Par exemple, vous pouvez rechercher uniquement des documents Word ou des feuilles de calcul Excel. Vous pouvez également analyser le trafic de navigation Web ou FTP.<br><br>Vous pouvez créer des modèles de données personnalisées et les associer aux profils de filtrage des données pour définir le type d'information que vous souhaitez filtrer. Créez des modèles de données basés sur :<br>• **Predefined Patterns (Modèles prédéfinis)** - Filtre pour numéros de carte de crédit et de sécurité sociale (avec ou sans tirets), en utilisant des modèles prédéfinis.<br>• **Regular Expressions (Expressions courantes)** - Filtre pour une chaîne de caractères.<br>• **File Properties (Propriétés des fichiers)** - Filtre basé sur les propriétés des fichiers et les valeurs basés sur le type de fichier.<br><br>*Si vous utilisez une solution de prévention des fuites de données (DLP) gérée par un tiers pour remplir les propriétés afin d'indiquer le contenu sensible, cette option permet au pare-feu de mettre en place votre politique DLP.*<br><br>Pour commencer, Configurez le filtrage des données. |
| Profils de blocage des fichiers | Le pare-feu utilise les profils de blocage des fichiers pour bloquer des types de fichiers donnés sur des applications données et dans le sens du flux de session donné (entrant, sortant ou les deux). Vous pouvez configurer le profil de manière à alerter ou bloquer le chargement et/ou le téléchargement et indiquer les applications soumises au profil de blocage des fichiers. Vous pouvez également configurer des pages de blocage personnalisées qui apparaîtront lorsque l'utilisateur tentera de télécharger le type de fichier donné. Cela permet à l'utilisateur de prendre un moment pour choisir de télécharger un fichier ou pas. |

| Type de profil | Description |
| --- | --- |
| | Vous pouvez définir vos propres profils de blocage des fichiers personnalisés, ou choisir l'un des profils prédéfinis suivants lors de l'application de blocage de fichiers à une règle de politique de sécurité. Les modèles prédéfinis, disponibles à partir de la version de contenu 653 et ultérieure, vous permettent d'activer rapidement des réglages de Pratiques exemplaires pour le blocage des fichiers :<br>• **basic file blocking (blocage de base des fichiers)** : Associez ce profil aux règles de politique de sécurité qui autorisent du trafic en provenance de et en destination des applications moins sensibles afin de bloquer des fichiers qui sont fréquemment inclus dans les campagnes d'attaques par logiciels malveillants ou qui n'ont pas besoin d'être chargés ou téléchargés. Ces profils bloquent le chargement/téléchargement de fichiers PE ( .scr, .cpl, .dll, .ocx, .pif, .exe) , de fichiers de classe Java (.class, .jar), de fichiers d'aide (.chm, .hlp) et d'autres types de fichiers potentiellement malveillants, comprenant les fichiers .vbe, .hta, .wsf, .torrent, .7z, .rar, .bat. De plus, cela invite les utilisateurs à accepter de télécharger des fichiers rar chiffrés ou des fichiers zip chiffrés. Cette règle génère une alerte pour tous les autres types de fichier pour vous apporter une visibilité complète sur tous les fichiers qui entrent et sortent de votre réseau.<br>• **strict file blocking (blocage strict de fichiers)** : utiliser ce profil plus strict pour les règles de politique de sécurité permettant un accès aux applications les plus sensibles. Ce profil bloque le même type de fichiers que l'autre profil, et bloque également les fichiers flash, .tar, .cab, .msi, les fichiers avec codage à niveaux multiples, les fichiers rar chiffrés, ainsi que les fichiers zip chiffrés.<br>Configurez un profil de blocage des fichiers avec les actions suivantes :<br>• **Alerter** : lorsque le type de fichier donné est détecté, un journal est généré dans le journal de filtrage des données.<br>• **Block (Bloquer)** - Lorsque le type de fichier donné est détecté, le fichier est bloqué et une page de blocage est présentée à l'utilisateur. Une entrée est également générée dans le log de filtrage des données.<br>• **Continue (Continuer)** - Lorsque le type de fichier donné est détecté, l'utilisateur voit une page de réponse personnalisable s'afficher. L'utilisateur peut cliquer sur la page pour télécharger le fichier. Une entrée est également générée dans le log de filtrage des données. Comme ce type d'action de transfert nécessite l'intervention de l'utilisateur, il s'applique uniquement au trafic Web.<br>Pour commencer, Configurez le blocage des fichiers. |
| Profils d'analyse WildFire | Servez-vous d'un profil d'analyse WildFire pour que le pare-feu transfère les fichiers ou les liens d'e-mail inconnus pour analyse par WildFire. Précisez les fichiers qui doivent être transférés aux fins d'analyse selon |

| Type de profil | Description |
| --- | --- |
| | l'application, le type de fichier ou le sens de transmission (chargement ou téléchargement). Les fichiers ou les liens d'e-mail qui correspondent à la règle de profil sont transmis au cloud WildFire public ou au cloud WildFire privé (hébergé par un appareil WF-500), selon l'emplacement de l'analyse qui a été défini pour la règle. Si une règle de profil stipule de transmettre les fichiers au cloud WildFire public, le pare-feu transmet également les fichiers correspondant à des signatures antivirus, en plus des fichiers inconnus.<br><br>Vous pouvez également utiliser les profils d'analyse WildFire pour configurer un déploiement de cloud Wildfire hybride. Si vous utilisez un appareil WildFire pour analyser localement les fichiers sensibles (comme des PDF), vous pouvez indiquer que les types de fichiers moins sensibles (comme les fichiers PE) ou les types de fichiers qui ne sont pas pris en charge pour analyse par l'appareil WildFire (comme les APK) soient analysés par le cloud WildFire public. En vous servant de l'appareil WildFire et du cloud WildFire à des fins d'analyse, vous obtenez un verdict rapide relativement aux fichiers qui ont déjà été traités par le cloud et aux fichiers qui ne sont pas pris en charge à des fins d'analyse par l'appareil et vous libérez la capacité de l'appareil, qui peut ainsi servir au traitement du contenu de nature délicate. |
| Profils de protection DoS | Les profils de protection DoS fournissent un contrôle détaillé des politiques de protection de déni de service (DoS). Les politiques DoS vous permettent de contrôler le nombre de sessions entre des interfaces, des zones, des adresses et des pays en se basant sur des sessions ou sur des adresses IP source et/ou de destination agrégées. Les pare-feu Palo Alto Networks prennent en charge deux méthodes de protection DoS.<br><br>• **Flood Protection (Protection contre la saturation)** : détecte et empêche les attaques où le réseau est saturé de paquets suite à un trop grand nombre de sessions à moitié ouvertes et/ou de services incapables de répondre à chaque requête. Dans ce cas, l'adresse source de l'attaque est généralement usurpée. Reportez-vous à la section Protection DoS contre la saturation de nouvelles sessions.<br>• **Resource Protection (Protection des ressources)** : détecte et empêche les attaques par épuisement de sessions. Dans ce type d'attaque, un grand nombre d'hôtes (robots) sont utilisés pour établir autant de sessions que possible pour consommer toutes les ressources d'un système.<br><br>Vous pouvez activer les deux types de mécanismes de protection dans un seul profil de protection DoS.<br><br>Le profil DoS est utilisé pour indiquer le type d'action à entreprendre et les informations relatives aux critères de correspondance pour la politique DoS. Le profil DoS définit les paramètres pour la saturation SYN, UDP et ICMP, peut activer la protection des ressources et détermine le nombre maximum de connexions simultanées. Une fois que |

| Type de profil | Description |
|---|---|
| | vous avez configuré le profil de protection DoS, vous pouvez l'associer à une politique DoS.<br><br>Lors de la configuration de la protection DoS, il est important d'analyser votre environnement afin de définir des seuils corrects et, étant donné la complexité de la définition des politiques de protection DoS, ce guide n'en fournit aucun exemple détaillé. |
| Profils de protection de zone | Les Profils de protection de zone fournissent à des zones réseau spécifiques une protection supplémentaire contre les attaques. Le profil doit être appliqué à toute la zone ; par conséquent, il est important de tester les profils afin d'éviter les problèmes qui peuvent se produire avec le trafic normal traversant les zones. Lors de la définition de limites de seuils en paquets par seconde (pps) pour les profils de protection de zone, le seuil se base sur des paquets par seconde qui ne correspondent pas à une session précédemment établie. |
| Groupe de profils de sécurité | Un groupe de profils de sécurité est un ensemble de profils de sécurité qui peut être traité comme une unité puis facilement ajouté à des politiques de sécurité. Les profils qui sont souvent affectés ensemble peuvent être ajoutés à des groupes de profils pour simplifier la création de politiques de sécurité. Vous pouvez également configurer un groupe de profils de sécurité par défaut. Les nouvelles politiques de sécurité utiliseront alors les paramètres définis dans le groupe de profils par défaut pour vérifier et contrôler le trafic qui correspond à la politique de sécurité. Nommez un groupe de profils de sécurité par défaut pour permettre l'ajout par défaut des profils de ce groupe aux nouvelles politiques de sécurité. Cela vous permet d'inclure automatiquement les paramètres de profil préférés de votre entreprise dans les nouvelles politiques, sans avoir à ajouter manuellement des profils de sécurité à chaque fois que vous créez de nouvelles règles.<br><br>Reportez-vous à la section Créer un groupe de profils de sécurité et à la section Paramétrer ou remplacer un groupe de profils de sécurité par défaut.<br><br>***Pour connaître les recommandations relatives aux meilleures pratiques en matière de profils de sécurité, reportez-vous à la section*** Création de profils de sécurité exemplaires pour la passerelle Internet**.** |

## Créer un groupe de profils de sécurité

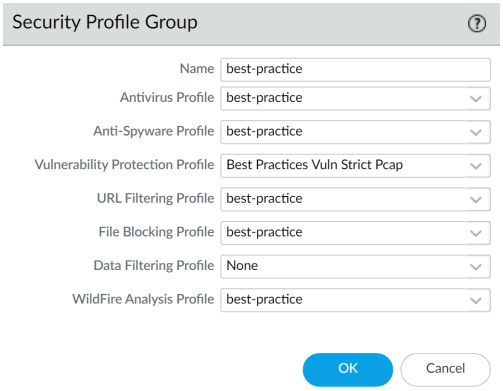
Suivez les étapes ci-dessous pour créer un groupe de profils de sécurité et l'ajouter à une politique de sécurité.

**STEP 1 |** Créez un groupe de profils de sécurité.

*Si vous nommé le groupe `par défaut`, le pare-feu l'associera automatiquement aux nouvelles règles que vous créez. Cette façon de faire vous permettra de gagner du temps si vous disposez d'un ensemble de profils de sécurité privilégiés que vous souhaitez associer à chaque nouvelle règle.*

1. Sélectionnez **Objects (Objets)** > **Security Profile Groups (Groupes de profils de sécurité)** et **Add (Ajoutez)** un nouveau groupe de profils de sécurité.
2. Donnez au groupe un **Name (Nom)** descriptif, par exemple, Menaces.
3. Si le pare-feu est en mode Systèmes virtuels multiples, autorisez le **Shared (Partage)** du profil avec l'ensemble des systèmes virtuels.
4. Ajoutez des profils existants au groupe.




5. Cliquez sur **OK (OK)** pour enregistrer le groupe de profils.

**STEP 2 |** Ajoutez un groupe de profils de sécurité à une politique de sécurité.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et **Add (ajoutez)** ou modifiez une règle de politique de sécurité.
2. Sélectionnez l'onglet **Actions (Actions)**.
3. Dans la section Profile Setting (Paramètres des profils), sélectionnez **Group (Groupe)** comme **Profile Type (Type de profil)**.
4. Dans la liste déroulante **Group Profil (Profil de groupe)**, sélectionnez le groupe créé (par exemple, sélectionnez le groupe Meilleures-pratiques) :


5. Cliquez sur **OK** pour enregistrer la politique et **Commit (Validez)** vos modifications.

**STEP 3 |** Cliquez sur Save (Enregistrer) pour enregistrer vos modifications.

Cliquez sur **Commit (Valider)**.

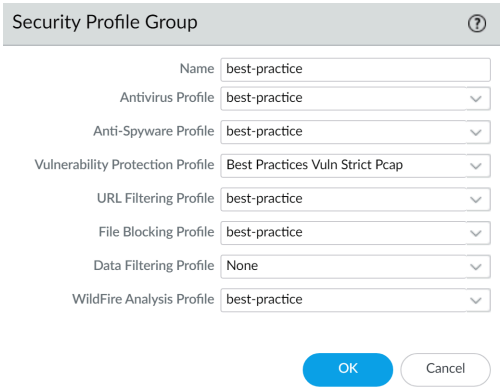
 

# Paramétrage ou remplacement d'un groupe de profils de sécurité par défaut

Les options suivantes vous permettent de configurer l'utilisation par défaut d'un groupe de profils de sécurité dans les nouvelles politiques de sécurité ou de remplacer un groupe par défaut existant. Lorsqu'un administrateur crée une nouvelle politique de sécurité, le groupe de profils par défaut est automatiquement sélectionné comme paramètres de profil de la politique et le trafic correspondant à la politique est vérifié selon les paramètres définis dans le groupe de profils (l'administrateur peut choisir de sélectionner manuellement d'autres paramètres de profil s'il le souhaite). Les options suivantes vous permettent de configurer un groupe de profils de sécurité par défaut ou de remplacer vos paramètres par défaut.

*S'il n'existe aucun profil de sécurité par défaut, les paramètres du profil d'une nouvelle politique de sécurité sont définis par défaut sur **None (Aucun)**.*

- Créez un groupe de profils de sécurité.
  1. Sélectionnez **Objects (Objets)** > **Security Profile Groups (Groupes de profils de sécurité)** et ajoutez un nouveau groupe de profils de sécurité.
  2. Donnez au groupe un **Name (Nom)** descriptif, par exemple, Menaces.
  3. Si le pare-feu est en mode Systèmes virtuels multiples, autorisez le **Shared (Partage)** du profil avec l'ensemble des systèmes virtuels.
  4. Ajoutez des profils existants au groupe. Pour plus d'informations sur la création de profils, reportez-vous à la section Profils de Sécurité.

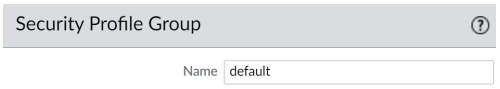



  5. Cliquez sur **OK (OK)** pour enregistrer le groupe de profils.
  6. Ajoutez le groupe de profils de sécurité à une politique de sécurité.
  7. **Add (Ajoutez)** ou modifiez une règle de politique de sécurité et sélectionnez l'onglet **Actions**.
  8. Sélectionnez **Group (Groupe)** comme **Profile Type (Type de profil)**.
  9. Dans la liste déroulante **Group Profile (Profil de groupe)**, sélectionnez le groupe créé (par exemple, sélectionnez le groupe Menaces) :


  10. Cliquez sur **OK** pour enregistrer la politique et **Commit (Validez)** vos modifications.

- Configurez un groupe de profils de sécurité par défaut.
  1. Sélectionnez **Objects (Objets)** > **Security Profile Groups (Groupes de profils de sécurité)** et ajoutez un nouveau groupe de profils de sécurité ou modifiez-en un existant.
  2. **Name (Nommez)** le groupe de profils de sécurité **`default (par défaut)`** :

  3. Cliquez sur **OK**, puis sur **Commit (Valider)**.
  4. Vérifiez que le groupe de profils de sécurité par défaut est inclus par défaut dans les nouvelles politiques de sécurité :
     1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et **Add (Ajoutez)** une nouvelle politique de sécurité.
     2. Sélectionnez l'onglet **Actions** pour afficher les champs **Profile Settings (Paramètres des profils)** :

        Par défaut, la nouvelle politique de sécurité affiche correctement le **Profile Type (Type de profil)** défini sur Groupe et le **Group Profile (Profil de groupe)** par défaut est sélectionné.

- Remplacez un groupe de profils de sécurité par défaut.

  Si vous disposez d'un groupe de profils de sécurité par défaut existant et que vous ne voulez pas que cet ensemble de profils soit associé à une nouvelle politique de sécurité, vous pouvez modifier les champs Paramètres des profils selon vos préférences. Commencez par sélectionner un autre type de profil pour votre politique (**Policies (Politiques)** > **Security (Sécurité)** > **Security Policy Rule (Règle de politique de sécurité)** > **Actions**).

# Suivi des règles au sein d'une base de règles

Pour faire le suivi des règles au sein d'une base de règles, vous pouvez vous référer au ***numéro de règle***, qui modifie en fonction de l'ordre qu'occupe une règle dans la base de règles. Le numéro de règle détermine l'ordre dans lequel le pare-feu applique la règle.

Le ***universally unique identifier (identifiant unique universel ; UUID)*** d'une règle ne change jamais même si vous modifiez la règle, par exemple lorsque vous modifiez le nom de la règle. L'UUID vous permet de suivre la règle sur l'ensemble des bases de règles, même après l'avoir supprimée.

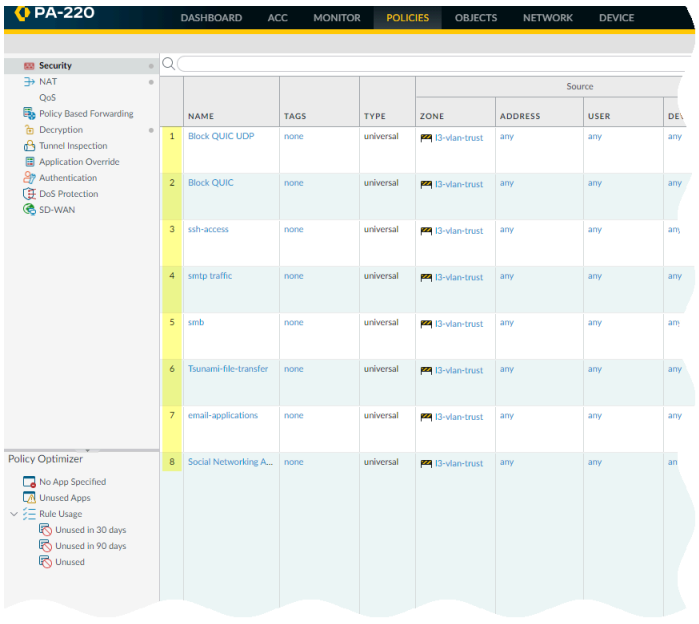
## Numéros de règle

Le pare-feu numérote automatiquement chaque règle d'une base de règles. Lorsque vous déplacez ou réorganisez les règles, les numéros changent en fonction de leur nouvel ordre. Lorsque vous filtrez la liste des règles pour chercher des règles correspondant aux critères spécifiés, le pare-feu affiche chaque règle avec son numéro en tenant compte de l'ensemble des règles comprises dans la base de règles et de sa position dans l'ordre d'évaluation.

Panorama numérote indépendamment les règles avant, après et par défaut. Lorsque Panorama transmet des règles à un pare-feu, le numéro de la règle indique la hiérarchie et l'ordre d'évaluation des règles partagées, des règles avant du groupe de périphériques, des règles du pare-feu, des règles après du groupe de périphériques et des règles par défaut. Vous pouvez sélectionner **Preview Rules (Aperçu des règles)** de Panorama pour afficher une liste ordonnée du nombre total de règles sur un pare-feu.

- Affichez la liste ordonnée des règles sur le pare-feu.

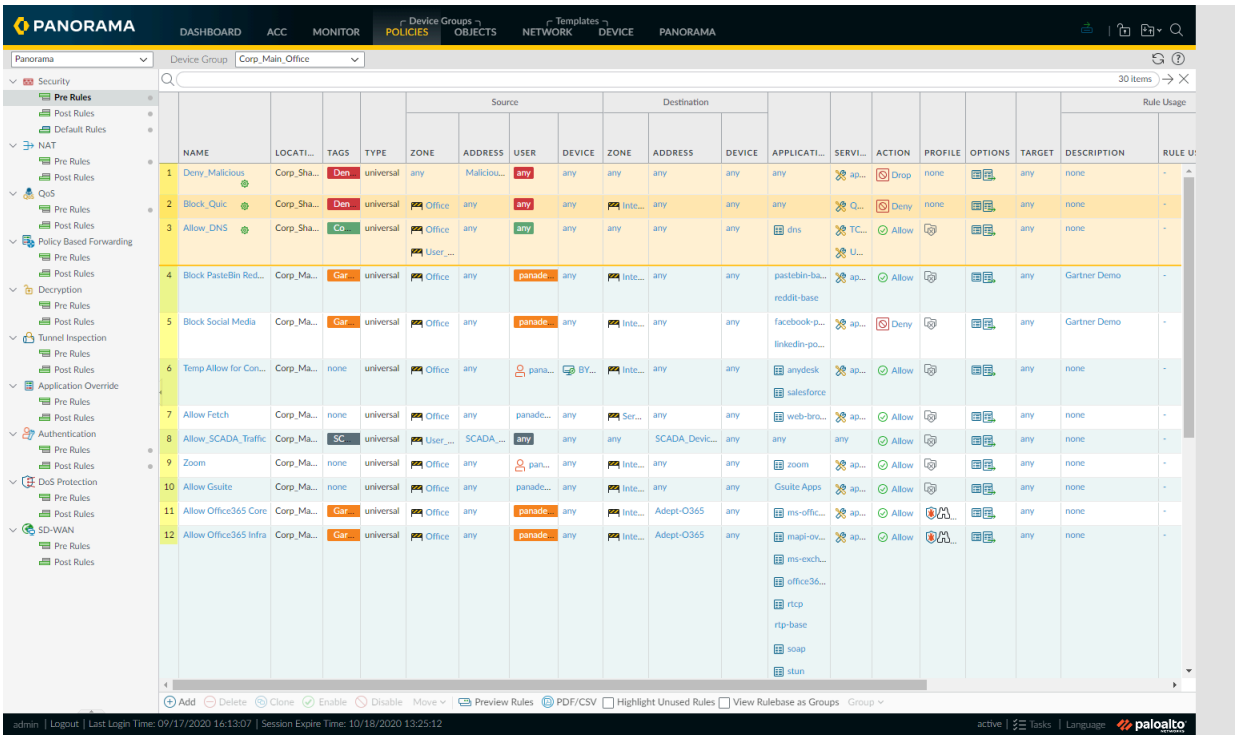
  Sélectionnez **Policies (Politiques)** et toute base de règles en dessous. Par exemple, **Policies (Politiques)** > **Security (Sécurité)**. La colonne la plus à gauche du tableau affiche le numéro de la règle.



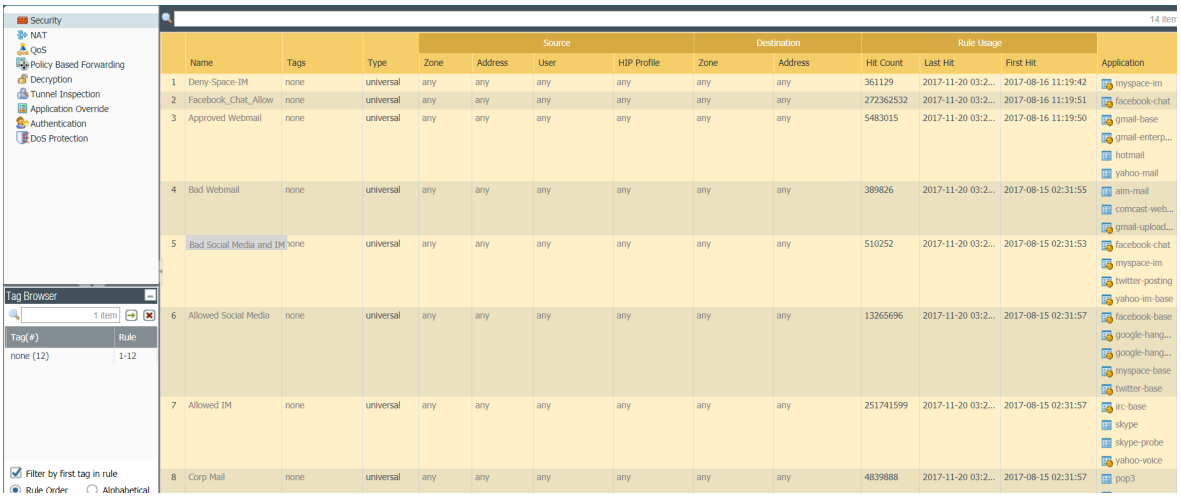
- Affichez la liste ordonnée des règles sur Panorama.

  Sélectionnez **Policies (Politiques)** et toute base de règles en dessous. Par exemple, **Policies (Politiques)** > **Security (Sécurité)** > **Pre-rules (Pré-règles)**.




- Une fois les règles transférées à partir de Panorama, affichez la liste complète des règles et leur numéro sur le pare-feu.

  Dans l'interface Web du pare-feu, sélectionnez **Policies (Politiques)** et choisissez une base de règles en dessous. Par exemple, sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et affichez l'ensemble complet des règles numérotées que le pare-feu évaluera.



# UUID des règles

L'universally unique identifier (identifiant unique universel ; UUID) d'une règle est une chaîne de 32 caractères (basée sur des données comme l'adresse réseau et l'horodatage de création) que le pare-feu ou Panorama attribue à la règle. L'UUID utilise le format 8-4-4-4-12 (où 8, 4 et 12 représentent le nombre de caractères uniques séparés par des tirets). Les UUID identifient les règles de toutes les bases de règles de politique. Vous pouvez également utiliser les UUID pour identifier les règles applicables dans les types de journaux suivants : De Trafic, de Menaces, d'envois WildFire, de Filtrage des données, GTP, SCTP, d'Inspection des tunnels, de configuration et unifiés.

Si vous utilisez l'UUID pour chercher une règle, vous pourrez trouver la règle spécifique que vous souhaitez trouver parmi des milliers de règles qui peuvent porter des noms identiques ou similaires. Les UUID simplifient également l'automatisation et l'intégration des règles dans des systèmes tiers (comme d'attribution de billets ou d'orchestration) qui ne prennent pas en charge les noms.

Dans certains cas, vous pourriez devoir générer de nouveaux UUID pour les bases de règles existantes. Par exemple, si vous souhaitez exporter une configuration vers un autre pare-feu, vous devez ***régénérer les UUID*** des règles lors de l'importation de la configuration pour vous assurer qu'il n'y a pas de UUID en double. Si vous régénérez des UUID, vous n'êtes plus en mesure de suivre ces règles à l'aide de leurs UUID précédents et les données de correspondance et les données sur les utilisations des applications pour ces règles sont réinitialisées.

Le pare-feu ou Panorama affecte des UUID lorsque vous :

- Créez de nouvelles règles
- Clonez des règles existantes
- Exercez un contrôle prioritaire sur les règles de sécurité par défaut
- Chargez une configuration nommée et régénérer des UUID
- Chargez une configuration nommée contenant de nouvelles règles qui ne se trouvent pas dans la configuration active
- Mettez à niveau le pare-feu ou Panorama vers PAN-OS 9.0.

Lorsque vous chargez une configuration qui contient des règles avec des UUID, le pare-feu considère que les règles sont identiques si le nom de la règle, la base de règles et le système virtuel concordent tous. Panorama considère que les règles sont identiques si le nom de la règle, la base de règles et le groupe de périphériques concordent tous.

Tenez compte des points importants suivants pour les UUID :

- Si vous gérez la politique du pare-feu à partir de Panorama, les UUID sont générés sur Panorama et doivent donc être transmis à partir de Panorama. Si vous ne transmettez pas la configuration depuis Panorama avant de mettre les pare-feu à niveau vers PAN-OS 9.0, la mise à niveau du pare-feu échouera, car les UUID seront absents.
- De plus, si vous mettez une paire HA à niveau, lors de la mise à niveau vers PAN-OS 9.0, chaque homologue affecte indépendamment les UUID à chaque règle de politique. Pour cette raison, les homologues seront désynchronisés jusqu'à ce que vous synchronisiez la configuration (**Dashboard (Tableau)** > **Widgets** > **System (Système)** > **High Availability (Haute disponibilité)** > **Sync to peer (Synchronisation avec l'homologue)**).
- Si vous supprimez une configuration High Availability (haute disponibilité ; HA) après la mise à niveau vers PAN-OS 9.0, vous devez régénérez les UUID sur l'un des homologues (**Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)** > **Load named configuration**

**snapshot (Charger l'instantané de la configuration)** > **Regenerate UUIDs for the selected named configuration (Régénérer les UUID de la configuration sélectionnée)**) et validez les modifications pour empêche le dédoublement des UUID.

- Toutes les règles transmises depuis Panorama partageront le même UUID ; toutes les règles qui sont locales à un pare-feu ont des UUID différents. Si vous créez un règle localement sur le pare-feu après avoir transmis les règles de Panorama aux pare-feu, la règle que vous avez créée localement possède son propre UUID.
- Pour remplacer une RMA Panorama, assurez-vous de **Retain Rule UUIDs (Conserver les UUID des règles)** lorsque vous chargez l'instantané de configuration Panorama. Si vous ne sélectionnez pas cette option, Panorama supprime tous les UUID des règles précédents de l'instantané de configure et affecte de nouveaux UUID aux règles sur Panorama, ce qui signifie qu'il ne conserve pas les informations associées aux UUID antérieurs, comme le nombre de correspondance à la règle de politique.

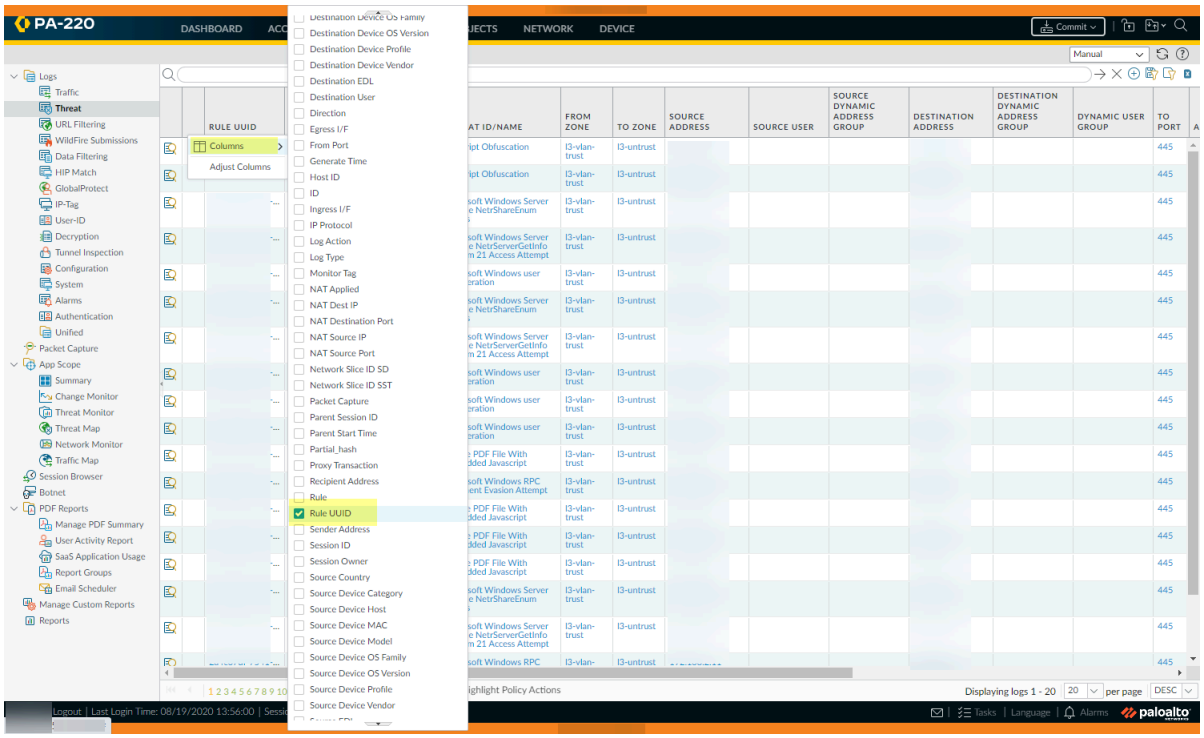
 

- Affichez la colonne relative à l'UUID de la règle pour les journaux et la colonne UUID pour les règles de politique.

  Pour afficher les UUID, vous devez afficher la colonne, qui ne s'affiche pas par défaut.

  - Pour afficher l'UUID dans les journaux :

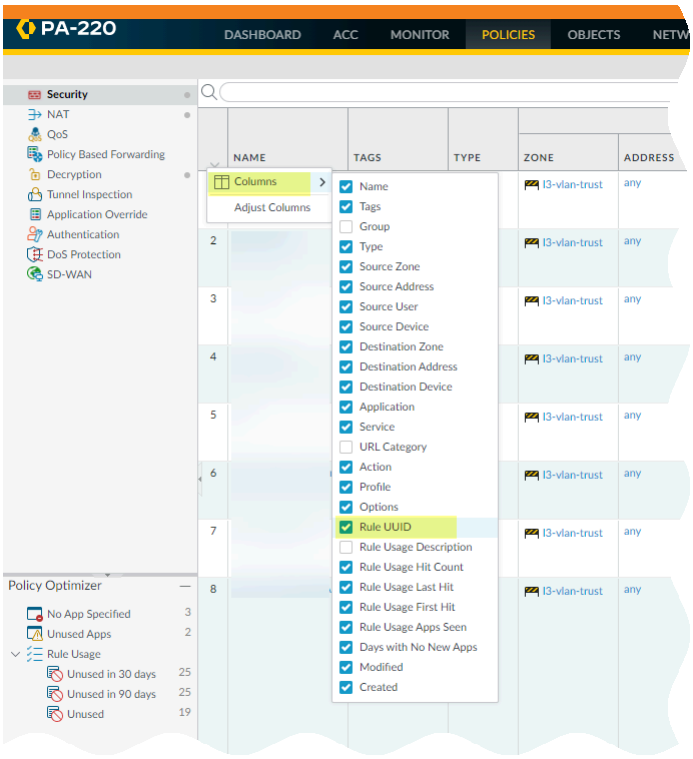
    1. Sélectionnez **Monitor (Surveillance)**, puis développez l'en-tête de colonne ( ).
    2. Sélectionnez **Columns (Colonnes)**.
    3. Activez le **Rule UUID (UUID de la règle)**.




  - Pour afficher les UUID dans la base de règles de politique :

    1. Sélectionnez **Policies (Politiques)**, puis développez l'en-tête de colonne ( ).
    2. Sélectionnez **Columns (Colonnes)**.
    3. Activez le **Rule UUID (UUID de la règle)**.

       Les UUID sont disponibles pour toutes les bases de règles de politique.

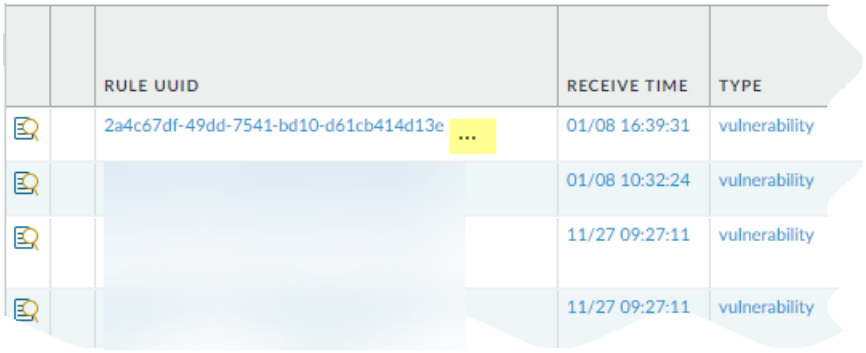


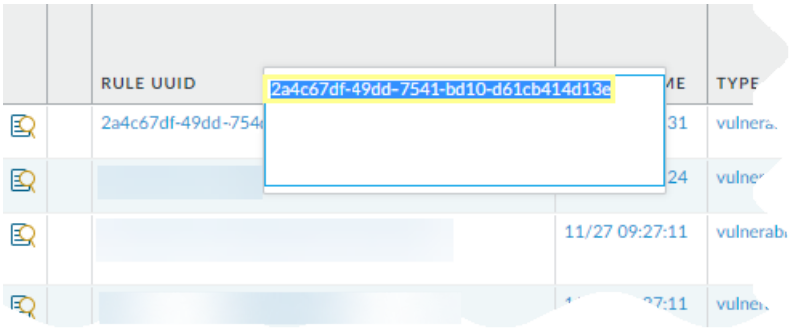
- Copiez l'UUID d'un journal ou d'une règle de politique.

  La copie de l'UUID vous permet de coller l'UUID dans les recherches, dans l'ACC, dans les rapports personnalisé, dans les filtres et partout où vous souhaitez localiser une règle identifiée par cet UUID.

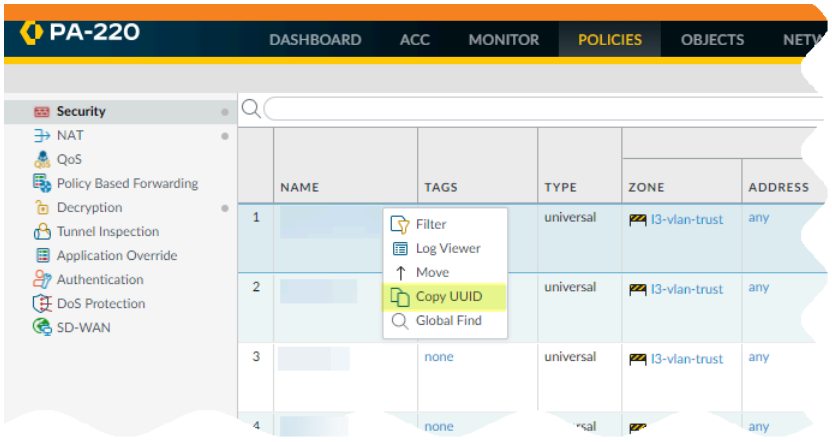
  1. Sélectionnez les ellipses qui s'affichent lorsque vous déplacez votre curseur sur l'entrée de la colonne Rule UUID (UUID de la règle).

  2. Copiez l'UUID à partir de la fenêtre contextuelle.

     Vous pouvez également vous rendez à l'onglet **Policies (Politiques)** cliquer sur la flèche qui apparaît à droit du nom de la règle et **Copy UUID (Copier l'UUID)**.

- Consultez les journaux de configuration pour afficher les UUID des règles supprimées.

  Pour afficher l'UUID d'une règle supprimée, sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Configuration**.

# Application de la description, de l'étiquette ou du commentaire d'audit d'une règle de politique

Lors de la création ou de la modification des règles, vous pouvez exiger qu'une description de la règle, qu'une étiquette ou qu'un commentaire d'audit soient saisis pour veiller à la bonne organisation et au bon regroupement de la base de règles de politique ainsi que pour préserver l'histoire des règles importantes à des fins d'audit. En exigeant la saisie d'une description de la règle, d'une étiquette et d'un commentaire d'audit, vous pouvez simplifier votre examen de la base de règles de politique en vous assurant que les règles sont bien regroupées et que l'historique des modifications apportées aux règles font l'objet d'un suivi lors de la création ou de la modification d'une règle. Par souci d'uniformité, vous pouvez définir des exigences spécifiques afin de préciser les éléments que le commentaire d'audit doit inclure.

Par défaut, l'application d'une description, d'une étiquette et d'un commentaire d'audit n'est pas activé. Vous pouvez spécifier si une description, une étiquette, un commentaire d'audit ou toute combinaison de ces trois éléments sont nécessaires pour ajouter ou modifier avec succès une règle. L'archive des commentaires d'audit vous permet d'afficher les commentaires d'audit saisis pour une règle sélectionnée, d'examiner l'historique des journaux de configuration et de comparer les versions de configuration des règles.

**STEP 1 |** Lancement de l'interface Web.

**STEP 2 |** Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les Policy Rulebase Settings (Paramètres de la base de règles de politique).

**STEP 3 |** Configurez les paramètres que vous souhaitez appliquer. Dans cet exemple, les étiquettes et les commentaires d'audit sont obligatoires pour toutes les politiques.

***Appliquez les commentaires d'audit pour que les règles de politique capturent la raison pour laquelle l'administrateur crée ou modifie une règle. En exigeant la saisie de commentaires d'audit sur les règles de politique vous permet de conserver une historique précis des règles à des fins d'audit.***

**STEP 4 |** Configurez l'expression régulière des commentaires d'audit pour spécifier le format des commentaires d'audit.

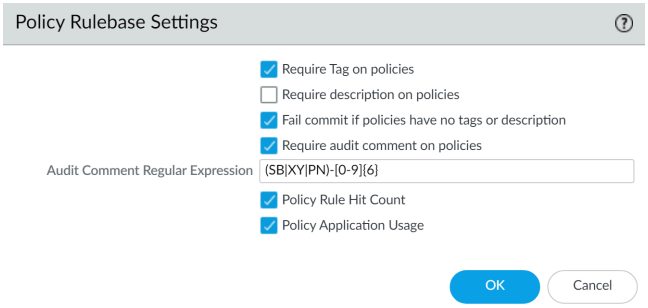
Lorsque les administrateurs créent ou modifient une règle, vous pouvez exiger qu'ils saisissent des commentaires d'audit qui respectent un format donné qui correspond à vos besoins d'affaires et d'audit en spécifiant des expressions chiffres et en lettres. Par exemple, vous pouvez utiliser ce paramètre pour spécifier des expressions régulières qui correspondent à vos formats d'attribution du numéros de billets :

- **`[0-9]{<Nombre de chiffres>}`** : exige que le commentaire d'audit contienne un nombre minimum de chiffres allant de 0 à 9. Par exemple, **`[0-9]{6}`** exige la présence de six chiffres dans une expression numérique composée de chiffres entre 0 et 9.
- <**`Expression en lettres`**> : exige que le commentaire d'audit contienne une expression en lettres. Par exemple, **`Reason for Change-`** exige que l'administrateur commence son commentaire d'audit avec cette expression.

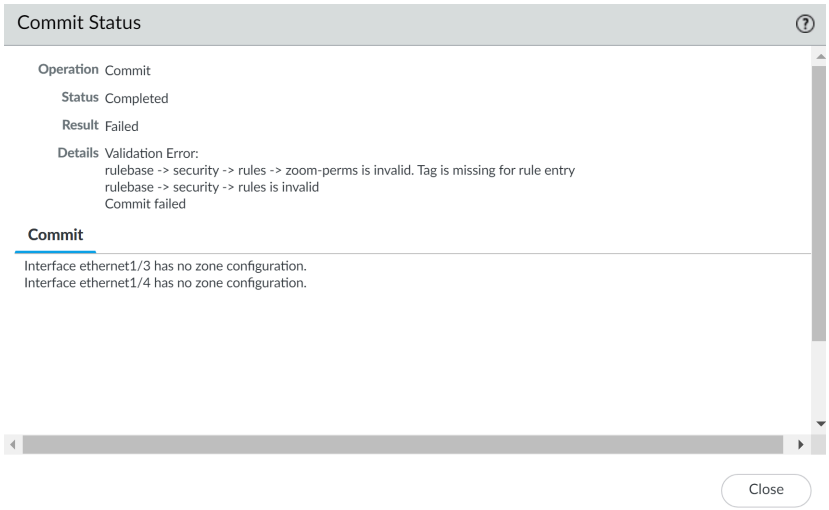
- <**Expression en lettres**>-**[0-9]{<Nombre de chiffres>}** : exige que le commentaire d'audit contienne un caractère prédéfini suivi d'un nombre minimum de chiffres allant de 0 à 9. Par exemple, **SB-[0-9]{6}** exige que le commentaire d'audit commence par **SB-**, suivi d'au moins six chiffres présentés sous une expression numérique comportant des valeurs de 0 à 9. Par exemple, **SB-012345**.
- **(**<**Expression en lettres**>**)|(**<**Expression en lettres**>**)|(**<**Expression en lettres**>**)|-[0-9]{<Nombre de chiffres>}** : exige que le commentaire d'audit contienne un préfixe se servant de l'une des expressions en lettres prédéfinie et un nombre minimum de chiffres allant de 0 à 9. Par exemple, **(SB|XY|PN)-[0-9]{6}** exige que le format du commentaire d'audit commence par **SB-**, **XY-** ou **PN-** , suivi d'au moins six chiffres dans une expression numérique dont les valeurs se situent entre 0 et 9. Par exemple, **SB-012345**, **XY-654321** ou **PN-012543**.

**STEP 5 |** Cliquez sur **OK** pour appliquer les nouveaux paramètres de la base de règles de politique.




**STEP 6 |** **Commit (Validez)** les modifications.

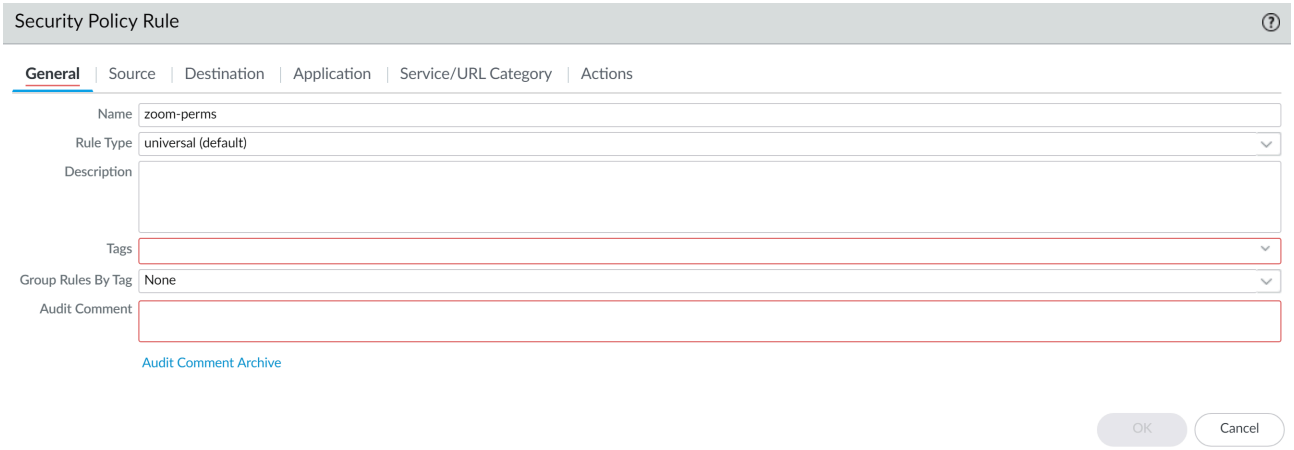
*Après avoir validé les modifications des paramètres de la base de règles de politique, modifiez la règle de politique existante en fonction des paramètres de la base de règles que vous avez décidé d'appliquer.*



**STEP 7 |** Vérifiez que le pare-feu applique les nouveaux paramètres de la base de règles de politique.

1. Sélectionnez **Policies (Politiques)**, et **Add (Ajoutez)** une nouvelle règle.
2. Confirmez que vous devez ajouter une étiquette et saisissez un commentaire d'audit, puis cliquez sur **OK**.



# Migration ou clonage d'un objet ou d'une règle de politique sur un autre système virtuel

Sur un pare-feu qui comporte plus d'un système virtuel (vsys), vous pouvez migrer ou cloner des règles de politique ou des objets vers un autre système virtuel ou vers l'emplacement partagé. Grâce à la migration ou au clonage, vous n'avez plus à supprimer, recréer ou renommer des règles et des objets. Si la règle de politique ou l'objet que vous migrerez ou clonerez à partir d'un système virtuel faire référence à des objets contenus dans ce système virtuel, migrez ou clonez ces objets également. Si les références touchent des objets partagés, vous n'avez pas à les inclure lors de la migration ou du clonage. A titre de référence, vous pouvez utiliser Recherche globale pour effectuer des recherches dans le pare-feu ou dans le serveur de gestion Panorama.

*Lorsque vous clonez plusieurs règles de politiques, l'ordre dans lequel vous sélectionnez les règles détermine l'ordre dans lequel elles sont copiées dans le groupe de périphériques. Par exemple, si vous avez les règles 1 à 4 et que votre ordre de sélection est 2-1-4-3, le groupe de périphériques dans lequel ces règles seront clonées affichera les règles dans le même ordre que celui que vous avez sélectionné. Cependant, vous pouvez réorganiser les règles comme bon vous semble une fois qu'elles ont été copiées avec succès.*

**STEP 1 |** Sélectionnez le type de politique (par exemple, **Policy (Politique)** > **Security (Sécurité)** ou le type d'objet (par exemple, **Objects (Objets)** > **Addresses (Adresses)**).

**STEP 2 |** Sélectionnez le **Système virtuel** et sélectionnez une ou plusieurs règles de politiques ou objets.

**STEP 3 |** Effectuez l'une des étapes suivantes :

- Sélectionnez **Move (Déplacer)** > **Move to other vsys(Déplacer vers d'autres vsys)** (pour les règles de politique).
- Cliquez sur **Move (Déplacer)** (pour les objets).
- Cliquez sur **Clone (Cloner)** (pour les règles de politique ou les objets).

**STEP 4 |** Dans le menu déroulant **Destination**, sélectionnez le nouveau système virtuel ou **Shared (Partagé)**.

**STEP 5 |** (Règles de politique uniquement) Sélectionnez l'**Rule order (Ordre des règles)** :

- **Move top (Déplacer vers le haut)** (par défaut) — la règle se mettra en avant de toutes les autres règles.
- **Move bottom (Déplacer vers le bas)** la règle viendra après toutes les autres règles.
- **Before rule (Avant la règle)** - Dans la liste déroulante adjacente, sélectionnez la règle qui vient après les règles sélectionnées.
- **After rule (Après la règle)** —Dans le déroulant adjacent, sélectionnez la règle qui précède les règles sélectionnées.

**STEP 6 |** La case **Erreur sortante dès la première erreur détectée lors de la validation** est cochée par défaut. Le pare-feu cesse de vérifier les actions Déplacer ou Cloner dès qu'il trouve la première erreur et n'affiche que cette erreur. Par exemple, si une erreur se produit lorsque le système virtuel **Destination** ne possède aucun objet auquel la règle de politique que vous déplacez fait

référence, le pare-feu affichera l'erreur et cessera les validations. Lorsque vous déplacez ou clonez plusieurs éléments à la fois, en cochant cette case vous pourrez trouver une erreur à la fois et la régler. Si vous décochez la case, le pare-feu collecte et affiche une liste des erreurs. S'il y a des erreurs de validation, l'objet n'est pas migré ni cloné tant que toutes les erreurs n'ont pas été corrigées.

**STEP 7 |** Cliquez sur **OK** pour démarrer la validation de l'erreur. Si le pare-feu affiche des erreurs, corrigez-les et essayez de nouveau l'opération Déplacer ou Cloner. Si le pare-feu ne trouve aucune erreur, l'objet est déplacé ou cloné avec succès. Une fois l'opération terminée, cliquez sur **Valider**.

# Utilisation d'un objet d'adresse pour représenter des adresses IP

Créez un objet d'adresse sur le pare-feu pour regroupe les adresses IP ou pour préciser un FQDG, puis référencez l'objet d'adresse dans une règle de politique du pare-feu, dans un filtre ou dans une autre fonction pour éviter d'avoir à spécifier individuellement plusieurs adresses IP dans la règle, le filtre ou l'autre fonction.

De plus, vous pouvez référencer le même objet d'adresse dans plusieurs règles de politique, filtres ou autres fonctions sans avoir à préciser les mêmes adresses individuelles à chaque utilisation. Par exemple, vous pouvez créer un objet d'adresse qui spécifie une plage d'adresses IPv4, puis référencez l'objet d'adresse dans une règle de politique de sécurité, dans une règle de politique NAT et dans un filtre du journal du rapport personnalisé.

- Objets d'adresse
- Création d'un objet d'adresse

## Objets d'adresse

Un objet d'adresse est un ensemble d'adresses IP que vous pouvez gérer en un seul endroit, puis utiliser dans de multiples règles de politique, de filtres et d'autres fonctions du pare-feu. Il existe quatre types d'objet d'adresse : **IP Netmask (Masque réseau IP)**, **IP Range (Plage d'adresses IP)**, **IP Wildcard Mask (Masque générique IP)** et **FQDN**.

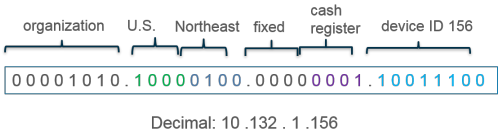
Un objet d'adresse de type **IP Netmask (Masque réseau IP)**, **IP Range (Plage d'adresses IP)** ou **FQDN** peut spécifier des adresses IPv4 ou IPv6. Un objet d'adresse de type **IP Wildcard Mask (Masque générique IP)** peut spécifier des adresses IPv4 uniquement.

Avec un objet d'adresse de type **IP Netmask (Masque réseau IP)**, vous devez saisir l'adresse IP ou le réseau à l'aide de la notation contenant des barres obliques pour indiquer le réseau IPv4 ou la longueur de préfixe IPv6. Par exemple, 192.168.18.0/24 ou 2001:db8:123:1::/64.

Avec un objets d'adresse de type **IP Range (Plage d'adresses IP)**, vous devez saisir la plage des adresses IPv4 ou IPv6, séparées par un tiret.

Un objet d'adresse de type **FQDN** (par exemple, paloaltonetworks.com) facilite l'utilisation, car DNS fournit la résolution du FQDN en adresses IP. Vous n'avez donc pas à connaître les adresses IP et à les charger manuellement chaque fois que le FQDN se résout en de nouvelles adresses IP.

Un objet d'adresse de type **IP Wildcard Mask (Masque générique IP)** s'avère utile si vous définissez les adresses IPv4 privées pour les périphériques internes et votre structure d'adressage attribue un sens à certains bits de l'adresse. Par exemple, l'adresse IP de la caisse 156 dans le nord-est des États-Unis pourrait être 10.132.1.156 en fonction des affectations de bits suivants :




Un objet d'adresse de type **IP Wildcard Mask (Masque générique IP)** spécifie les adresses source ou de destination qui sont soumises à une règle de politique de sécurité. Par exemple,

10.132.1.1/0.0.2.255. Dans le masque, un bit de zéro (**0**) indique que le bit faisant l'objet de la comparaison doit correspondre au bit qui est indiqué dans l'adresse IP qui est couverte par le zéro. Dans le masque, un bit de un (**1**) (un bit générique) indique que le bit faisant l'objet de la comparaison doit correspondre au bit qui est indiqué dans l'adresse IP. Les extraits d'adresse IP et de masque générique suivants illustrent la façon dont ils donnent lieu à quatre correspondances :


Après avoir Création d'un objet d'adresse :

- Vous pouvez faire référence à un objet d'adresse de type **IP Netmask (Masque réseau IP)**, **IP Range (Plage d'adresses IP)** ou **FQDN** dans une règle de politique de sécurité, d'authentification, de NAT, de NAT64, de déchiffrement, de protection DoS Protection, de transfert basé sur une politique, QoS, de contrôle prioritaire sur l'application ou d'inspection des tunnels; ou dans un pool d'adresses NAT, un tunnel VPN, une surveillance des chemins, une liste dynamique externe, la protection contre la reconnaissance, un filtre global ACC, un filtre de journal ou un filtre de journaux sur les rapports personnalisés.
- Vous pouvez faire référence à un objet d'adresse de type **IP Wildcard Mask (Masque générique IP)** uniquement dans une règle de politique de sécurité.

## Création d'un objet d'adresse

Créez un address object (objet d'adresse) pour représenter une ou plusieurs adresses IP, puis référencez l'objet d'adresse dans un ou plusieurs filtres, règles de politique ou autres fonctions du pare-feu. Si vous voulez modifier l'ensemble d'adresses, vous pouvez modifier l'objet d'adresse une seule fois plutôt que de modifier plusieurs règles de politique ou filtres, réduisant ainsi les frais généraux.

**STEP 1 |** Créez un objet d'adresse.

1. Sélectionnez **Objects (Objets)** > **Addresses (Adresses)** et **Add (Ajoutez)** un objet d'adresse par **Name (Nom)**. Le nom est sensible à la casse, doit être unique et ne peut contenir que 63 caractères (des lettres, des chiffres, des espaces, des traits d'union et des caractères de soulignement).
2. Sélectionnez le **Type (Type)** d'objet d'adresse :
   - **IP Netmask (Masque réseau IP)** : spécifiez une adresse IPv4 ou IPv6 simple, un réseau IPv4 avec la notation contenant des barres obliques ou une adresse IPv6 et un préfixe. Par exemple, 192.168.80.0/24 ou 2001:db8:123:1::/64. Vous pouvez également cliquer sur **Resolve (Résoudre)** pour voir le FQDN associé (selon la configuration DNS du pare-feu ou de Panorama). Pour faire passer le type d'objet d'adresse de **IP Netmask (Masque réseau IP)** à **FQDN**, sélectionnez le FQDN et cliquez sur **Use this FQDN (Utiliser ce FQDN)**. Le **Type** passe à **FQDN** et le FQDN que vous sélectionnez apparaît dans le champ texte.
   - **IP Range (Plage d'adresses IP)** : spécifiez la plage des adresses IPv4 ou IPv6, séparées par un tiret. Par exemple, 192.168.40.1-192.168.40.255 ou 2001:db8:123:1::1-2001:db8:123:1::22.

- **Masque générique IP** spécifiez une adresse IP générique (adresse IPv4 suivie d'une barre oblique et d'un masque, qui doit commencer par zéro). Par exemple : 10.5.1.1/0.127.248.2. Dans le masque, un bit de zéro (**0**) indique que le bit faisant l'objet de la comparaison doit correspondre au bit qui est indiqué dans l'adresse IP qui est couverte par le zéro. Dans le masque, un bit de **1** (bit générique) indique que le bit faisant l'objet de la comparaison doit correspondre au bit qui est indiqué dans l'adresse IP qui est couverte par le un.
- **FQDN** : indiquez le nom de domaine. Le FQDN est résolu au moment de la validation. Le pare-feu actualise par la suite le FQDN en fonction de la Time To Live (durée de vie ; TTL) du FQDN dans DNS tant que la TTL est supérieure ou égale au **Minimum FQDN Refresh Time (Fréquence d'actualisation minimale du FQDN)** que vous avez configuré (ou à la valeur par défaut, soit 30 secondes). Le FQDN est résolu par le serveur DNS du système ou un objet proxy DNS, si un proxy est configuré. Vous pouvez également cliquer sur **Resolve (Résoudre)** pour voir l'adresse IP associée (selon la configuration DNS du pare-feu ou de Panorama). Pour faire passer le type d'objet d'adresse de FQDN à masque réseau IP, sélectionnez un masque réseau IP et cliquez sur **Use this address (Utiliser cette adresse)**. Le **Type** passe à **IP Netmask (Masque réseau IP)** et l'adresse IP que vous sélectionnez apparaît dans le champ texte.

3. (Facultatif) Saisissez une ou plusieurs étiquettes à appliquer à l'objet d'adresse.
4. Cliquez sur **OK**.

**STEP 2 |** **Commit (Validez)** vos modifications.

**STEP 3 |** Affichez les journaux filtrés par objet adresse, groupe d'adresses ou adresse générique.

1. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)**, par exemple, pour afficher les journaux de trafic.
2. Sélectionnez **+** pour ajouter un filtre de journal.
3. Sélectionnez l' attribut de **Address (Adresse)**, l'opérateur **in (dans)** et saisissez le nom de l'objet d'adresse duquel vous souhaitez afficher les journaux. Vous pouvez également saisir un nom de groupe ou une adresse générique, comme 10.155.3.4/0.0.240.255.
4. Cliquez sur **Apply (Appliquer)**.

**STEP 4 |** Afficher un rapport personnalisés en fonction d'un objet d'adresse.

1. Sélectionnez **Monitor (Surveillance)** > **Manage Custom Reports (Gérer des rapports personnalisés)** et sélectionnez un rapport qui utilise une base de données, comme Traffic Log (Journal du trafic).
2. Sélectionnez **Filter Builder (Générateur de filtre)**.
3. Sélectionnez un attribut, comme **Address (Adresse)**, **Destination Address (Adresse de destination)** ou **Source Address (Adresse source)**, sélectionnez un opérateur, puis saisissez le nom de l'objet d'adresse duquel vous souhaitez afficher le rapport.

**STEP 5 |** Utilisez un filtre dans l'ACC pour afficher l'activité du réseau en fonction d'une adresse IP source ou d'une adresse IP de destination qui utilise un objet d'adresse.

1. Sélectionnez **ACC** > **Network Activity (Activité du réseau)**.
2. Afficher **l'activité des IP source** : pour les filtres généraux, cliquez sur **+** pour ajouter un filtre et sélectionnez l'une des options suivantes : **Address (Adresse)** ou **Source** > **Source**

**Address (Adresse source)** or **Destination** > **Destination Address (Adresse de destination)** et sélectionnez un objet d'adresse.

3. Afficher **l'activité des IP de destination : pour les filtres généraux**, cliquez **+** pour ajouter un filtre et sélectionnez l'une des options suivantes : **Address (Adresse)** ou **Source** > **Source Address (Adresse source)** or **Destination** > **Destination Address (Adresse de destination)** et sélectionnez un objet d'adresse.

# Utilisation d'étiquettes pour regrouper et distinguer visuellement les objets

Vous pouvez appliquer une étiquette à des objets pour regrouper des éléments associés et ajouter des couleurs à l'étiquette afin de les distinguer visuellement pour en faciliter l'analyse. Vous pouvez créer des étiquettes pour les objets suivants : objets d'adresse, groupes d'adresses, groupes d'utilisateurs, zones, groupes de services et règles de politique.

Le pare-feu et Panorama prennent en charge les étiquettes statiques et les étiquettes dynamiques. Les étiquettes dynamiques sont enregistrées à partir de différentes sources et ne sont pas affichées avec les étiquettes statiques, car elles ne font pas partie de la configuration du pare-feu ou de Panorama. Pour plus d'informations sur l'enregistrement dynamique des étiquettes, reportez-vous à la section Enregistrement dynamique des adresses IP et des étiquettes. Les étiquettes décrites dans cette section sont ajoutées de manière statique et font partie de la configuration.

Une ou plusieurs étiquettes peuvent être appliquées à des objets et des règles de politique ; 64 étiquettes maximum peuvent être appliquées à un objet. Panorama prend en charge 10 000 étiquettes maximum, que vous pouvez répartir entre Panorama (groupes partagés et de périphérique) et les pare-feu gérés (y compris les pare-feu disposant de systèmes virtuels multiples).

- Création et application d'étiquettes
- Modification d'étiquettes
- Afficher les règles par groupe d'étiquettes

## Création et application d'étiquettes

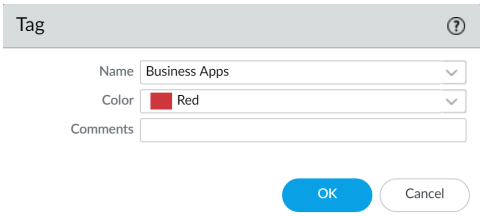
Utilisez les étiquettes pour identifier l'objectif d'une règle ou d'un objet de configuration et améliorer votre organisation de votre base de règles. Pour veiller au bon balisage des règles de politique, voyez comment Application de la description, de l'étiquette ou du commentaire d'audit d'une règle de politique. De plus, vous pouvez Afficher les règles par groupe d'étiquettes en créant d'abord l'étiquette et en la définissant en tant qu'étiquette de groupe.

**STEP 1 |** Créez des règles.

*Pour identifier une zone, vous devez créer une étiquette portant le même nom que la zone. Lorsque la zone est associée à des règles de politiques, la couleur de l'étiquette s'affiche automatiquement comme couleur d'arrière-plan du nom de la zone.*

1. Sélectionnez **Objects (Objets)** > **Tags (Étiquettes)**.
2. Sur Panorama ou un pare-feu disposant de systèmes virtuels multiples, sélectionnez le **Device Group (Groupe de périphériques)** ou le **Virtual System (Système virtuel)** auquel rendre l'étiquette disponible.
3. **Add (Ajoutez)** une étiquette et entrez un **Name (Nom)** pour identifier l'étiquette ou sélectionnez le **Name (Nom)** d'une zone si vous voulez créer une étiquette applicable à une zone. La longueur est de 127 caractères maximum.
4. (Facultatif) Sélectionnez **Shared (Partagé)** pour créer l'objet dans un emplacement partagé de manière à ce qu'il puisse être accessible en tant qu'objet partagé dans Panorama ou utilisé par tous les systèmes virtuels d'un pare-feu disposant de systèmes virtuels multiples.
5. (Facultatif) Affectez une **Color (Couleur)** dans les 17 couleurs prédéfinies. Par défaut, **Color (Couleur)** est définie sur **None (Aucune)**.




6. Cliquez sur **OK (OK)** puis sur **Commit (Valider)** pour enregistrer vos modifications.

**STEP 2 |** Appliquer les étiquettes à la politique.

1. Sélectionnez **Policies (Politiques)** et toute base de règles en dessous.
2. **Add (Ajoutez)** une règle de politique et utilisez les objets identifiés que vous avez créés à l'étape 1.
3. Vérifiez que les étiquettes sont utilisées.

| | | | | Source | | | | Destination | |
|---|---|---|---|---|---|---|---|---|---|
| | NAME | TAGS | TYPE | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS |
| 1 | General Business Apps | Business Apps | universal | any | any | known-user | any | any | any |

**STEP 3 |** Appliquez des étiquettes à un objet d'adresse, un groupe d'adresses, un service ou un groupe de services.

1. Créez l'objet.

   Par exemple, pour créer un groupe de services, sélectionnez **Objects (Objets)** > **Service Groups (Groupes de services)** > **Add (Ajouter)**.
2. Sélectionnez une étiquette (**Tags (Étiquettes)** ou saisissez un nom dans le champ pour créer une nouvelle étiquette.

   Pour modifier une étiquette ou ajouter une couleur à l'étiquette, reportez-vous à la section Modification d'étiquettes.

# Modification d'étiquettes

- Sélectionnez **Objects (Objets)** > **Tags (Étiquettes)** pour effectuer l'une des opérations suivantes avec les étiquettes :
  - Cliquez sur le **Name (Nom)** pour modifier les propriétés d'une étiquette.
  - Sélectionnez une étiquette dans le tableau, puis **Delete (Supprimez)** l'étiquette du pare-feu.
  - **Clone (Clonez)** une étiquette pour la dupliquer avec les mêmes propriétés. Un suffixe numérique est ajouté au nom de l'étiquette (par exemple, FTP-1).

  Pour plus d'informations sur la création d'étiquettes, reportez-vous à la section Création et application d'étiquettes. Pour plus d'informations sur l'utilisation d'étiquettes, reportez-vous à la section Afficher les règles par groupe d'étiquettes.

# Afficher les règles par groupe d'étiquettes

Affichez votre base de règles de politique en tant que groupes d'étiquettes selon la structure d'étiquetage que vous avez créée. Dans cet affichage, vous pouvez effectuer les procédures opérationnelles, comme l'ajout, la suppression ou le déplacement des règles du groupe d'étiquettes sélectionné plus facilement. L'affichage de la base de règles en tant que groupes d'étiquettes conserve l'ordre d'évaluation des règles, et une étiquette peut apparaître plusieurs fois dans la base de règles afin de préserver la hiérarchie des règles.

Vous devez créer l'étiquette avant de pouvoir l'assigner comme étiquette de groupes à une règle. La première étiquette des règles qui sont déjà étiquetées lors de la mise à niveau vers PAN-OS 9.0 devient automatiquement l'étiquette de groupe. Avant de passer à PAN-OS 9.0, passez en revue les règles étiquetées de votre base de règles pour vous assurer que les règles sont bien groupées lors de la mise à jour. Vous devez modifier manuellement chaque règle d'étiquette et configurer la bonne étiquette de groupe si vos règles sont mal regroupés après votre mise à niveau vers PAN-OS 9.0.

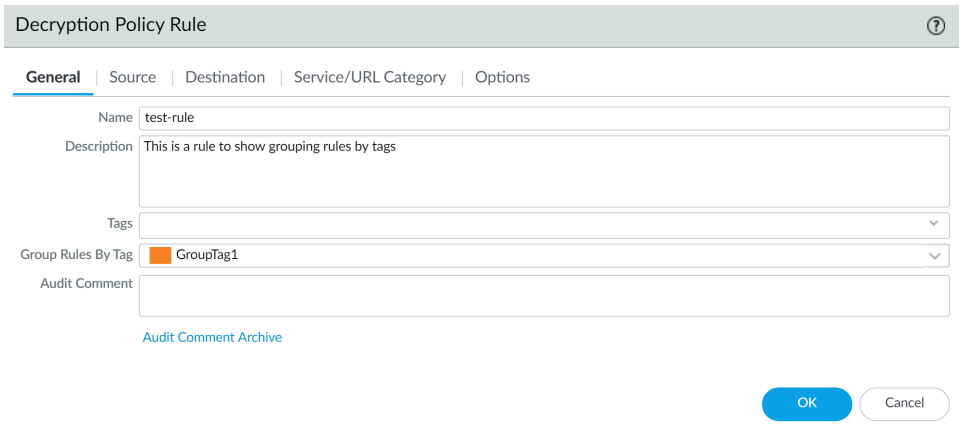

**STEP 1 |** Lancement de l'interface Web.

**STEP 2 |** Création et application d'étiquettes que vous voulez utiliser pour les règles de regroupement.

**STEP 3 |** Affectez une règle de politique à un groupe d'étiquettes.

1. Créez une règle de politique. Reportez-vous à la section Politique pour obtenir de plus amples informations sur la création de règles de politique.
2. Dans le champ **Group Rules by Tag (Regrouper des règles par étiquette)**, sélectionnez l'étiquette dans le menu déroulant, puis cliquez sur **OK**.

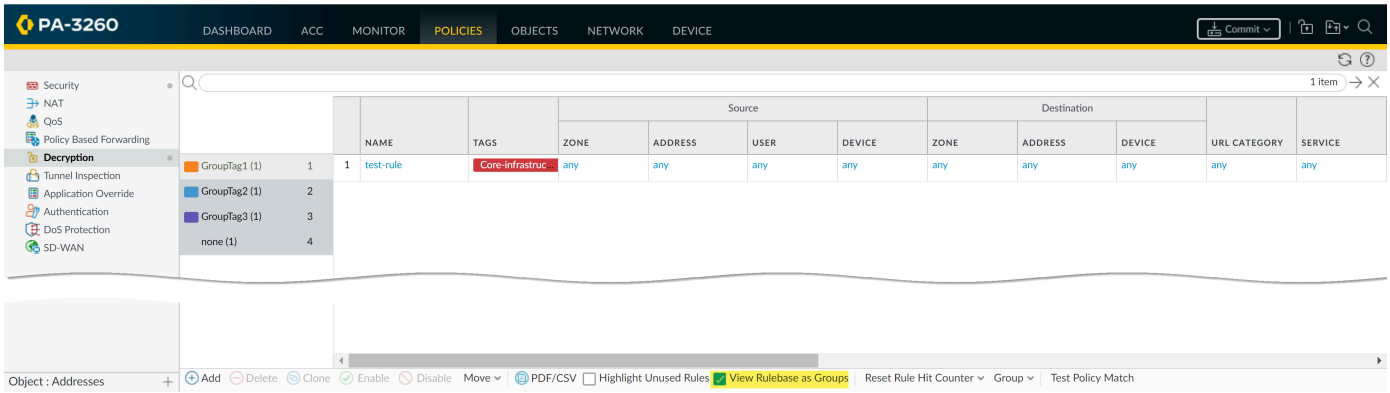



3. **Commit (Validez)** vos modifications.

**STEP 4 |** Affichez votre base de règles de politique en tant que groupes.

1. (Panorama uniquement) Dans le menu déroulant **Device Group (Groupe de périphériques)**, sélectionnez la base de règles de groupe de périphériques à afficher ou affichez toutes les règles partagées.
2. Cliquez sur **Policies (Politiques)** et sélectionnez la base de règles dans laquelle vous avez créé les règles à l'étape 2.
3. Cochez la case **View Rulebase as Groups (Afficher la base de règles en tant que groupes)** au bas.

*Les règles qui ne sont pas affectées à un groupe d'étiquettes s'affichent en tant que **None (Aucune)**.*

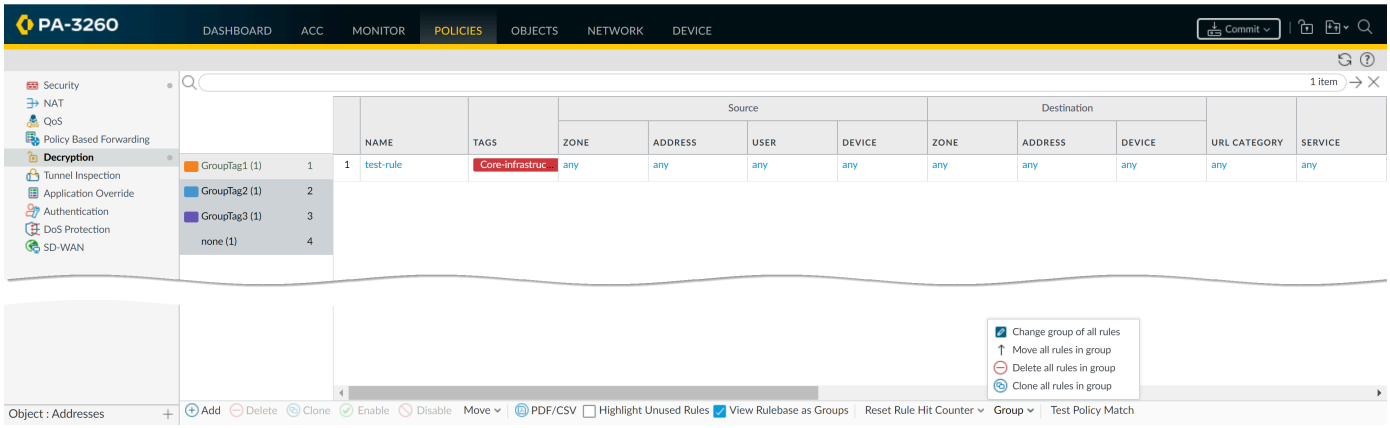


**STEP 5 |** Effectuez les opérations de groupe au besoin.

1. Cliquez sur **Group (Groupe)** pour effectuer les opérations de groupe pour les règles du groupe d'étiquettes sélectionné.

   - (Panorama uniquement) **Move rules in group to a different rulebase or device group (Déplacer les règles du groupe vers une autre base de règles ou un autre groupe de périphériques)** : déplacez toutes les règles de politique du groupe d'étiquettes sélectionné vers la base des règles avant ou la base des règles après, ou à un autre groupe de périphériques.
   - **Change group of all rules (Modifier le groupe de toutes les règles)** : déplacez toutes les règles du groupe d'étiquettes sélectionné vers un autre groupe d'étiquettes.
   - **Move all rules in group (Déplacer toutes les règles du groupe)** : déplacez toutes les règles du groupe d'étiquettes sélectionné afin de changer l'ordre de priorité des règles.
   - **Delete all rules in group (Supprimer toutes les règles du groupe)** : supprimez toutes les règles d'un groupe d'étiquettes sélectionné.
   - **Clone all rules in group (Cloner toutes les règles du groupe)** : clonez toutes les règles d'un groupe d'étiquettes sélectionné.




2. **Commit (Validez)** vos modifications.

# Utilisation d'une liste dynamique externe dans une politique

Une liste dynamique externe (anciennement appelée Liste d'interdictions dynamiques) est un fichier texte que vous (ou une autre source) hébergez sur un serveur Web externe pour que le pare-feu puisse importer des objets (adresses IP, URL, domaines) en vue d'appliquer une politique sur les entrées de la liste. Lorsque la liste est mise à jour, le pare-feu importe la liste de manière dynamique à l'intervalle configuré et applique la politique sans devoir effectuer des modifications de configuration ou des validations sur le pare-feu.

- Liste dynamique externe
- Directives de mise en forme d'une liste dynamique externe
- Listes dynamiques externes intégrées
- Configuration du pare-feu pour qu'il accède à une liste dynamique externe
- Configurer le Pare-feu pour Accéder à une liste dynamique externe à partir du service d'hébergement EDL
- Récupération d'une liste dynamique externe du serveur Web
- Afficher les entrées de la liste dynamique externe
- Exclure des entrées d'une liste dynamique externe
- Application de la politique à une liste dynamique externe
- Trouver les listes dynamiques externes dont l'authentification a échoué
- Désactivation de l'authentification d'une liste dynamique externe

## Liste dynamique externe

Une liste dynamique externe est un fichier texte qui est hébergé sur un serveur web externe afin que le pare-feu puisse importer des objets - adresses IP, URL, domaines, identités internationales d'équipement mobile (IMEI), identités internationales d'abonnés mobiles (IMSI) - inclus dans la liste et appliquer la politique. Pour appliquer la politique de sécurité aux entrées incluses dans la liste dynamique externe, vous devez faire référence à la liste dans une règle ou un profil politique pris en charge. Lorsque plusieurs listes sont référencées, vous pouvez organiser l'ordre d'évaluation pour vous assurer que les EDL les plus importantes sont validées avant d'atteindre les limites de capacité. Lorsque vous modifiez la liste, le pare-feu importe la liste de manière dynamique à l'intervalle configuré et applique la politique sans devoir effectuer des modifications de configuration ou des validations sur le pare-feu. Si le serveur web est inaccessible, le pare-feu utilise la dernière liste récupérée avec succès pour appliquer la politique jusqu'à ce que la connexion soit rétablie avec le serveur web. En cas d'échec de l'authentification sur l'EDL, la politique de sécurité cesse d'appliquer l'EDL. Pour récupérer la liste dynamique externe, le pare-feu utilise l'interface qui est configurée avec l'itinéraire de service **Palo Alto Networks Services (Services Palo Alto Networks)**.

Le pare-feu prend en charge ces types de listes dynamiques externes :

- **Adresse IP prédéfinie** : une liste d'adresses IP prédéfinies est un type de liste d'adresses IP qui fait référence à des listes d'adresses IP dynamiques intégrées qui possèdent du contenu fixe ou prédéfini. Ces listes dynamiques externes intégrées—pour les fournisseurs d'hébergement à toute épreuve, les sites malveillants connus et les adresses IP à risque élevé—sont automatiquement

ajoutées à votre pare-feu si vous disposez d'une licence de prévention contre les menaces actives. Une liste d'adresses IP prédéfinies peut également faire référence à une liste dynamique externe qui utilise l'une des listes intégrées en tant que source. Comme vous ne pouvez pas modifier le contenu d'une liste prédéfinie, vous pouvez utiliser une liste prédéfinie comme source pour une autre ED si vous souhaitez ajouter ou exclure des entrées de liste.

- **Predefined URL List (Liste d'URL prédéfinies)** : ce type de liste dynamique externe contient des URL pré-remplies que les applications utilisent pour des services en arrière-plan, tels que les mises à jour ou les vérifications de la liste de révocation des certificats (CRL), que le pare-feu peut exclure sans risque de la politique d'authentification. Palo Alto Networks révise et maintient ce type de liste dynamique externe, également connue sous le nom de Authentication Portal Exclude List (Liste d'exclusion de portail d'authentification), par des mises à jour du contenu.
- **Adresse IP** : le pare-feu applique généralement une politique pour une adresse IP source ou de destination définie comme objet statique sur le pare-feu (reportez-vous à la section Application d'une politique sur une liste dynamique externe). Si vous avez besoin de souplesse pour appliquer une politique pour une liste d'adresses IP sources ou de destination qui apparaissent ad hoc, vous pouvez utiliser une liste dynamique externe d'adresses IP en tant qu'objet d'adresse source ou de destination dans les règles de politique et configurer le pare-feu pour autoriser ou refuser l'accès aux adresses IP (adresses IPv4 et IPv6, plages d'adresses IP et sous-réseaux IP) comprises dans la liste. Vous pouvez également utiliser une EDL d'adresses IP dans la source ou la destination d'une règle de politique SD-WAN. Le pare-feu traite une liste dynamique externe d'adresses IP en tant qu'objet d'adresse ; toutes les adresses IP comprises dans une liste sont traitées en tant qu'un seul objet d'adresse.
- **Domain (Domaine)** : ce type de liste dynamique externe vous permet d'importer des noms de domaine personnalisés dans le pare-feu pour appliquer la politique à l'aide d'un profil antispyware ou d'une règle de politique SD-WAN. Une EDL dans un profil antispyware est très utile si vous êtes abonné à des flux de renseignements sur les menaces de tiers et que vous souhaitez protéger votre réseau contre de nouvelles sources de menaces ou de logiciels malveillants dès que vous êtes mis au courant de l'existence d'un domaine malveillant. Pour chaque domaine que vous incluez dans la liste dynamique externe, le pare-feu crée une signature de logiciel espion basée sur DNS pour que vous puissiez activer la mise en entonnoir DNS. La signature de logiciel espion basée sur DNS est de type logiciel espion de niveau de gravité moyen ; chaque signature est nommée **`Custom Malicious DNS Query <nom_de_domaine>`**. Vous pouvez également spécifier le pare-feu afin d'inclure les sous-domaines d'un domaine spécifié. Par exemple, si votre liste des domaines comprend paloaltonetworks.com, toutes les composantes de niveau inférieur du nom de domaine (p. ex., *.paloaltonetworks.com) seront également comprises dans la liste. Lorsque ce paramètre est activé, chaque domaine d'une liste donnée exige une entrée supplémentaire, ce qui a pour effet de doubler le nombre d'entrées utilisées par la liste. Pour de plus amples précisions sur la configuration des listes de domaine, reportez-vous à la section Configuration de la mise en entonnoir DNS pour une liste de domaines personnalisés.
- **URL** : ce type de liste dynamique externe vous donne la souplesse nécessaire pour protéger votre réseau contre de nouvelles sources de menaces ou de logiciels malveillants. Le pare-feu traite une liste dynamique externe d'URL en tant que catégorie d'URL personnalisée ; vous pouvez utiliser cette liste de l'une ou l'autre des façons suivantes :
  - En tant que critère de correspondance dans les règles de politique de sécurité, les règles de politique de déchiffrement et les règles de politique QoS afin d'autoriser, d'ignorer, de déchiffrer, de ne pas déchiffrer ou d'allouer de la bande passante aux URL de la catégorie personnalisée.

  - Dans un profil de filtrage des URL, pour lequel vous pouvez définir des actions plus granulaires, comme continuer, alerter ou écraser, avant d'associer le profil à une règle de politique de sécurité (reportez-vous à la section Utilisation d'une liste dynamique externe dans un profil de filtrage des URL).
- **Equipment Identity (Identité d'équipement)** : vous pouvez faire référence à une liste dynamique externe d'appareils IdO définis par des identités internationales d'équipements mobiles (IMEI) dans une règle de politique de sécurité qui contrôle le trafic des équipements connectés à un réseau 5G ou 4G. Reportez-vous à la section «Premiers pas avec l'infrastructure de réseau mobile» pour obtenir des informations sur la configuration de la sécurité de l'identification de l'équipement sur les modèles de pare-feu pris en charge.
- **Subscriber Identity (Identité d'abonné)** : vous pouvez faire référence à une liste dynamique externe d'identités internationales d'abonnés mobiles (IMSI) dans une règle de politique de sécurité qui contrôle le trafic des abonnés connectés à un réseau 5G ou 4G. Reportez-vous à la section «Premiers pas avec l'infrastructure de réseau mobile» pour obtenir des informations sur la configuration de la sécurité de l'identification de l'abonné sur les modèles de pare-feu pris en charge.

Sur chaque modèle de pare-feu, vous pouvez ajouter un maximum de 30 EDL personnalisées avec des sources uniques to enforce policy (pour appliquer la politique). La limite du nombre de listes dynamiques externes ne s'applique pas à Panorama. Lorsque vous utilisez Panorama pour gérer un pare-feu sur lequel plusieurs systèmes virtuels sont activés, si vous dépassez la limite du pare-feu, une erreur de validation s'affiche sur Panorama. Une source est une URL qui comprend l'adresse IP ou le nome d'hôte, le chemin et le nom de fichier pour la liste dynamique externe. Le pare-feu fait correspondre l'URL (chaîne complète) pour déterminer si une source est unique.

Bien que le pare-feu n'impose pas de limites quant au nombre de listes maximal d'un type particulier, les limites suivantes s'appliquent :

- Adresse IP - Les pare-feu PA-5200 Series et PA-7000 Series prennent en charge un maximum de 150 000 adresses IP totales ; tous les autres modèles prennent en charge un maximum de 50 000 adresses IP totales. Aucune limite n'est en vigueur pour le nombre d'adresses IP par liste. Lorsque la limite d'adresses IP prises en charge est atteinte sur le pare-feu, le pare-feu génère un message Syslog. Les adresses IP qui figurent dans les listes d'adresses IP prédéfinies ne sont pas comptabilisées dans la limite.
- URL et domaine : le nombre maximal d'URL et de domaines pris en charge varie selon le modèle. Aucune limite n'est en vigueur pour le nombre d'URL ou de domaines par liste. Reportez-vous au tableau suivant pour connaître les spécifications relatives à votre modèle :

| Modèle | Limites du nombre d'URL par liste | Limites du nombre de domaines par liste |
|---|---|---|
| PA-5200 Series, PA-7000 Series (mis à niveau avec la NPC 20GXM du PA-7000, la NPC 20GQXM du PA-7000 ou la NPC 100G du PA-7000). | 250 000 | 4 000 000 |

| Modèle | Limites du nombre d'URL par liste | Limites du nombre de domaines par liste |
|---|---|---|
| *Les appareil PA-7000 qui possèdent des NPC mixtes ne prennent en charge que les capacités standard.* | | |
| VM-500, VM-700 | 100 000 | 2 000 000 |
| PA-850, PA-820, PA-3200 Series | 100 000 | 1 000 000 |
| PA-7000 Series (et appareils mis à niveau avec la NPC 20GQ du PA-7000 ou la NPC 20G du PA-7000), VM-300 | 100 000 | 500 000 |
| PA-220, VM-50, VM-50 (Lite), VM-100, VM-1000-HV | 50 000 | 50 000 |

Les entrées de la liste ne sont comptabilisées dans les limites du pare-feu que si elles appartiennent à une liste dynamique externe qui est utilisée dans la politique.

- *Lorsque vous effectuez une analyse syntaxique de la liste, le pare-feu saute toutes les entrées qui ne correspondent pas au type de liste et ignore les entrées qui dépassent le nombre maximum d'entrées prises en charge sur le modèle. Pour veiller à ce que le nombre d'entrées ne dépasse pas la limite, vérifiez le nombre d'entrées qui sont actuellement utilisées dans la politique. Sélectionnez* ***Objects (Objets)*** *>* ***External Dynamic Lists (Listes dynamiques externes)****, puis cliquez sur* ***List Capacities (Capacités de la liste)****.*
- *Une liste dynamique externe doit contenir des entrées. Si vous ne souhaitez plus utiliser la liste, supprimez la référence de la règle de politique ou du profil en laissant la liste vide. Si la liste ne contient aucune entrée, le pare-feu n'actualise pas la liste et continue à utiliser les dernières informations qu'il a récupérées.*
- *Palo Alto Networks recommande d'utiliser des listes dynamiques externes partagées lorsque plusieurs systèmes virtuels sont utilisés. L'utilisation de listes dynamiques externes individuelles avec des entrées doubles pour chaque système virtuel utilise plus de mémoire, ce qui peut entraîner une surutilisation des ressources du pare-feu.*
- *Le nombre d'entrée EDL sur les pare-feu exploitant des plusieurs systèmes virtuels tiennent compte de facteurs supplémentaires (tels que les DAG, le nombre de systèmes virtuels, les bases de règles) pour générer une liste plus précise de la consommation de capacité. Il peut en découler une divergence dans l'utilisation des capacités après la mise à jour des versions PAN-OS 8.x.*
- *Selon les fonctions qui sont activées sur le pare-feu, les limites d'utilisation de la mémoire peuvent être dépassées avant l'atteinte des limites de capacité des EDL, en raison des mises à jour de l'allocation de la mémoire. Palo Alto Networks recommande de revoir les capacités des EDL et, au besoin, de supprimer des EDL ou d'en regroupe dans des listes partagées afin de minimiser l'utilisation de la mémoire.*

## Directives de mise en forme d'une liste dynamique externe

Une liste dynamique externe d'un type (adresse IP, URL ou domaine) doit comprendre des entrées de ce type uniquement. Les entrées d'une liste d'adresses IP prédéfinies respectent les directives de mise en forme de listes d'adresses IP.

- Liste d'adresses IP
- Liste des domaines
- Liste des URL

## Liste d'adresses IP

Une liste dynamique externe peut inclure des adresses IP, des adresses de sous-réseau (adresse/masque) ou une plage d'adresses IP. En outre, la liste d'interdiction peut contenir des commentaires et des caractères spéciaux, tels que ***** , **:** , **;** , **#** ou **/**. La syntaxe de chaque ligne de la liste est **[adresse IP, adresse IP/masque, ou début de la plage d'adresses IP et fin de la plage d'adresses IP] [espace] [commentaire]**.

Saisissez chaque adresse IP/plage d'adresses IP/sous-réseau IP sur une nouvelle ligne ; les URL ou domaines ne sont pas pris en charge dans cette liste. Un sous-réseau ou une plage d'adresses IP comme 92.168.20.0/24 ou 192.168.20.40-192.168.20.50, sont comptabilisés comme une entrée d'adresse IP et pas comme plusieurs adresses IP. Si vous ajoutez des commentaires, ils doivent être sur la même ligne que l'adresse IP/plage d'adresses IP/sous-réseau IP. L'espace à la fin de l'adresse IP est le délimiteur qui sépare un commentaire de l'adresse IP.

Une liste d'adresse IP type :

```
192.168.20.10/32
 2001:db8:123:1::1 #test IPv6 address
 192.168.20.0/24 ; test internal subnet
 2001:db8:123:1::/64 test internal IPv6 range
 192.168.20.40-192.168.20.50
```

*Vous pouvez afficher une page de notification pour une adresse IP bloquée uniquement si le protocole est HTTP.*

## Liste des domaines

Vous pouvez utiliser des caractères génériques dans les listes de domaine pour configurer une entrée simple à faire correspondre à plusieurs sous-domaines de sites Web, pages, y compris des domaines entiers de premier niveau, et à des pages Web spécifiques.

Suivez les directives suivantes lorsque vous créez des entrées de listes de domaine :

- Saisissez chaque nom de domaine sur une nouvelle ligne ; les URL ou les adresses IP ne sont pas prises en charge dans cette liste.
- N'inscrivez pas http:// ou https:// devant le nom de domaine.
- Vous pouvez utiliser un astérisque (*) pour indiquer une valeur générique.
- Vous pouvez utiliser un caret (^) pour indiquer une valeur de correspondance exacte.
- Les caractères suivants sont considérés comme des séparateurs de jetons : . / ? & = ; +

  Chaque chaîne séparée par un ou deux de ces caractères est un jeton. Utilisez les caractères génériques en tant que marque substitutive d'un jeton, laquelle indique qu'un jeton spécifique peut contenir une valeur.
- Les caractères génériques sont les seuls caractères autorisés au sein d'un jeton ; cependant, une entrée peut contenir plusieurs caractères génériques.
- Chaque entrée de domaine peut contenir un maximum de 255 caractères.

**Quand utiliser un astérisque (*) :**

Utilisez un astérisque (*) pour indiquer un ou plusieurs sous-domaines variables. Par exemple, pour préciser l'application du site Web de Palo Alto Networks, peu importe l'extension du domaine utilisée, qui peut comporter un ou deux sous-domaine selon l'emplacement, vous ajouteriez l'entrée suivante : **`*.paloaltonetworks.com`**. Cette entrée correspondrait à docs.paloaltonetworks.com et à support.paloaltonetworks.com.

Vous pouvez également utiliser ce caractère générique pour indiquer des domaines entiers de premier niveau. Par exemple, pour préciser l'application d'un TLD nommé .work, vous ajouteriez l'entrée suivante : **`*.work`**. Cette entrée correspond à tous les sites Web qui se terminent par .work.

*Le caractère générique (*) ne peut être ajouté que dans les entrées de domaine.*

**Exemples d'astérisques (*)**

| Entrée de la liste des domaines EDL | Sites correspondants |
|---|---|
| **`*.company.com`** | eng.tools.company.com<br>support.tools.company.com<br>tools.company.com<br>docs.company.com |
| **`*.click`** | tous les sites Web qui se terminent par un domaine de premier niveau .click. |

**Quand utiliser un caret (^) :**

Utilisez les carets (^) pour indiquer une correspondance exacte d'un sous-domaine. Par exemple, **`^paloaltonetworks.com`** ne correspond qu'à paloaltonetworks.com. Cette entrée ne correspond à aucun autre site.

**Exemples de carets (^)**

| Entrée de la liste des domaines EDL | Site correspondant |
|---|---|
| **`^company.com`** | company.com |
| **`^eng.company.com`** | eng.company.com |

### Liste des URL

Reportez-vous à la section Exceptions de catégories d'URL.

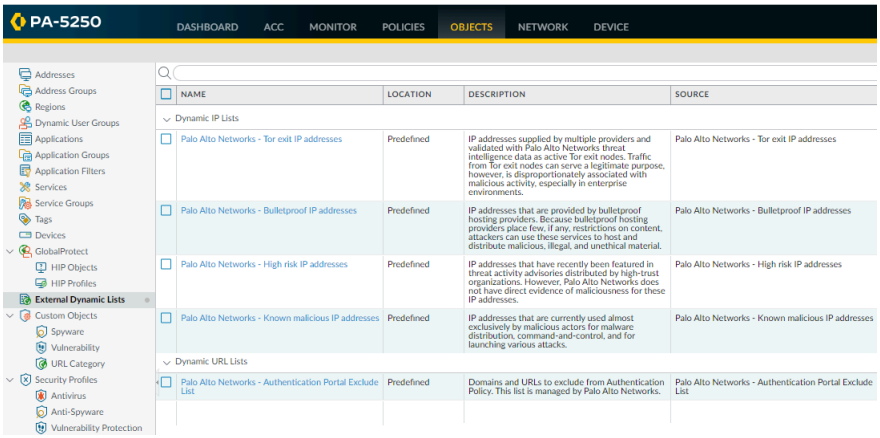
## Listes dynamiques externes intégrées

Avec une licence de prévention des menaces active, Palo Alto Networks fournit des EDL d'adresses IP intégrées que vous pouvez utiliser pour obtenir une protection contre les hôtes malveillants.

- **Adresses IP à toute épreuve de Palo Alto Networks** : contient des adresses IP fournies par des fournisseurs d'hébergement à toute épreuve. Comme les fournisseurs d'hébergement à toute épreuve ne placent que quelques (voire aucune) restrictions sur le contenu, les pirates utilisent souvent ces services pour héberger et distribuer du contenu malveillant, illégal et contraire à l'éthique.
- **Adresses IP à risque élevé Palo Alto Networks)** : contient les adresses IP des informations sur les menaces émises par les organisations tierces de confiance. Palo Alto Networks compile la liste des informations sur les menaces, mais n'a pas de preuve directe du caractère malveillant des adresses IP.
- **Adresses IP malveillantes connues de Palo Alto Networks** : contient les adresses IP qui sont malveillantes selon l'analyse effectuée par WildFire, la recherche de l'Unité 42 et les données recueillies de la télémétrie (Partage de Données de Prévention des Menaces avec Palo Alto Networks). Les pirates se servent de ces adresses IP presque exclusivement pour distribuer des logiciels malveillants, pour initier des activités de commande et contrôle et pour lancer des attaques.
- **Palo Alto Networks Tor Exit IP Addresses (Adresses IP de sortie Tor de Palo Alto Networks)** : contient des adresses IP fournies par plusieurs fournisseurs et validées avec les données de renseignements sur les menaces de Palo Alto Networks en tant que nœuds de sortie Tor actifs. Le trafic provenant des nœuds de sortie Tor peut servir un objectif légitime, cependant, il est associé de manière disproportionnée à des activités malveillantes, en particulier dans les environnements d'entreprise.

Le pare-feu reçoit des mises à jour pour ces flux par l'intermédiaire des mises à jour du contenu, ce qui permet au pare-feu d'appliquer automatiquement la politique en tenant compte des plus récentes informations sur les menaces de Palo Alto Networks. Vous ne pouvez pas modifier le contenu des listes intégrées. Utilisez-les telles quelles (voir Application de la politique à une liste dynamique externe) ou créer une liste dynamique externe personnalisée qui utilise l'une des listes en tant que source (voir Configuration du pare-feu pour qu'il accède à une liste dynamique externe) et exclure les entrées de la liste, au besoin.




# Configuration du pare-feu pour qu'il accède à une liste dynamique externe

Vous devez établir la connexion entre le pare-feu et la source qui héberge la liste dynamique externe avant de pouvoir procéder à l'application de la politique sur une liste dynamique externe.

**STEP 1 |** (Facultatif) Personnalisez l'itinéraire de service que le pare-feu utilise pour récupérer les listes dynamiques externes.

Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Services (Services)** > **Service Route Configuration (Configuration de l'itinéraire de service)** > **Customize (Personnaliser)**, puis modifiez l'itinéraire de service des **listes dynamiques externes**.

*Le pare-feu n'utilise pas l'itinéraire de service des listes dynamiques externes pour récupérer les* Listes dynamiques externes intégrées *; les mises à jour du contenu modifient ou mettent à jour les contenus de ces listes (licence Prévention des menaces active nécessaire).*

**STEP 2 |** Trouvez une liste dynamique externe à utiliser avec le pare-feu.

- Créez une liste dynamique externe et hébergez-la sur un serveur Web. Saisissez les adresses IP, les domaines ou les URL dans un fichier texte vide. Chaque entrée de la liste doit se trouver sur une nouvelle ligne. Par exemple :

  ```
  financialtimes.co.in

  www.wallaby.au/joey

  www.exyang.com/auto-tutorials/How-to-enter-Data-for-Success.aspx
  ```

  Reportez-vous à la section Directives de mise en forme d'une liste dynamique externe pour garantir que le pare-feu ne saute pas des entrées. Pour éviter les erreurs de validation et les entrées non valides, n'inscrivez pas http:// ou https:// au début des entrées.
- Utilisez une liste dynamique externe hébergée par une autre source et vérifiez qu'elle respecte les directives de mise en forme d'une liste dynamique externe.

**STEP 3 |** Sélectionnez **Objects (Objets)** > **External Dynamic Lists (Listes dynamiques externes)**.

**STEP 4 |** Cliquez sur **Add (Ajouter)** et donnez un **Name (Nom)** descriptif à la liste.

**STEP 5 |** (Facultatif) Sélectionnez l'option **Shared (Partagé)** pour partager la liste avec tous les systèmes virtuels sur un périphérique prenant en charge plusieurs systèmes virtuels. Par défaut, l'objet est créé sur le système virtuel actuellement sélectionné dans la liste déroulante **Virtual Systems (Systèmes virtuels)**.

*Palo Alto Networks recommande d'utiliser des listes dynamiques externes partagées lorsque plusieurs systèmes virtuels sont utilisés. L'utilisation de listes dynamiques externes individuelles avec des entrées reprises pour chaque système virtuel utilise plus de mémoire, ce qui peut entraîner une surutilisation des ressources du pare-feu.*

**STEP 6 |** (Panorama uniquement) Sélectionnez **Disable override (Désactiver le contrôle prioritaire)** pour veiller à ce qu'un administrateur de pare-feu ne puisse appliquer de contrôle prioritaire sur les paramètres locaux d'un pare-feu qui hérite de cette configuration via une validation d'un groupe de périphériques de Panorama.

**STEP 7 |** Sélectionnez le **Type (Type)** de liste (par exemple, **URL List (Liste d'URL)**).

Assurez-vous que la liste n'inclut que les entrées correspondant à ce type de liste. Reportez-vous à la section Vérifiez si les entrées de la liste dynamique externe ont été ignorées ou sautées.

Si vous utilisez une liste des domaines, vous pouvez éventuellement activer l'option **Automatically expand to include subdomains (Élargir automatiquement sur l'inclusion de sous-domaines)** afin d'inclure également les sous-domaines d'un domaine spécifié. Par exemple, si votre liste des domaines comprend paloaltonetworks.com, toutes les composantes de niveau inférieur du nom de domaine (p. ex., *.paloaltonetworks.com) seront également comprises dans la liste. N'oubliez pas que lorsque ce paramètre est activé, chaque domaine d'une liste donnée exige une entrée supplémentaire, ce qui a pour effet de doubler le nombre d'entrées consommées.

**STEP 8 |** Saisissez la **Source (Source)** de la liste que vous venez de créer sur le serveur Web. La source doit inclure le chemin complet pour accéder à la liste. Par exemple, **`https://1.2.3.4/EDL_IP_2015`**.

- Si vous créez une liste dynamique externe d'adresses IP prédéfinies, sélectionnez un flux d'adresses IP malveillantes Palo Alto Networks à utiliser en tant que source.
- Si vous créez une liste dynamique externe d'URL prédéfinies, sélectionnez **panw-auth-portal-exclude-list** en tant que source.

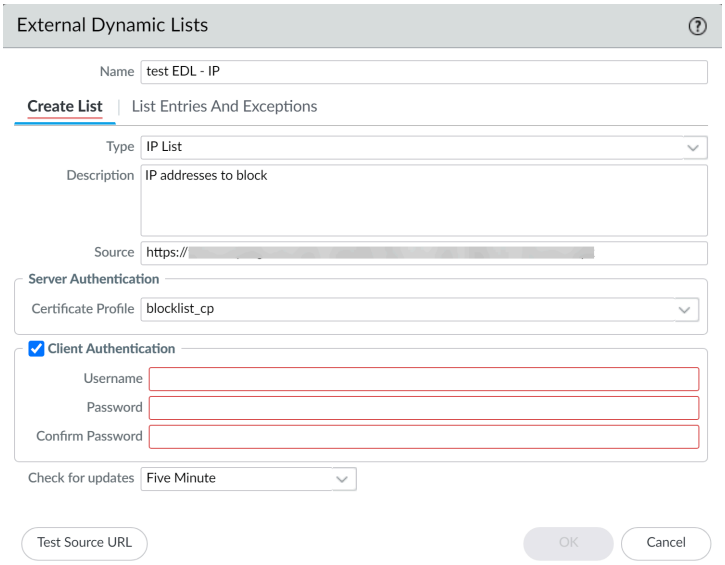
**STEP 9 |** Si la liste source est sécurisée par SSL (c.-à-d. des listes dotées d'URL HTTPS), activez l'authentification serveur. Sélectionnez un **Certificate Profile (Profil de certificat)** ou créez un **New Certificate Profile (Nouveau profil de certificat)** pour authentifier le serveur qui héberge la liste. Le profil de certificat que vous sélectionnez doit comprendre des certificats d'autorité de certification (CA) racine et intermédiaires qui correspondent aux certificats installés sur le serveur que vous authentifiez.

*Maximisez le nombre de listes dynamiques externes que vous pouvez utiliser pour mettre en œuvre la politique. Utilisez le même profil de certificat pour authentifier les listes dynamiques externes d'une même adresse URL source. Si vous affectez des profils de certificat différent à des listes dynamiques externes d'une même adresse URL source, le pare-feu compte chaque liste comme une liste dynamique externe unique.*

**STEP 10 |** Activez l'authentification client si la liste source comporte une adresse URL HTTPS et exige une authentification HTTP de base pour accéder à la liste.

1. Sélectionnez **Client Authentication (Authentification client)**.
2. Saisissez un **Username (Nom d'utilisateur)** valide pour accéder à la liste.
3. Saisissez le **Password (Mot de passe)** et **Confirm Password (Confirmez le mot de passe)**.




**STEP 11 |** (Non disponible sur Panorama ou pour les EDL d'URL prédéfinies) Cliquez sur **Test Source URL (Tester l'URL source)** pour vérifier que le pare-feu peut se connecter au serveur Web.

*La fonction **Test Source URL (Tester l'URL source)** n'est pas disponible lorsque l'authentification est utilisée pour l'accès à l'EDL.*

**STEP 12 |** (Facultatif) Spécifiez la fréquence à laquelle le pare-feu doit **Check for updates (Vérifier les mises à jour)** de la liste. Par défaut, le pare-feu récupère la liste toutes les heures et valide les modifications.

*L'intervalle est fonction de la dernière validation. Ainsi, pour un intervalle de cinq minutes, la validation se ferra dans cinq minutes si la dernière validation a eu lieu il y a une heure. Pour récupérer la liste immédiatement, reportez-vous à la section* Récupération d'une liste dynamique externe du serveur Web.

**STEP 13 |** Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.

**STEP 14 |** (Facultatif) Les listes dynamiques externes sont présentées dans l'ordre d'évaluation de haut en bas. Utilisez les commandes directionnelles au bas de la page pour changer l'ordre de la liste. Ces commandes vous permettent d'organiser l'ordre des listes pour vous assurer que les EDL les plus importantes sont validées avant d'atteindre les limites de capacité.

*Vous pouvez également modifier l'ordre de la EDL lorsque l'option **Group By Type (Regrouper par type)** est décochée.*

**STEP 15 |** Application de la politique à une liste dynamique externe .

***En cas d'échec de l'authentification serveur ou client, le pare-feu cesse d'appliquer la politique selon la dernière liste externe dynamique qui a été récupérée avec succès.*** Trouvez des listes dynamiques externes dont l'authentification a échoué ***et examinez pourquoi l'authentification a échoué.***

# Configurer le Pare-feu pour Accéder à une liste dynamique externe à partir du service d'hébergement EDL

Configurer le pare-feu pour accéder à une liste dynamique externe (EDL) à partir du service d'hébergement EDL pour les applications Software-as-a-Service (SaaS)

- Créer une liste dynamique externe à l'aide du service d'hébergement EDL
- Convertir le certificat GlobalSign Root R1 au format PEM

## Créer une liste dynamique externe à l'aide du service d'hébergement EDL

Certains fournisseurs de logiciels en tant que service (SaaS) publient des listes d'adresses IP et d'URL en tant que points de terminaison de destination pour leurs applications SaaS. Les fournisseurs SaaS mettent fréquemment à jour les listes de points de terminaison de destination des applications SaaS à mesure que le support augmente et que le service se développe. Cela vous oblige à surveiller manuellement les points de terminaison d'application SaaS pour les modifications et à mettre à jour manuellement la configuration de votre politique pour assurer la connectivité à ces applications SaaS critiques ou à configurer un outil externe pour surveiller et mettre à jour vos EDL.

Configurez une EDL à l'aide du EDL Hosting Service (service d'hébergement EDL) maintenu par Palo Alto Networks pour alléger la charge opérationnelle de la maintenance d'une EDL pour une application SaaS. Le service d'hébergement EDL fournit des URL de flux accessibles au public pour les points de terminaison d'application SaaS publiés par le fournisseur d'applications SaaS. L'utilisation d'une URL de flux comme source dans un EDL permet une application dynamique du trafic des applications SaaS sans que vous ayez besoin d'héberger et de gérer votre propre source EDL.

Palo Alto Networks vérifie quotidiennement les URL de flux d'applications publiées par les fournisseurs SaaS. Pour les flux basés sur IP, Palo Alto Networks effectue des optimisations pour combiner les entrées d'un masque de réseau continu et une déduplication est effectuée si les points de terminaison se chevauchent dans plusieurs zones. De plus, les points de terminaison de l'application Microsoft 365 Common et Office Online SaaS sont toujours ajoutés à chaque URL de flux dans le service d'hébergement EDL.

Microsoft met à jour toutes les URL de flux Microsoft 365 à la fin de chaque mois civil et fournit un préavis de 30 jours avant la mise à jour. Consultez la official Microsoft 365 Web Services page (page officielle des services Web Microsoft 365) pour plus d'informations. L'état de disponibilité et les mises à jour du service d'hébergement EDL sont publiés sur la page Palo Alto Networks Cloud Services Status (état des services cloud de Palo Alto Networks).

**STEP 1 |** Visitez le EDL Hosting Service (service d'hébergement EDL) et identifiez l'URL du flux pour votre application SaaS.

Consultez la Microsoft 365 documentation (documentation Microsoft 365) pour plus d'informations sur l'URL de flux qui convient le mieux à votre cas d'utilisation. De plus, tenez compte de l'application SaaS et de l'emplacement des utilisateurs accédant à l'application SaaS

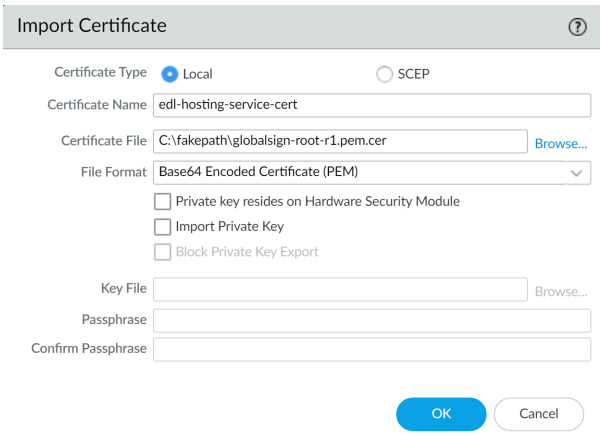
lors de l'identification d'une URL de flux vers. Par exemple, si vous avez une succursale en Allemagne qui n'a besoin d'accéder qu'à Exchange Online, sélectionnez une URL de flux dans la **zone de service : Échange en ligne** pour l'**Allemagne**.

***Pour une règle de politique de** policy-based forwarding (transfert basée sur une politique), **utilisez une URL de flux basée sur IP.***

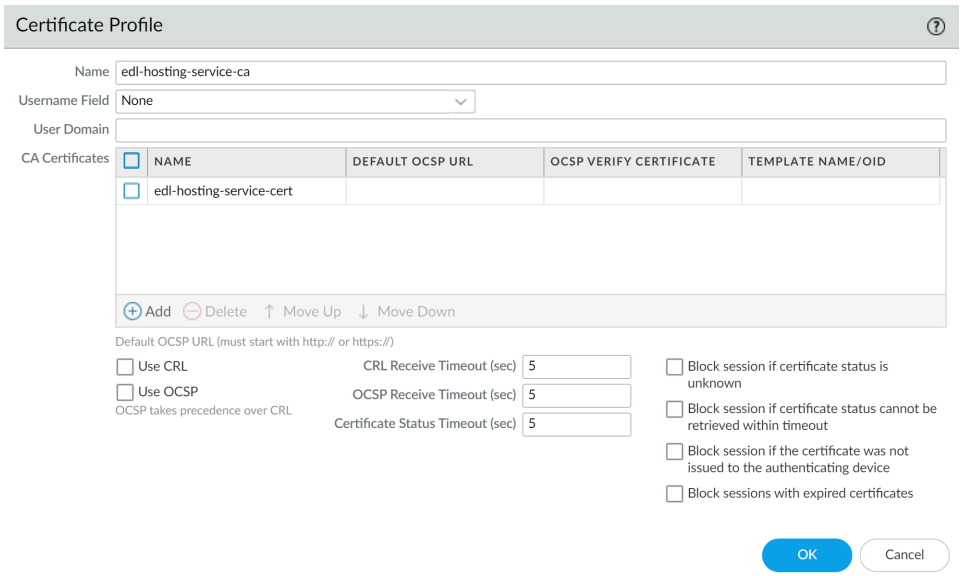
**STEP 2 |** (Best Practices (Meilleures pratiques)) Créez un profil de certificat pour authentifier le service d'hébergement EDL.

1. Téléchargez le GlobalSign Root R1 certificate (certificat GlobalSign Root R1).
2. Convertir le certificat GlobalSign Root R1 au format PEM.
3. Lancez l'interface Web du pare-feu.
4. Importez le certificat GlobalSign Root R1.
   1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** et **Import (Importez)** un nouveau certificat.
   2. Pour **Certificate Type (Type de certificat)**, sélectionnez **Local**.
   3. Saisissez un **Certificate Name (Nom de certificat)** descriptif.
   4. Pour le **Certificate File (fichier de certificat)**, sélectionnez **Browse (Parcourir)** et sélectionnez le certificat que vous avez converti à l'étape précédente.
   5. Pour le **File Format (format de fichier)**, sélectionnez **Base64 Encoded Certificate (PEM) (Certificat codé en Base64 (PEM))**.
   6. Cliquez sur **OK**.




5. Créez un profil de certificat d'autorité de certification (CA).
   1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificat)**, puis **Add (Ajouter)** un nouveau profil de certificat.
   2. Saisissez un **Name (Nom)** descriptif.
   3. Pour les **CA Certificates (certificats CA)**, **Add (ajoutez)** le certificat que vous avez importé à l'étape précédente.
   4. Cliquez sur **OK**.




6. **Commit** (Valider).

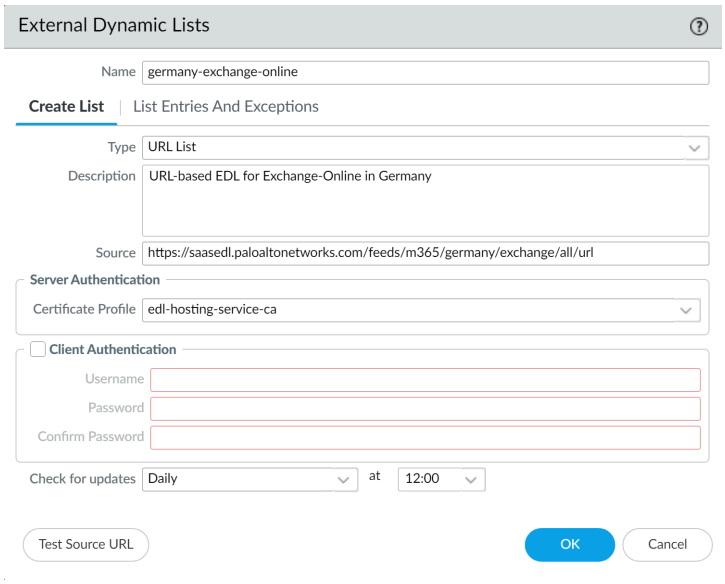
**STEP 3 |** Créez un EDL à l'aide d'une URL de flux du service d'hébergement EDL.

1. Sélectionnez **Objects (Objets)** > **External Dynamic Lists (Listes dynamiques externes)** et **Add (ajoutez)** une nouvelle liste EDL.
2. Donnez un **Name (Nom)** descriptif à l'EDL.
3. Sélectionnez le **Type** d'EDL.
   - Pour une liste EDL basée sur IP, sélectionnez **IP List (Liste IP)**.
   - Pour une liste EDL basée sur une URL, sélectionnez **URL List (Liste d'URL)**.
4. (Optional (Facultatif)) Saisissez une **Description for the EDL Description de l'EDI**.
5. Saisissez l'URL du flux comme **Source** d'EDL.

   *Appliquez tous les points de terminaison dans une URL de flux spécifique. L'ajout d'une exclusion d'un point de terminaison spécifique à partir d'une URL de flux peut entraîner des problèmes de connectivité à l'application SaaS.*
6. (**Best Practices (Bonnes pratiques)** Sélectionnez le Certificate Profile (Profil de certificat) que vous avez créé à l'étape précédente.
7. Spécifiez la fréquence à laquelle le pare-feu doit **Check for updates (rechercher des mises à jour)** pour correspondre à la fréquence de mise à jour de l'URL du flux.

   Par exemple, si l'URL du flux est mise à jour quotidiennement par Palo Alto Networks, configurez l'EDL pour rechercher les mises à jour **Daily (quotidiennement)**.

   Palo Alto Networks affiche la fréquence de mise à jour pour chaque URL de flux dans le EDL Hosting Service (service d'hébergement EDL). Les URL de flux sont automatiquement mises à jour avec tous les nouveaux points de terminaison.
8. Cliquez sur **Test Source URL (Tester l'URL source)** pour vérifier que le pare-feu peut accéder à l'URL du flux à partir du service d'hébergement EDL.
9. Cliquez sur **OK**.



**STEP 4 |** Application de la politique à une liste dynamique externe.

Lorsque vous appliquez une politique sur une EDL à partir du service d'hébergement EDL où l'EDL est la source, soyez précis lors de la configuration des utilisateurs qui ont accès à l'application SaaS pour éviter de surprovisionner l'accès à l'application.

***Tirez parti de** App-ID **aux côtés des EDL dans une règle de politique pour une application stricte supplémentaire du trafic des applications SaaS.***

## Convertir le certificat GlobalSign Root R1 au format PEM

Vous devez convertir le certificat GlobalSign Root R1 au format **PEM** pour créer un profil de certificat pour authentifier le service d'hébergement EDL. La création du profil de certificat pour authentifier le service d'hébergement EDL est une bonne pratique lors de l'utilisation du service d'hébergement EDL lorsque vous configure the firewall to access an external dynamic list from the EDL Hosting Service (configurez le pare-feu pour accéder à une liste dynamique externe à partir du service d'hébergement EDL).

Reportez-vous à la procédure appropriée en fonction du système d'exploitation du périphérique sur lequel vous avez téléchargé le certificat GlobalSign Root R1.

**STEP 1 |** Téléchargez le GlobalSign Root R1 certificate (certificat GlobalSign Root R1) si vous n'avez pas encore téléchargé le certificat.

**STEP 2 |** Convertissez le certificat.

- **Systèmes d'exploitation Mac et Linux**

1. Ouvrez le terminal et convertissez le certificat GlobalSign Root R1 que vous avez téléchargé.

```
admin:  openssl x509 -in <certificate-path>.crt -inform DER -out
 <target-export-path>.pem -outform PEM
```

```
admin-1@admin-1:~$ openssl x509 -in /home/admin-1/Downloads/Root-R1.crt -inform
DER -out /home/admin-1/Downloads/globalsign-root-r1.pem -outform PEM
```

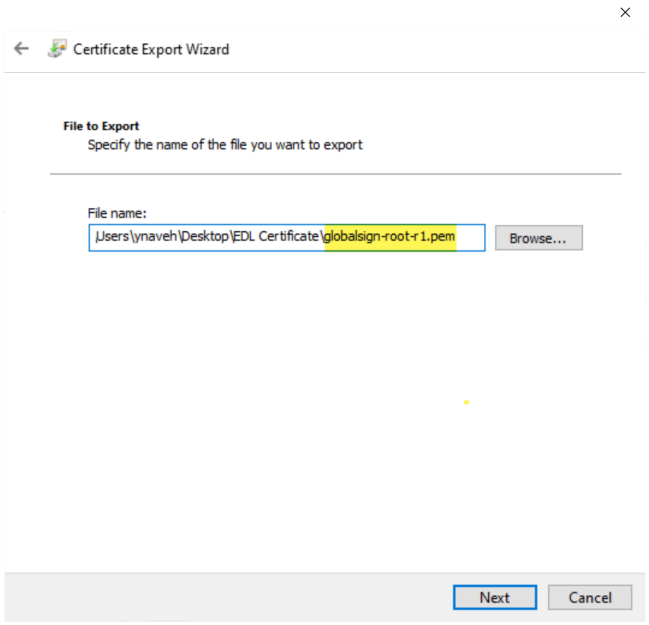
*Si aucun chemin d'exportation cible n'est spécifié, le certificat converti est créé sur le bureau du périphérique.*

- **Windows operating system (Système d'exploitation Windows)**

1. Accédez à l'emplacement où vous avez téléchargé le certificat GlobalSign Root1.
2. Double-cliquez et **Open (ouvrez)** le certificat.
3. Cliquez sur **Details (Détails)** et **Copy to File (copiez dans un fichier)**.

   Cliquez sur **Next (Suivant)** lorsque vous êtes invité à continuer.
4. Sélectionnez **Base-64 encoded x.509 (.CER)** et cliquez sur **Next (Suivant)**
5. Cliquez sur **Browse (Parcourir)** pour accéder à l'emplacement où vous souhaitez copier le certificat et entrez un nom pour le certificat qui inclut **`.pem`** ajouté à la fin du nom de fichier. Par exemple, **`globalsign-root-r1.pem`**

   **Save (Enregistrez)** le certificat. Le **File Name (nom de fichier)** affiché affiche le chemin d'exportation cible et le nom du certificat que vous avez entré avec `.cer` ajouté. Supprimez le`.cer`ajouté.




6. Cliquez sur **Next (Suivant)** et **Finish (terminer)** l'exportation du certificat.

## Récupération d'une liste dynamique externe du serveur Web

Quand vous Configurez le pare-feu pour qu'il accède à une liste dynamique externe, vous pouvez configurer le pare-feu pour qu'il récupère la liste du serveur web toutes les heures (par défaut), toutes les cinq minutes, tous les jours, toutes les semaines, ou tous les mois. Si vous avez ajouté ou supprimé des adresses IP de la liste et avez besoin d'une actualisation immédiate, utilisez le processus suivant pour récupérer la liste mise à jour.

**STEP 1 |** Pour récupérer la liste à la demande, sélectionnez **Objects (Objets)** > **External Dynamic Lists (Listes dynamiques externes)**.

**STEP 2 |** Sélectionnez la liste que vous souhaitez actualiser et cliquez sur **Importer maintenant**. La tâche d'importation de la liste sera ajoutée à la file d'attente.

**STEP 3 |** Pour afficher le statut de la tâche dans le Gestionnaire de tâches, reportez-vous à la section Gestion et surveillance des tâches administratives.

**STEP 4 |** (Facultatif) Une fois que le pare-feu a récupéré la liste, Affichez les entrées d'une liste dynamique externe.

## Afficher les entrées de la liste dynamique externe

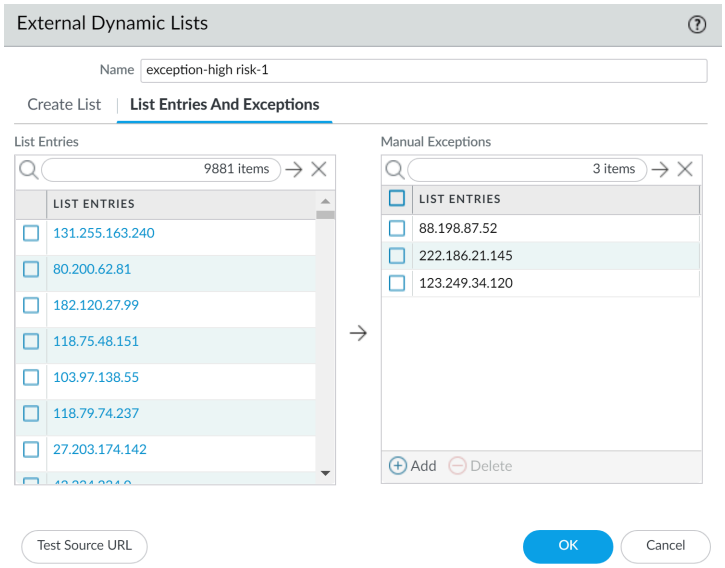
Avant d'Appliquer une politique sur une liste dynamique externe, vous pouvez afficher le contenu d'une liste dynamique externe directement sur le pare-feu pour vérifier s'il contient certaines valeurs d'adresse IP, de domaine ou d'URL. Les entrées affichées sont basées sur la version de la liste dynamique externe que le pare-feu a récupérée le plus récemment.

**STEP 1 |** Sélectionnez **Objects (Objets)** > **External Dynamic Lists (Listes dynamiques externes)**.

**STEP 2 |** Cliquez sur la liste dynamique externe que vous souhaitez afficher.

**STEP 3 |** Cliquez sur **List Entries and Exceptions (Répertorier les entrées et exceptions)** et affichez les objets que le pare-feu a récupérés dans la liste.




La liste peut être vide :

- L'EDL n'a pas encore été appliquée à une règle de politique de sécurité. Pour appliquer une liste EDL à une règle de stratégie de sécurité et remplir la liste EDL, reportez-vous à la section Application de la politique à une liste dynamique externe.
- Si le pare-feu n'a pas encore récupéré la liste dynamique externe. Pour forcer le pare-feu à récupérer la liste dynamique externe immédiatement, Récupérez une liste dynamique externe à partir du serveur Web.
- Le pare-feu ne parvient pas à accéder au serveur qui héberge la liste dynamique externe. Cliquez sur **Test Source URL (Tester l'URL source)** pour vérifier que le pare-feu peut se connecter au serveur.

**STEP 4 |** Saisissez une adresse IP, un domaine ou une URL (en fonction du type de liste) dans le champ de filtre et appliquez le filtre (→) pour vérifier sa présence dans la liste. Excluez les entrées d'une liste dynamique externe en fonction des adresses IP, domaines et URL que vous devez bloquer ou autoriser.

**STEP 5 |** (Facultatif) Affichez le Résumé des renseignements d'AutoFocus pour une entrée de liste. Placez le curseur sur une entrée pour ouvrir le menu déroulant, puis cliquez sur **AutoFocus**.

## Exclure des entrées d'une liste dynamique externe

Lors de l'affichage des entrées d'une liste dynamique externe, vous avez la possibilité d'en exclure 100 de la liste. Cette option vous permet d'appliquer la politique sur certaines des entrées d'une liste (mais pas toutes), ce qui peut s'avérer utile si vous ne pouvez modifier le contenu d'une liste dynamique externe (comme le flux d'adresse IP à risque élevé Palo Alto Networks), car elle provient d'une source tierce.

**STEP 1 |** Affichez les entrées de la liste dynamique externe.

**STEP 2 |** Sélectionnez un maximum de 100 entrées à exclure de la liste et cliquez sur Submit (Soumettre) (→) ou **Add (Ajoutez)** manuellement une exception à la liste.

- Vous ne pouvez pas enregistrer vos modifications dans la liste dynamique externe si vous avez des entrées en double dans la liste des Exceptions manuelles. Pour identifier des entrées doubles, cherchez les entrées qui sont surlignées en rouge.
- Une exception manuelle doit correspondre exactement à une entrée de la liste. De plus, vous ne pouvez pas exclure une adresse IP spécifique d'une plage d'adresses IP. Pour exclure une adresse IP spécifique d'une plage d'adresses IP, vous devez ajouter chaque adresse IP de la plage en tant qu'entrée de liste, puis exclure l'adresse IP souhaitée.

  Le pare-feu ne prend pas en charge l'exclusion d'une adresse IP individuelle d'une plage d'adresses IP.

**STEP 3 |** Cliquez sur **OK (OK)** puis sur **Commit (Valider)** pour enregistrer vos modifications.

**STEP 4 |** (Facultatif) Application de la politique à une liste dynamique externe.

## Application de la politique à une liste dynamique externe

Bloquez ou autoriser le trafic selon les adresses IP ou les URL qui figurent dans une liste dynamique externe ou utilisez une liste de domaines dynamiques avec la mise en entonnoir DNS pour prévenir l'accès à des domaines malveillants.

*Conseils pour mettre en œuvre la politique sur le pare-feu à l'aide de listes dynamiques externes :*

- *Lorsque vous affichez des listes dynamiques externes sur le pare-feu (**Objects (Objets) > External Dynamic Lists (Listes dynamiques externes)**), cliquez sur **List Capacities (Capacités de la liste)** pour comparer le nombre d'adresses IP, de domaines et d'URL qui sont actuellement utilisées dans une politique au nombre total d'entrées que le pare-feu prend en charge pour chaque type de listes.*
- *Procédez à l'*utilisation de la recherche globale pour effectuer une recherche sur le serveur de gestion du pare-feu ou de Panorama *pour un domaine, une adresse IP ou une URL qui appartient à une ou plusieurs listes dynamiques externes utilisées dans une politique. Cette recherche s'avère utile pour déterminer la liste dynamique externe (dont une règle de politique de sécurité fait référence) qui fait en sorte que le pare-feu bloque ou autorise un certain domaine, une certaine adresse IP ou une certaine URL.*
- *Utilisez les commandes directionnelles au bas de la page pour changer l'ordre d'évaluation des EDL. Ces commandes vous permettent d'organiser l'ordre des listes pour vous assurer que les entrées les plus importantes d'une EDL sont validées avant d'atteindre les limites de capacité.*

  *Vous pouvez également modifier l'ordre de la EDL lorsque l'option **Group By Type (Regrouper par type)** est décochée.*

- Configuration de la mise en entonnoir DNS pour une liste de domaines personnalisés.
- Utilisation d'une liste dynamique externe dans un profil de filtrage des URL

- **Utilisation d'une liste dynamique externe de Type URL en tant que critère de correspondance dans une règle de politique de sécurité.**
  1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
  2. Cliquez sur **Add (Ajouter)** et donnez un **Name (Nom)** descriptif à la règle.
  3. Dans l'onglet **Source (Source)**, sélectionnez la **Source Zone (Zone source)**.
  4. Dans l'onglet **Destination (Destination)**, sélectionnez la **Destination Zone (Zone de destination)**.
  5. Dans l'onglet **Service/URL Category (Catégorie de service/d'URL)**, cliquez sur **Add (Ajouter)** pour sélectionner la bonne liste dynamique externe dans la liste Catégorie d'URL.
  6. Dans l'onglet **Actions (Actions)**, définissez le **Action Setting (Paramètre d'action)** sur **Allow (Autoriser)** ou **Deny (Refuser)**.
  7. Cliquez sur **OK**, puis sur **Commit (Valider)**.
  8. Vérifiez si les entrées de la liste dynamique externe ont été ignorées ou sautées.

     Pour revoir les détails d'une liste, servez-vous de la commande CLI suivante sur un pare-feu :

     ```
     request
     system external-list show type <domain | ip | url>
      name_of_list
     ```

     Par exemple :

     ```
     request system
     external-list show type url EBL_ISAC_Alert_List
     ```
  9. Vérifiez que l'action de politique est appliquée.
     1. Affichez les entrées de la liste dynamique externe pour la liste d'URL, et tentez d'accéder à une URL de la liste.
     2. Vérifiez que l'action que vous avez définie est appliquée.
     3. Pour surveiller l'activité sur le pare-feu :
        - Sélectionnez **ACC (ACC)** et ajoutez un domaine d'URL en tant que filtre général pour afficher l'activité sur le réseau et l'activité bloquée pour l'URL à laquelle vous avez accédé.
        - Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **URL Filtering (Filtrage des URL)** pour accéder à la vue détaillée du journal.

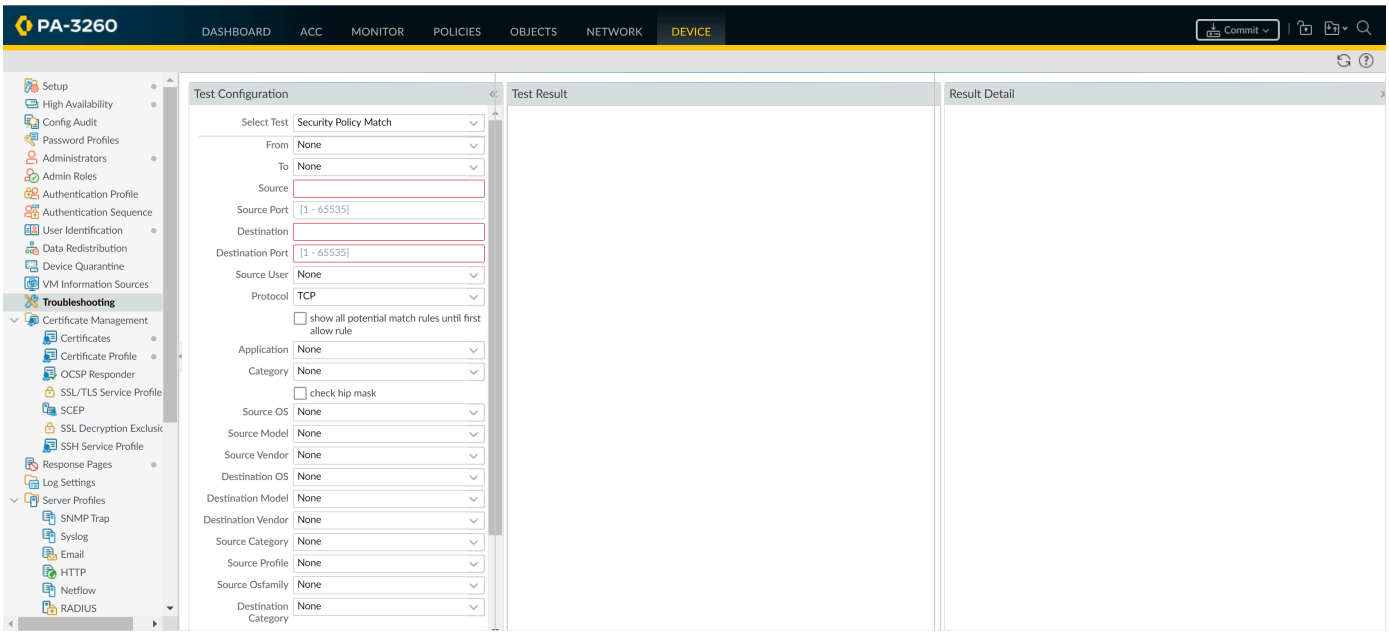
- **Utilisez une liste dynamique externe IP ou une liste dynamique externe IP prédéfinie comme objet d'adresse source ou de destination dans une règle de politique de sécurité.**

  Cette fonctionnalité s'avère utile si vous déployez de nouveaux serveurs et souhaitez autoriser l'accès aux serveurs nouvellement déployés sans qu'une validation du pare-feu soit nécessaire.

  1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
  2. Cliquez sur **Add (Ajouter)**, donnez un **Name (Nom)** descriptif à la règle.
  3. Dans les onglets **Source/Destination**, définissez la liste dynamique externe à utiliser en tant que **Source/Destination Address (Adresse source/de destination)**.
  4. Dans l'onglet Catégorie de service/d'URL, assurez-vous que le **service** est défini sur **application-default (Par défaut de l'application)**.
  5. Dans l'onglet Actions (Actions), définissez le Action Setting (Paramètre d'action) sur **Allow (Autoriser)** ou **Deny (Refuser)**.

     *Créez des listes dynamiques externes distinctes si vous souhaitez indiquer des actions Autoriser et Refuser pour certaines adresses IP.*
  6. Laissez toutes les autres valeurs à leurs valeurs par défaut.
  7. Cliquez sur **OK (OK)** pour enregistrer les modifications.
  8. **Commit (Validez)** les modifications.
  9. Vérifiez que l'action de politique est appliquée.
     1. Affichez les entrées de la liste dynamique externe pour la liste dynamique externe, puis tentez d'accéder à une adresse IP qui figure dans la liste.
     2. Vérifiez que l'action que vous avez définie est appliquée.
     3. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)** pour afficher l'entrée de journal de la session.
     4. Pour vérifier la règle de politique qui correspond à un flux, sélectionnez **Device (Périphérique)** > **Troubleshooting (Résolution des problèmes)**, puis exécutez un test de correspondance à la politique de sécurité :




- **Utilisez une liste dynamique externe d'URL prédéfinies pour exclure de la politique d'authentification les domaines bénins que les applications utilisent pour le trafic en arrière-plan.**

  Lorsque vous sélectionnez le type EDL **panw-auth-portal-exclude-list**, vous pouvez facilement exclure de l'application de la politique d'authentification les domaines que de nombreuses applications utilisent pour le trafic en arrière-plan, tels que les mises à jour et autres services de confiance. Cela garantit que le pare-feu ne bloque pas le trafic nécessaire pour ces services et que la maintenance des applications n'est pas interrompue.

  1. Sélectionnez **Policies (Politiques)** > **Authentication (Authentification)**.
  2. Dans l'onglet **Service/URL Category (Service/Catégorie d'URL)**, sélectionnez l'EDL d'UR prédéfinie **URL Category (Catégorie d'URL)**.
  3. Sur l'onglet **Actions**, sélectionnez **`default-no-captive-portal`** comme **Authentication Enforcement (Application de l'authentification)**.
  4. Cliquez sur **OK**.
  5. **Move (Déplacez)** la règle au sommet de sorte qu'elle soit la première règle dans la politique.
  6. **Commit (Validez)** vos modifications.

## Trouver les listes dynamiques externes dont l'authentification a échoué

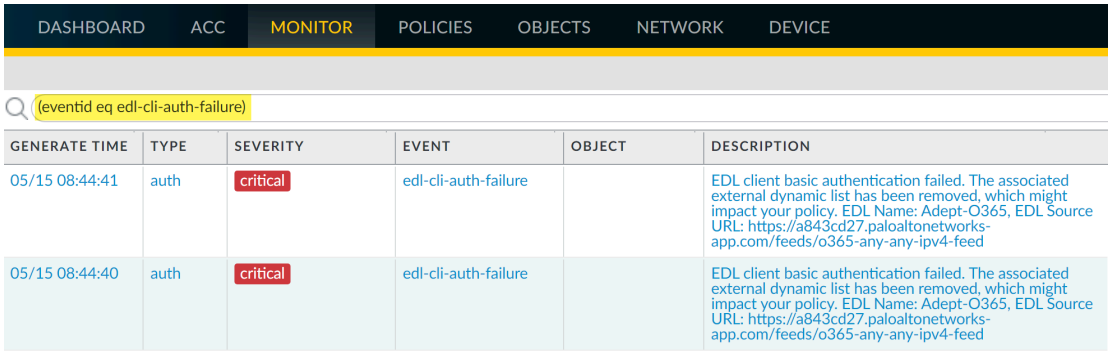
En cas d'échec de l'authentification d'une liste dynamique externe qui repose sur le protocole SSL auprès du serveur ou du client, le pare-feu génère un journal système de gravité critique. Le journal est critique puisque, après l'échec de l'authentification, le pare-feu cesse d'appliquer la politique en fonction de la liste dynamique externe. Servez-vous du processus suivant pour consulter les messages critiques du journal système vous avisant de tout échec de l'authentification qui concerne les listes dynamiques externes.

**STEP 1 |** Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **System (Système)**.

**STEP 2 |** Construisez les filtres suivants pour afficher les messages liés à un échec d'authentification, et appliquez les filtres. Pour plus d'informations, passez en revue le flux de travail complet pour filtrer les journaux.

- Échec de l'authentification serveur : **`(eventid eq tls-edl-auth-failure)`**
- Échec de l'authentification client : **`(eventid eq edl-cli-auth-failure)`**




**STEP 3 |** Passez en revue les messages des journaux système. Le nom de la liste dynamique externe, l'URL source de la liste et la raison pour laquelle l'authentification a échoué sont indiqués dans la description des messages.

L'authentification du serveur qui héberge la liste dynamique externe échoue si le certificat est expiré. Si vous avez configuré le profil de certificat pour vérifier l'état de révocation du certificat via la Certificate Revocation List (liste de révocation de certificats ; CRL) ou le Online Certificate Status Protocol (protocole de statut de certificat ouvert ; OCSP), l'authentification du serveur pourrait également échoué si :

- Le certificat est révoqué.
- L'état de révocation du certificat est inconnu.
- La connexion expire tandis que le pare-feu tente de se connecter au service CRL/OCSP.

Pour plus d'informations sur les paramètres du profil de certificat, reportez-vous aux étapes à suivre pour la configuration d'un profil de certificat.

***Vérifiez que vous avez ajouté la CA racine et la CA intermédiaire du serveur au profil du certificat configuré avec la liste dynamique externe. Autrement, la liste ne sera pas authentifiée correctement par le pare-feu.***

L'authentification client échoue si vous avez saisi une combinaison nom d'utilisateur/mot de passe erronée pour la liste dynamique externe.

**STEP 4 |** (Facultatif) Procédez à la désactivation de l'authentification d'une liste dynamique externe dont l'authentification a échoué comme solution provisoire en attendant que le propriétaire de la liste renouvelle le ou les certificats du serveur qui héberge la liste.

# Désactivation de l'authentification d'une liste dynamique externe

Palo Alto Networks recommande que vous activiez l'authentification des serveurs qui hébergent les listes dynamiques externes configurées sur votre pare-feu. Cependant, si vous trouvez des listes dynamiques externes dont l'authentification a échoué et préférez désactiver l'authentification au serveur de ces listes, vous pouvez le faire via la CLI. La procédure décrite ci-dessous ne s'applique qu'aux listes dynamiques externes qui sont sécurisées par SSL (c.-à-d., les listes qui possèdent une URL HTTPS) ; le pare-feu n'applique pas l'authentification au serveur pour les listes qui comportent une URL HTTP.

***La désactivation de l'authentification serveur d'une liste dynamique externe entraîne la désactivation de l'authentification client. Lorsque l'authentification client est désactivée, le pare-feu n'est pas en mesure de se connecter à une liste dynamique externe à laquelle un nom d'utilisateur et un mot de passe donnent accès.***

**STEP 1 |** Lancez la CLI et procédez comme suit pour passer en mode configuration :

```
username@hostname> configure
Entering configuration mode
[edit]
username@hostname#
```

Lorsque le symbole passe de > à #, c'est que vous êtes désormais en mode configuration.

**STEP 2 |** Saisissez la commande de la CLI qui correspond au type de liste :

- Adresse IP

```
set external-list <external dynamic list name> type ip
 certificate-profile None
```

- Domain (Domaine)

```
set external-list <external dynamic list name> type ip
 certificate-profile None
```

- URL

```
set external-list <external dynamic list name> type url
 certificate-profile None
```

**STEP 3 |** Vérifiez que l'authentification de la liste dynamique externe est désactivée.

Lancez l'actualisation de la liste (reportez-vous à la section Récupération d'une liste dynamique externe du serveur Web). Si le pare-feu parvient à récupérer la liste, l'authentification serveur est désactivée.

# Enregistrement dynamique des adresses IP et des étiquettes

Aujourd'hui, afin de surmonter les défis de l'évolution, du manque de flexibilité et des performances, l'architecture des réseaux permet la configuration, la modification et la suppression de clients, serveurs et applications à la demande. Cette souplesse constitue toutefois un défi pour les administrateurs de sécurité, car ils ont une visibilité réduite des adresses IP des serveurs et des clients configurés de manière dynamique, ainsi que des nombreuses applications pouvant être activées sur ces ressources virtuelles.

Le pare-feu-feu (modèles matériels et VM-Series) prend en charge la possibilité d'enregistrer dynamiquement les adresses IP, les ensembles IP (plages IP et sous-réseaux) et les étiquettes. Les adresses IP et les étiquettes peuvent être enregistrées directement sur le pare-feu ou via Panorama. Vous pouvez aussi supprimer des étiquettes de manière automatique sur les adresses IP source et de destination incluses dans le journal du pare-feu.

*PAN-OS ne prend en charge que les sous-réseaux IPv4 et les plages dans les groupes d'adresses dynamiques.*

Vous pouvez activer le processus d'enregistrement dynamique en utilisant l'une des options suivantes :

- **Agent User-ID pour Windows** : dans un environnement où vous avez déployé l'agent User-ID, ce dernier peut surveiller jusqu'à 100 serveurs VMware ESXi ou vCenter, ou une combinaison des deux. Lorsque vous configurez ou modifiez les machines virtuelles sur ces serveurs VMWare, l'agent peut récupérer les modifications d'adresse IP et les partager avec le pare-feu.
- **Sources d'informations de machine virtuelle** : cette option vous permet de surveiller les serveurs VMware ESXi, vCenter Server, AWS-VPC et Google Compute Engines nativement sur le pare-feu afin de récupérer les modifications d'adresse IP, lorsque vous configurez ou modifiez les machines virtuelles sur ces sources. Les sources d'informations de machines virtuelles recherchent un ensemble prédéfini d'attributs et ne nécessitent aucun script externe pour enregistrer les adresses IP via l'API XML. Reportez-vous à la section Surveillance des changements dans l'environnement virtuel.
- **Plug-in Panorama** : vous pouvez activer un appareil M-Series ou virtuel Panorama™ pour vous connecter à vos abonnements au cloud public d'Azure et de récupérer le mappage adresse IP-étiquette de vos machines virtuelles Azure déployées dans votre abonnement ou VPC. Panorama enregistre ensuite les informations de la machine virtuelle sur les pare-feux Palo Alto Networks gérés que vous avez configurés à des fins de notification, et vous pouvez utiliser ces attributs pour définir des groupes d'adresses dynamiques et les associer à des règles de politique de sécurité pour autoriser ou interdire le trafic vers ces machines virtuelles, ou depuis celles-ci.
- **VMware Service Manager** (solutions NSX intégrées uniquement) : la solution NSX intégrée a été conçue pour la configuration et la distribution automatiques de la plateforme d'exploitation dernière génération de Palo Alto Networks, ainsi que pour la fourniture de politiques de sécurité dynamiques basées sur le contexte à l'aide de Panorama. NSX Manager met à jour Panorama avec les dernières informations sur les adresses IP, ensembles IP et les étiquettes associées aux machines virtuelles déployées dans cette solution intégrée. Pour plus d'informations sur cette solution, reportez-vous à la section Paramétrage d'un pare-feu VM-Series NSX Edition.

- **API XML** : le pare-feu et Panorama prennent en charge une API XML qui utilise des requêtes HTTP standard pour envoyer et recevoir des données. Vous pouvez utiliser cette API pour enregistrer les adresses IP et les étiquettes sur le pare-feu ou via Panorama. Vous pouvez émettre des appels API directement ou en utilisant des structures de scripts ou d'applications prenant en charge les services basés sur REST. Pour plus d'informations, reportez-vous au Guide d'utilisation de l'API XML PAN-OS.
- **Étiquetage Automatique** : étiquetez l'adresse IP source ou de destination de manière automatique quand un journal est généré sur le pare-feu, et enregistrez cette adresse IP et ce mappage d'étiquettes auprès d'un agent User-ID sur le pare-feu ou dans Panorama, ou encore auprès d'un agent User-ID distant, en utilisant un profil serveur HTTP. Par exemple, à chaque fois qu'un pare-feu génère un journal de menaces, vous pouvez configurer le pare-feu pour qu'il étiquette l'adresse IP source dans le journal de menace avec un nom d'étiquette spécifique. Pour en savoir plus, reportez-vous à la section Utilisation de l'auto-étiquetage pour automatiser les actions de sécurité.

  De plus, vous pouvez configurer le pare-feu pour qu'il désenregistre dynamiquement une étiquette à l'issue d'une période de temps configurée. Par exemple, vous pouvez configurer le délai d'expiration pour qu'il est la même durée de temps que le délai du bail DHCP de l'adresse IP. Le mappage adresse IP-étiquette peut ainsi expirer en même temps que le bail DHCP, ce qui évite que vous appliquiez involontairement la politique lorsque l'adresse IP est réaffectée.

  Reportez-vous à Transférer les journaux vers une destination HTTP(s).

Pour plus d'information sur la création et l'utilisation de groupes d'adresses, reportez-vous à Utilisation de groupes d'adresses dynamiques dans une politique.

Reportez-vous à la rubrique Commandes CLI pour les adresses IP dynamiques et les étiquettes pour connaître les commandes CLI à utiliser pour enregistrer des étiquettes de manière dynamique.

# Utilisation de groupes d'utilisateurs dynamiques dans une politique

Les groupes d'utilisateurs dynamiques vous aident à créer une politique qui permet de remédier automatiquement aux comportements anormaux des utilisateurs et aux activités malveillantes tout en maintenant la visibilité de l'utilisateur. Après avoir créé le groupe et validé les changements, le pare-feu enregistre les utilisateurs et étiquettes associés et ensuite met à jour automatiquement l'appartenance dynamique des utilisateurs aux groupes Parce que les mises à jour d'appartenance des utilisateurs aux groupes est automatique, utilisez les groupes dynamiques d'utilisateurs au lieu des objets statiques de groupe pour répondre aux changements dans les comportements utilisateur ou menaces potentielles sans changement manuelle de politiques

Pour déterminer quels utilisateurs inclure en tant que membres, un groupe dynamique d'utilisateurs utilise des étiquettes comme critère de filtrage Dès qu'un utilisateur correspond au critère de filtrage, cet utilisateur devient un membre du groupe dynamique d'utilisateurs Le filtre utilise les opérateurs logiques ***et*** et ***ou***. Chaque étiquette est un élément metadata ou une paire attribut-valeur que vous enregistrez sur la source statiquement ou dynamiquement Les étiquettes statiques font partie de la configuration du pare-feu, tandis que les étiquettes dynamiques font partie de la configuration d'exécution Comme résultat, vous n'avez pas besoin de valider les mises à jour pour les étiquettes dynamiques si elles sont déjà associées à une politique que vous avez validé sur le pare-feu.

Pour dynamiquement enregistrer des étiquettes, vous pouvez utiliser :

- API XML
- agent User-ID
- Panorama
- Connectez-vous à l'interface Web du pare-feu.

Le pare-feu redistribue les étiquettes pour les groupes dynamiques d'utilisateurs aux agents de redistribution qui écoutent, qui incluent les autres pare-feux, Panorama, ou un collecteur de journaux dédié, ou encore les applications Cortex

***Pour supporter la redistribution d'étiquettes pour les groupes dynamiques d'utilisateurs, tous les pare-feux doivent être en 9.1 pour recevoir les étiquettes des sources enregistrées***

Le pare-feu redistribue les étiquettes pour les groupes dynamiques d'utilisateurs au saut suivant et vous pouvez configurer le transfert des journaux pour envoyer les journaux à un serveur spécifique Le transfert des journaux permet aussi d'utiliser l'auto-étiquetage pour automatiquement ajouter ou supprimer les membres de groupes dynamiques d'utilisateurs en s'appuyant sur les événements dans les journaux

**STEP 1 |** Sélectionnez **Objets** > **Groupes dynamiques d'utilisateurs** et **Ajoutez** un nouveau groupe dynamique d'utilisateurs

**STEP 2 |** Définissez l'adhésion à un groupe dynamique d'utilisateurs

1. Donnez un **Name (Nom)** à la zone.
2. (Facultatif) Saisissez une **Description** de l'interface.
3. **Ajouter un critères de correspondance** en utilisant les étiquettes dynamiques pour définir les membres du groupe dynamique d'utilisateurs.
4. (Optionnel) Utilise le **Et** ou **Ou** opérateurs avec le(s) étiquette(s) que vous voulez utiliser pour filtrer.
5. Cliquez sur **OK**.
6. (Optionnel) Sélectionnez les **Etiquettes** que vous voulez assigner au groupe lui-même

   *Cette étiquette affiche dans la colonne **Etiquettes** dans la liste **Groupe dynamique d'utilisateurs** et définit l'objet du groupe dynamique, pas les membres dans le groupe.*
7. Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.

   *Si vous mettez à jour le filtre d'objet groupes d'utilisateurs, vous devez valider les changements pour mettre à jour la configuration*

**STEP 3 |** En fonction de l'information de journal que vous souhaitez utiliser en tant que critères de correspondance, configurez l'auto-étiquetage en créant un profil de transfert des journaux ou en configurant les paramètres de journaux.

- Pour les journaux d'authentification, de données, de trafic, d'inspection Tunnel, d'URLs et de Wildfire, créez un profil de transfert des journaux.
- Pour les journaux User-ID, correspondance HIP, GlobalProtect et IP-étiquette, configurez les log settings (paramètres de journaux).

**STEP 4 |** (Facultatif) Pour retourner les membres du groupe dynamique d'utilisateurs à leurs groupes d'origine après une durée spécifique, entrez un **Délai d'expiration** en minutes (le défaut est 0, l'intervalle est 0-43200).

**STEP 5 |** Utilisez le groupe dynamique d'utilisateurs dans une politique pour réguler le trafic pour les membres du groupe.

Vous aurez besoin de créer au moins deux règles: Une pour autoriser le trafic initial pour remplir le groupe dynamique d'utilisateurs et une pour bloquer le trafic pour les activités que vous souhaitez empêcher Pour étiqueter les utilisateurs, la règle qui autorise le trafic doit avoir un numéro de règle plus haut dans votre jeu de règles que la règle qui interdit le trafic

1. Sélectionnez le groupe dynamique d'utilisateurs de l'étape 1 comme l'**Utilisateur Source**.
2. Créez la règle où l'**Action** bloque le trafic vers les membres du groupe dynamique d'utilisateurs
3. Créez la règle qui autorise le trafic pour remplir les membres du groupe dynamique d'utilisateurs
4. Si vous configurez un **profil de transfert des journaux** dans l'étape 3, sélectionnez le pour l'ajouter à la politique
5. **Commit (Validez)** vos modifications.

**STEP 6 |** (Optionnel) Affinez l'appartenance au groupe et définissez la source d'enregistrement pour les mises à jour du mappage utilisateur-vers-étiquette

Si le mappage initial utilisateur-vers-étiquette récupère des utilisateurs qui ne devraient pas être membres ou s'il n'inclut pas des utilisateurs qui devraient l'être, modifiez les membres du groupe pour inclure les utilisateurs pour qui vous voulez mettre en œuvre la politique et spécifier la source pour le mappage.

1. Dans la colonne **Utilisateurs** , sélectionnez **plus**.
2. **Enregistrez les utilisateurs** pour les ajouter au groupe et sélectionnez la **Source d'enregistrement** pour les étiquettes et le mappage utilisateurs-vers-étiquette
   - **Local** (Default)—Enregistrez les étiquettes et le mappage pour les membres du groupe dynamique d'utilisateurs localement sur le pare-feu
   - **Agent User-ID Panorama** —Enregistre les étiquettes et les mappages pour les membres des groupes dynamiques d'utilisateurs sur un agent User-ID connecté à Panorama Si le groupe dynamique d'utilisateurs provient de Panorama, la ligne s'affiche en jaune et le nom du groupe, la description, les critères de correspondance et les étiquettes sont en lecture seule Cependant, vous pouvez toujours enregistrer ou désenregistrer des utilisateurs du groupe
   - **Agent User-ID Panorama** —Enregistre les étiquettes et les mappages pour les membres des groupes dynamiques d'utilisateurs sur un agent User-ID connecté à Panorama Pour sélectionner cette option, vous devez d'abord configurer un profil de serveur HTTP.
3. Sélectionnez les **Etiquettes** que vous souhaitez enregistrer sur la source en utilisant les étiquettes que vous avez utilisé pour configurer le groupe
4. (Facultatif) Pour retourner les membres du groupe dynamique d'utilisateurs à leurs groupes d'origine après une durée spécifique, entrez un **Délai d'expiration** en minutes (le défaut est 0, l'intervalle est 0-43200).
5. **Ajoutez** ou **Supprimez** les utilisateurs si nécessaire
6. (Optionnel) **Désenregistrer les utilisateurs** pour supprimer les étiquettes et les mappages utilisateurs-vers-étiquettes

**STEP 7 |** Vérifiez que le pare-feu remplit correctement les utilisateurs dans le groupe dynamique d'utilisateurs

1. Confirmez que la colonne **Groupe dynamique d'utilisateurs** dans les journaux de trafic, de menaces, de filtrage des URL, soumissions Wildfire, Filtrage des données et inspection des tunnels affichent les groupes dynamiques d'utilisateurs correctement
2. Utilisez la commande **`show user group list dynamic`** pour afficher une liste de tous les groupes dynamiques d'utilisateurs et également le nombre total de groupes d'utilisateurs dynamiques
3. Utilisez la commande **`show object registered-user all`** pour afficher la liste des utilisateurs enregistrés comme membres de groupes dynamiques d'utilisateurs
4. Utilisez la commande **`show user group name`** ***`group-name`*** pour afficher les informations à propos des groupes dynamiques d'utilisateurs, comme le type de la source

# Utilisation de l'auto-étiquetage pour automatiser les actions de sécurité

L'auto-étiquetage permet au pare-feu ou à Panorama d'étiqueter un objet de politique lorsqu'il reçoit un journal qui correspond à un critère spécifique et d'établir un mappage adresse IP-étiquette ou utilisateur-étiquette. Par exemple, lorsqu'un pare-feu génère un journal de menaces, vous pouvez configurer le pare-feu pour qu'il étiquette l'adresse IP source ou l'utilisateur source dans le journal des menaces avec un nom d'étiquette spécifique. Vous pouvez ensuite utiliser ces étiquettes pour automatiquement générer des objets de politique, comme des groupes d'utilisateurs dynamiques ou des groupes d'adresses dynamiques, qui peuvent ensuite servir à automatiser les actions de sécurité dans les politiques de sécurité, d'authentification ou de décryptage. Par exemple, lorsque vous créez un filtre pour les journaux URL logs for `yes` in the **Credential Detected** column, you can apply a tag to the user that enforces an authentication policy that requires user to authenticate using multi-factor authentication (MFA).

*Les groupes d'utilisateurs dynamiques ne prennent pas en charge le marquage automatique à partir des journaux HIP Match.*

Redistribuer le mappage au sein de votre réseau en enregistrant le mapping adresse IP-vers-étiquette et utilisateurs-vers-étiquette sur un agent User-ID intégré à PAN-OS sur le pare-feu ou sur un agent distant User-ID en utilisant un profil de serveur HTTP Le pare-feu peut automatiquement enlever (désenregistrer) une étiquette associée à une adresse IP ou à un utilisateur lorsque vous configurez un délai d'expiration dans une action pré-construite pour un profil de transfert des journaux ou dans les configurations de transfert des journaux Par exemple, si le pare-feu détecte qu'un utilisateur a potentiellement des identifiants compromis, vous pouvez configurer le pare-feu pour exiger une authentification MFA de l'utilisateur sur une période de temps donné, ensuite configurer un délai d'expiration pour retirer l'utilisateur du groupe d'exigence MFA

**STEP 1 |** En fonction du type de journaux que vous souhaitez utiliser pour l'étiquetage, créez un profil de transfert des journaux ou configure les configurations de journaux pour définir comment vous souhaitez que le pare-feu ou Panorama traite les journaux

- Pour les journaux d'authentification, de données, de trafic, d'inspection Tunnel, d'URLs et de Wildfire, créez un profil de transfert des journaux
- Pour les journaux User-ID, correspondance HIP, GlobalProtect et IP-étiquette, configurez les paramètres de journaux.

**STEP 2 |** Définissez le critère de correspondance qui déterminer quand le pare-feu ou Panorama ajoute l'étiquette à l'objet politique.

Par exemple, vous pouvez utiliser un filtre pour configurer un seuil ou définir une valeur (tel que **`user eq "unknown"`** pour identifier les utilisateurs que le pare-feu n'a pas encore mappé); quand le pare-feu atteint ce seuil ou trouve la valeur, le pare-feu ajoute l'étiquette

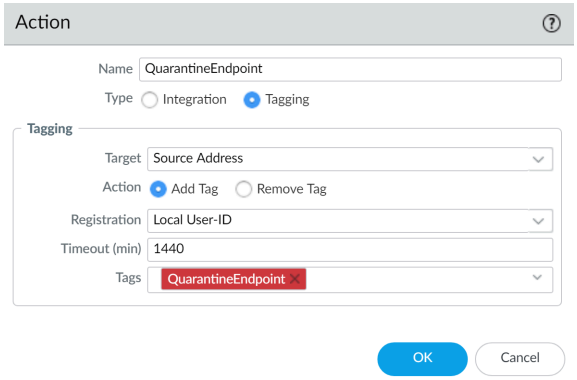
- Pour créer un profil de transfert des journaux, **Ajoutez** le et sélectionnez le **Type de journal** que vous voulez surveiller pour des critères de correspondance (**Objects** > **Log Forwarding**).
- Pour configurer les paramètres de journal, **Ajoutez** les paramètres de journaux pour le type de journal que vous souhaitez surveillez pour les critères de correspondance (**Device** > **Log Settings**).

**STEP 3 |** Copiez et coller une valeur de**Filtre** ou utilisez le **Constructeur de filtre** pour définir les critères de correspondance pour l'étiquette

**STEP 4 |** Ajoutez une action pré-construite pour étiqueter l'objet politique

1. **Ajoutez** les **actions pré-construites** que vous souhaitez que le pare-feu ou Panorama prenne quand les journaux contiennent une entrée qui correspond au critère de correspondance.
2. **Définissez** l'action :
3. Sélectionnez le type de **Cible** que vous souhaitez étiqueter (**Destination Address**, **Source Address**, **User**, or **X-Forwarded-For Address**).
4. Confirmez que **Ajoutez une étiquette** est l'**Action**.
5. Sélectionnez l'**Enregistrement** source pour l'étiquette pour déterminer comment le pare-feu ou Panorama redistribue le mappage Adresse IP-vers-étiquette
   - **User-ID local** -- Redistribuez le mappage Adresse IP-vers-étiquette sur l'agent User-ID sur le pare-feu ou Panorama
   - **User-ID Panorama** -- Redistribuez le mappage Adresse IP-vers-étiquette sur Panorama
   - **User-ID distant** -- Redistribuez le mappage Adresse IP-vers-étiquette sur un autre agent User-ID en utilisant le profil de serveur HTTP Si vous sélectionnez cette option, vous devez configurer un profil de serveur HTTP (voir Etape 5).
6. Entrez ou sélectionnez les **Etiquettes** que vous souhaitez ajouter à l'objet politique.
   Vous pouvez avoir besoin de cliquer en dehors du champ ou d'appuyer sur Entrée pour activer le bouton **OK**
7. Cliquez sur **OK**.



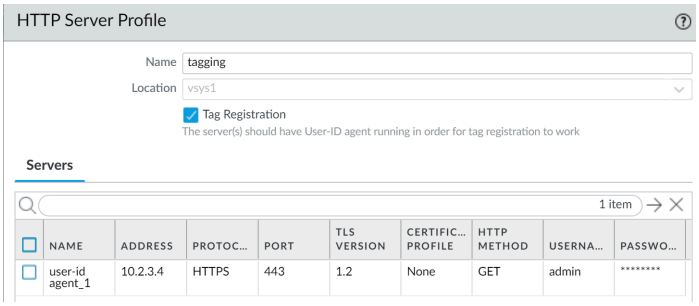

**STEP 5 |** (Remote User-ID distant seulement) Configurez un profil de serveur HTTP pour transférer les journaux vers un agent distant User-ID

1. Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveur)** > **Email (Messagerie)**.
2. Donnez un **Name (Nom)** au profil de serveur et sélectionnez un **Location (Emplacement)**.
3. (Pare-feu possédant des systèmes virtuels multiples uniquement) Sélectionnez le **Location (Emplacement)**. Le profil peut être **Shared (Partagé)** par tous les systèmes virtuels ou appartenir à un système virtuel donné.
4. Sélectionnez **Tag Registration (Enregistrement des étiquettes)** pour permettre au pare-feu d'enregistrer l'adresse IP et d'étiqueter le mappage avec l'agent User-ID qui se trouve

sur un pare-feu distant. Lorsque l'enregistrement des étiquettes est activé, vous ne pouvez préciser le format de la charge utile.

5. **Ajoutez** les détails de la connexion pour accéder à l'agent User-ID distant et cliquez **OK**.




6. Sélectionnez le profil de transfert des journaux que vous avez créé ensuite sélectionnez ce profil de serveur comme profil de serveur HTTP pour votre**Enregistrement Remote User-ID** tag

**STEP 6 |** Définissez les objets politique pour lesquels vous souhaitez appliquer les étiquettes

1. Créez ou sélectionner un des objets politique suivants: dynamic address groups, Utilisation de groupes d'utilisateurs dynamiques dans une politique, addresses, address groups, zones, policy rules, services, ou service groups.
2. Entrez les étiquettes que vous souhaitez appliquer à l'objet comme critères de **correspondance**

   Confirmez que l'étiquette est identique à l'étiquette à l'étape 4.

**STEP 7 |** Ajoutez les objets politique étiquetés à votre politique.

Cette procédure utilise une politique de sécurité comme un exemple, mais vous pouvez aussi utiliser des objet politique étiquetés dans la politique d'authentification

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
2. Cliquez sur **Add (Ajouter)** et saisissez un **Name (nom)** et une **Description (description)** pour identifier la politique.
3. **Zone source** : approuvée (d'où provient le trafic)
4. Ajoutez la **Destination Zone (Zone de destination)** dans laquelle se termine le trafic.
5. Sélectionnez l'objet **Source** vous avez crée à l'étape 5.1
6. Sélectionnez si la règle va **autoriser** ou **interdire** le trafic.

**STEP 8 |** Si vous configurez un profil de transfert des journaux, assignez-le à votre politique de sécurité

Vous pouvez assigner un seul profil de transfert des journaux pour chaque politique mais vous pouvez assigner plusieurs méthodes et actions par profil Pour un exemple, se référez à Utilisation de groupes d'adresses dynamiques dans une politique.

**STEP 9 |** **Commit (Validez)** vos modifications.

**STEP 10 |** {optionnel) Configurez un délai d'expiration pour supprimer l'étiquette de l'objet politique après que le temps spécifié soit écoulé

Spécifiez la durée (en minutes) qui s'écoule avant que le pare-feu supprime l'étiquette de l'objet politique. L'intervalle est entre 0 et 43200 Si vous fixez le délai d'expiration à 0, le mappage

Adresse IP-vers-étiquette n'expire pas et doit être supprimé avec une action explicite Si vous fixez le délai d'expiration à une valeur maximale de 43200 minutes, le pare-feu supprime l'étiquette après 30 jours

*Vous ne pouvez pas configurer un délai avec l'action **Remove Tag (Supprimer une étiquette)**.*

1. Sélectionnez un profil de Log Forwarding (Transfert des journaux).
2. **Ajoutez** ou éditez une des **Actions prédéfinis**.
3. Spécifiez le **Délai d'expiration** (en minutes). Quand le temps spécifié s'est écoulé, le pare-feu ou Panorama supprime l'étiquette

   *Vous devez définir le délai du mappage IP-étiquette sur la même durée de temps que le délai du bail DHCP d'une adresse IP. Le mappage IP-étiquette peut ainsi expirer en même temps que le bail DHCP, ce qui évite que vous appliquiez involontairement la politique lorsque l'adresse IP est réaffectée.*
4. Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.

# Surveillance des changements dans l'environnement virtuel

Afin de sécuriser les applications et prévenir les menaces dans un environnement où de nouveaux utilisateurs et serveurs ne cessent de voir le jour, votre politique de sécurité doit être souple. Pour cela, le pare-feu doit être capable d'apprendre les adresses IP nouvelles et modifiées, et d'appliquer systématiquement la politique sans aucune modification de configuration sur le pare-feu.

La coordination des fonctions **Sources d'informations de machine virtuelle** et **Groupes d'adresses dynamiques** sur le pare-feu permet d'utiliser cette fonctionnalité. Le pare-feu et Panorama permettent automatiquement de recueillir des informations sur l'inventaire de machines virtuelles (ou d'invités) sur chaque source surveillée et de créer des objets de politique qui restent synchronisés avec les modifications dynamiques sur le réseau.

- Activation de la surveillance des machines virtuelles pour suivre les modifications sur le réseau virtuel
- Attributs surveillés sur les machines virtuelles dans les plateformes en cloud
- Utilisation de groupes d'adresses dynamiques dans une politique

## Activation de la surveillance des machines virtuelles pour suivre les modifications sur le réseau virtuel

Les sources d'informations de machine virtuelle permettent automatiquement de recueillir des informations sur l'inventaire de machines virtuelles sur chaque source surveillée (hôte) ; le pare-feu peut surveiller les serveurs VMware ESXi, vCenter, AWS-VPC, Microsoft Azure VNet et Google Cloud. Lorsque des machines virtuelles (hôtes) sont déployées ou déplacées, le pare-feu collecte un ensemble prédéfini d'attributs (ou d'éléments de métadonnées), tels que les étiquettes ; ces étiquettes peuvent ensuite être utilisées pour définir des groupes d'adresses dynamiques (reportez-vous à la section Utilisation de groupes d'adresses dynamiques dans une politique) et mises en correspondance avec une politique.

Vous pouvez configurer directement le pare-feu ou utiliser des modèles Panorama pour surveiller un maximum de dix 10 sources d'information de machine virtuelle. Les **VM Information Sources (Sources d'informations de machine virtuelle)** facilitent la configuration et vous permettent de surveiller un ensemble prédéfini de 16 éléments de métadonnées ou d'attributs. Reportez-vous à la section Attributs surveillés sur les machines virtuelles dans les plateformes en cloud pour connaître la liste. Par défaut, le trafic entre le pare-feu et les sources surveillées utilise le port de gestion (MGT) sur le pare-feu.

- *Lors de la surveillance des serveurs ESXi qui font partie de la solution VM-Series édition NSX, utilisez des Groupes d'adresses dynamiques plutôt que d'utiliser des Sources d'informations de machine virtuelle pour en apprendre davantage sur les changements dans l'environnement virtuel. Pour la solution VM-Series édition NSX, le Gestionnaire NSX fournit à Panorama des informations sur le groupe de sécurité NSX auquel appartient une adresse IP. Les informations du Gestionnaire NSX fournit le contexte global permettant la définition des critères de correspondance dans un Groupe d'adresses dynamiques, car il utilise l'ID du profil de service en tant qu'attribut distinctif et vous permet de mettre en œuvre correctement la politique lorsque vous avez des adresses IP qui se chevauchent entre les différents groupes de sécurité NSX. Un maximum de 32 étiquettes (provenant d'un serveur vCenter et d'un Gestionnaire NSX) peuvent être enregistrées à une même adresse IP.*
- *Pour surveiller des machines virtuelles dans votre déploiement Azure, plutôt que d'utiliser les sources de surveillance VM, vous devez déployer le script de surveillance des machines virtuelles qui s'exécute sur une machine virtuelle au sein du cloud Azure public. Ce script collecte les informations de mappage adresse IP-étiquette de vos ressources Azure et les publie sur les pare-feu et les systèmes virtuels correspondants que vous spécifiez dans le script.*
- *Pour la version 8.1.3 de Panorama, ou toute version ultérieure, vous pouvez aussi utiliser le plugiciel Panorama pour AWS ou Azure pour récupérer les informations sur la machine virtuelle et l'enregistrer sur les pare-feu gérés. Reportez-vous à la section Attributs surveillés sur les machines virtuelles dans les plateformes en cloud pour obtenir plus de précisions.*

**STEP 1 |** Activez la surveillance des machines virtuelles.

*Vous pouvez configurer un maximum de dix sources d'informations de machine virtuelle pour chaque pare-feu, ou pour chaque système virtuel sur un pare-feu prenant en charge la fonction de systèmes virtuels multiples.*

Si vos pare-feu sont définis dans une configuration haute disponibilité :

- Dans une configuration active/passive, seul le pare-feu actif surveille les sources de machine virtuelle.
- Dans une configuration active/active, seul le pare-feu principal surveille les sources de machine virtuelle.

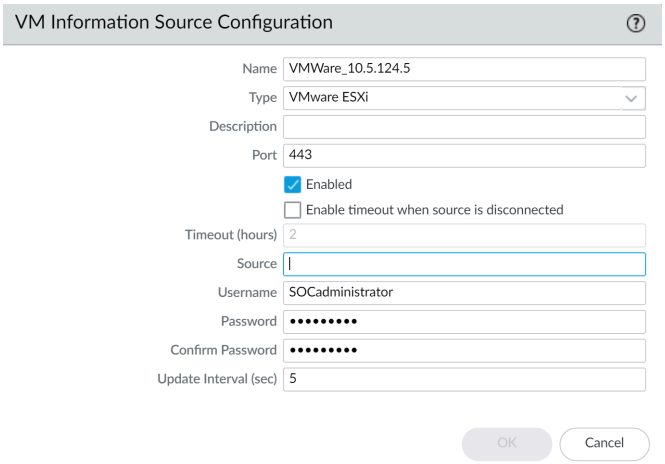
1. Sélectionnez **Device (Périphérique)** > **VM Information Sources (Sources d'informations de machine virtuelle)**. Cet exemple vous montre comment ajouter VMware ESX(i) ou le serveur vCenter.
2. Cliquez sur **Add (Ajouter)** et saisissez les informations suivantes :
   - Un **Name (Nom)** pour identifier la source que vous souhaitez surveiller.
   - Sélectionnez le **Type (Type)** pour indiquer si la source est un **AWS VPC**, une instance de **Google Compute Engine**, un serveur **VMware ESX(i)** ou un serveur **VMware vCenter**.

     *Le type choisi détermine les champs qui s'affichent.*

   - Saisissez le **Port** d'écoute de la source.

- Pour modifier la valeur par défaut, cochez la case **Enable timeout when the source is disconnected (Activer le délai d'expiration lorsque la source est déconnectée)** et indiquez une valeur. Lorsque la limite définie est atteinte ou si l'hôte n'est pas accessible ou ne répond pas, le pare-feu ferme la connexion à la source.
- Ajoutez les informations d'identification (**Username (Nom d'utilisateur)** et **Password (Mot de passe)**) pour l'authentification auprès du serveur indiqué ci-dessus.
- Définissez la **Source** : nom d'hôte ou adresse IP.
- (Facultatif) Modifiez l'**Update interval (Intervalle de mise à jour)** sur une valeur entre 5 et 600 secondes. Par défaut, le pare-feu effectue des recherches toutes les 5 secondes. Les appels API sont mis en file d'attente et récupérés toutes les 60 secondes. Par conséquent, les mises à jour peuvent prendre 60 secondes plus l'intervalle d'interrogation donné.




- Cliquez sur **OK** et sur **Commit (Valider)** pour enregistrer les modifications.
- Vérifiez que le **Status (État)** de connexion affiché est Connecté.

**STEP 2 |** Vérifiez l'état de la connexion.

Vérifiez que le **Status (État)** de connexion affiché est Connecté.


Si l'état de connexion est Pending (En attente) ou Disconnected (Déconnecté), vérifiez que la source est opérationnelle et que le pare-feu peut accéder à la source. Si vous utilisez un autre port que le port MGT pour la communication avec la source surveillée, vous devez modifier l'itinéraire de service (dans **Device (Périphérique)** > **Setup (Configuration)** > **Services (Services)**, cliquez sur le lien **Service Route Configuration (Configuration de l'itinéraire de service)** et modifiez la **Source Interface (Interface source)** du service **VM Monitor (Surveillance des machines virtuelles)**).

# Attributs surveillés sur les machines virtuelles dans les plateformes en cloud

Lors de la configuration ou de la suppression de machines virtuelles dans le cloud public ou privé, vous pouvez utiliser un plugin Panorama, un script de surveillance de machine virtuelle ou la source d'informations de machine virtuelle sur le pare-feu de prochaine génération pour surveiller les changements apportés aux machines virtuelles déployées dans les environnement virtuels.

**Sources d'informations de machine virtuelle** : sur un pare-feu matériel ou VM-Series, vous pouvez surveiller les instances de machine virtuelle et récupérer les modifications lorsque vous configurez ou modifiez les invités configurés sur les sources surveillées (AWS, ESXi ou vCenter Server ou AWS). Pour chaque pare-feu (et/ou système virtuel si votre pare-feu dispose de plusieurs fonctionnalités système), vous pouvez configurer un maximum de dix sources. Pour obtenir plus d'informations sur le fonctionnement synchrone des sources d'informations de machine virtuelle et des groupes d'adresses dynamiques travaillent de façon synchrone et surveiller les changements apportés à l'environnement virtuel, reportez-vous au Guide de déploiement de VM-Series .Si vos pare-feu sont configurés dans une configuration haute disponibilité :

- Dans une configuration active/passive, seul le pare-feu actif surveille les sources d'informations de machine virtuelle.
- Dans une configuration active/active, seul le pare-feu principal surveille les sources d'informations de machine virtuelle.

**Plugiciel Panorama** : Sur un appareil Panorama matériel ou virtuel exécutant la version 8.1.3, vous pouvez installer le plug-in pour Microsoft Azure et AWS. Le plugiciel vous permet de vous connecter à vos abonnements au cloud public d'Azure ou aux VPC AWS et de récupérer le mappage adresse IP-étiquette de vos machines virtuelles. Panorama enregistre ensuite les informations de la machine virtuelle sur les pare-feu Palo Alto Networks® que vous avez configurés pour la notification.

Utilisez les sections suivantes pour examiner les options prises en charge sur chaque fournisseur de cloud et les attributs des machines virtuelles que vous pouvez surveiller pour créer des groupes d'adresses dynamiques :

- VMware ESXi
- Amazon Web Services (AWS)
- Microsoft Azure
- Google

## VMware ESXi

VMware Tools doit être installé et exécuté sur chaque machine virtuelle se trouvant sur un serveur ESXi ou vCenter surveillé. VMware Tools permet de récupérer les adresses IP et d'autres valeurs affectées à chaque machine virtuelle.

*Lors de la surveillance des serveurs ESXi qui font partie de la solution VM-Series édition NSX, utilisez des Groupes d'adresses dynamiques plutôt que d'utiliser des Sources d'informations de machine virtuelle pour en apprendre davantage sur les changements dans l'environnement virtuel. Pour la solution VM-Series édition NSX, le Gestionnaire NSX fournit à Panorama des informations sur le groupe de sécurité NSX auquel appartient une adresse IP. Les informations du Gestionnaire NSX fournit le contexte global permettant la définition des critères de correspondance dans un Groupe d'adresses dynamiques, car il utilise l'ID du profil de service en tant qu'attribut distinctif et vous permet de mettre en œuvre correctement la politique lorsque vous avez des adresses IP qui se chevauchent entre les différents groupes de sécurité NSX.*

*Un maximum de 32 étiquettes (provenant d'un serveur vCenter et d'un Gestionnaire NSX) peuvent être enregistrées à une même adresse IP.*

Afin de collecter les valeurs affectées aux machines virtuelles surveillées, utilisez les sources d'informations de machine virtuelle sur le pare-feu pour surveiller l'ensemble prédéfini d'attributs ESXi suivant :

| Attributs surveillés sur une source VMware |
|---|
| UUID |
| Name (Nom) |
| Système d'exploitation invité |
| État de la machine virtuelle (l'état d'alimentation peut être Mis sous tension, Mis hors tension, En veille et Inconnu). |
| Annotation |
| Version |
| Réseau (Nom du commutateur virtuel, Nom du groupe de ports et ID de VLAN) |
| Nom du conteneur (Nom vCenter, Nom de l'objet de centre de données, Nom du pool de ressources, Nom du cluster, Hôte et Adresse IP de l'hôte) |

## Amazon Web Services (AWS)

Lors de la configuration ou de la modification des machines virtuelles sur vos VPC AWS, deux façons s'offrent à vous de surveiller ces instances et de récupérer les étiquettes à utiliser comme critères de comparaison dans des groupes d'adresses dynamiques.

- **Source d'informations de machine virtuelle** : Sur un pare-feu de prochaine génération, vous pouvez surveiller un maximum de 32 étiquettes, soit 14 étiquettes prédéfinies et 18 paires clé-valeur (étiquettes). Les attributs (ou noms d'étiquettes) suivants peuvent être utilisés comme critères de correspondance pour les groupes d'adresses dynamiques.
- **Plug-in AWS sur Panorama** : le plug-in Panorama pour AWS vous permet de connecter Panorama à vos VPC AWS et de récupérer le mappage d'adresse IP vers étiquette pour vos

machines virtuelles AWS. Panorama enregistre ensuite les informations de la machine virtuelle sur les pare-feu Palo Alto Networks® que vous avez configurés pour la notification. Grâce au plugin, Panorama peut récupérer un total de 32 étiquettes pour chaque machine virtuelle, soit 11 étiquettes prédéfinies et un maximum de 21 étiquettes définies par l'utilisateur.

| Attributs surveillés sur AWS-VPC | Source d'informations de machine virtuelle sur le pare-feu | Plugin AWS sur Panorama |
|---|---|---|
| Architecture | Oui | Non |
| Système d'exploitation invité | Oui | Non |
| ID AMI | Oui | Oui |
| Profil de l'instance IAM | Non | Oui |
| ID d'instance | Oui | Non |
| État de l'instance | Oui | Non |
| Type d'instance | Oui | Non |
| Nom de la clé | Oui | Oui |
| ID propriétaire | Non | Oui |
| Emplacement - Location | Oui | Oui |
| Emplacement - Nom du groupe | Oui | Oui |
| Emplacement - Zone de disponibilité | Oui | Oui |
| Nom DNS privé | Oui | Non |
| Nom DNS public | Oui | Oui |
| ID de sous-réseau | Oui | Oui |
| ID du groupe de sécurité | Non | Oui |
| Nom du groupe de sécurité | Non | Oui |

| Attributs surveillés sur AWS-VPC | Source d'informations de machine virtuelle sur le pare-feu | Plugin AWS sur Panorama |
|---|---|---|
| ID de VPC | Oui | Oui |
| Étiquette (clé, valeur) | Oui;<br>Un maximum de 18 étiquettes définies par l'utilisateur sont prises en charge. Les étiquettes définies par l'utilisateur sont triées par ordre alphabétique, et les 18 premières étiquettes peuvent être utilisées sur les pare-feu. | Oui;<br>Un maximum de 21 étiquettes définies par l'utilisateur sont prises en charge. Les étiquettes définies par l'utilisateur sont triées par ordre alphabétique, et les 21 premières étiquettes peuvent être utilisées sur les pare-feu. |

## Microsoft Azure

Pour la surveillance de machine virtuelle sur Azure, vous devez récupérer le mappage adresse IP-étiquette de vos VM Azure et le rendre disponible à titre de critères de mise en correspondance dans des groupes d'adresses dynamiques. Le plugin Panorama pour Microsoft Azure vous permet de connecter Panorama à vos souscriptions au nuage public Azure et de récupérer le mappage d'adresse IP à étiquette pour vos machines virtuelles Azure. Panorama peut récupérer un total de 26 étiquettes pour chaque machine virtuelle, 11 étiquettes prédéfinies et jusqu'à 15 étiquettes définies par l'utilisateur et enregistre les informations de la VM aux pare-feu Palo Alto Networks gérés que vous avez configurés à des fins de notification.

Avec le plugin Panorama pour Azure, vous pouvez surveiller l'ensemble d'attributs de machine virtuelle suivants dans votre déploiement Microsoft Azure.

| Attributs surveillés sur Microsoft Azure | Plugin Azure sur Panorama |
|---|---|
| Nom de la machine virtuelle | Oui |
| Taille de la machine virtuelle | Non |
| Network Security Group Name (Nom du groupe de sécurité réseau) | Oui |
| Type de système d'exploitation | Oui |
| Éditeur du système d'exploitation | Oui |
| Offre de système d'exploitation | Oui |
| SKU du système d'exploitation | Oui |
| Sous-réseau | Oui |

| Attributs surveillés sur Microsoft Azure | Plugin Azure sur Panorama |
|---|---|
| VNet (Réseau virtuel) | Oui |
| Région Azure | Oui |
| Nom du groupe de ressources | Oui |
| ID d'abonnement | Oui |
| Étiquettes définies par l'utilisateur | Oui<br>Un maximum de 15 étiquettes définies par l'utilisateur sont prises en charge. Les étiquettes définies par l'utilisateur sont triées par ordre alphabétique, et les 15 premières étiquettes peuvent être utilisées sur les pare-feu. |

### Google

L'utilisation de sources d'informations de machine virtuelle sur le pare-feu de nouvelle génération vous permet de surveiller l'ensemble d'attributs Google Compute Engine (GCE) prédéfinis suivant.

*Le haute disponibilité n'est pas prise en charge sur les pare-feu.*

| Attributs surveillés sur Google Compute Engine (CGE) |
|---|
| Nom d'hôte de la machine virtuelle |
| Type de machine |
| Numéro du projet |
| Source (Type de système d'exploitation) |
| Status (État) |
| Sous-réseau |
| Réseau VPC |

## Utilisation de groupes d'adresses dynamiques dans une politique

Les groupes d'adresses dynamiques peuvent être utilisés dans une politique. Ils vous permettent de créer une politique qui s'adapte automatiquement aux modifications (ajouts, déplacements

ou suppressions de serveurs). Les groupes d'adresses dynamiques vous permettent également d'appliquer différentes règles à un même serveur en fonction des ***étiquettes*** qui définissent son rôle sur le réseau, le système d'exploitation ou les différents types de trafic traités.

Un groupe d'adresses dynamiques utilise les étiquettes comme critères de filtrage pour déterminer ses membres. Le filtre utilise les opérateurs logiques ***et*** et ***ou***. Toutes les adresses IP ou tous les groupes d'adresses IP qui correspondent aux critères de filtrage deviennent membres du groupe d'adresses dynamiques. Les étiquettes peuvent être définies de manière statique et/ou enregistrées (de manière dynamique) sur le pare-feu. La différence entre les étiquettes statiques et dynamiques est que les étiquettes statiques font partie de la configuration du pare-feu, tandis que les étiquettes dynamiques font partie de la configuration d'exécution. Une validation n'est ainsi pas nécessaire pour mettre à jour les étiquettes dynamiques ; les étiquettes doivent toutefois être utilisées par les groupes d'adresses dynamiques référencés dans la politique, et la politique doit être validée sur le pare-feu.

Pour enregistrer les étiquettes de manière dynamique, vous pouvez utiliser l'API XML ou l'agent de surveillance des machines virtuelles sur le pare-feu, ou encore l'agent User-ID. Chaque étiquette est un élément de métadonnée ou une paire attribut/valeur enregistré(e) sur le pare-feu ou Panorama, par exemple, IP1 {étiquette1, étiquette2 ... étiquette32}, où l'adresse IP et les étiquettes associées sont conservées dans une liste. Chaque adresse IP enregistrée peut disposer de 32 étiquettes identifiant notamment le système d'exploitation, le centre de données ou le commutateur virtuel auquel elle appartient. Après avoir reçu l'appel API, le pare-feu enregistre l'adresse IP et les étiquettes associées, et met automatiquement à jour les informations d'appartenance aux groupes pour le(s) groupe(s) d'adresses dynamiques.

Le nombre maximum d'adresses IP qui peuvent être enregistrées est différent pour chaque modèle. Utilisez le tableau suivant pour connaître les spécifications relatives à votre modèle :

| Modèle | Nombre maximum d'adresses IP enregistrées de manière dynamique |
|---|---|
| Appareils M-Series et appareils virtuels Panorama | 500 000 |
| PA-5200 Series, VM-7000 SMC-B Series | 500 000 |
| VM-500, VM-700 | 300 000 |
| PA-3200 Series, VM-300 | 200 000 |
| PA-7000 Series | 100 000 |
| PA-850, VM-100 | 2 500 |
| PA-820, PA-220, VM-50 | 1 000 |

*Un ensemble d'adresses IP, tel qu'une plage ou un sous-réseau d'adresses IP, est considéré comme une seule adresse IP enregistrée lorsqu'il est compté dans le nombre maximum d'adresses IP enregistrées prises en charge par chaque modèle de pare-feu.*

L'exemple suivant indique comment les groupes d'adresses dynamiques peuvent simplifier l'application de la sécurité réseau. L'exemple de flux de travail suivant indique comment :

- Activer l'agent de surveillances des machines virtuelles sur le pare-feu pour surveiller l'hôte VMware ESX(i) ou le serveur vCenter et enregistrer les adresses IP des machines virtuelles et les étiquettes associées.
- Créer des groupes d'adresses dynamiques et définir les étiquettes à filtrer. Dans cet exemple, deux groupes d'adresses sont créés : un qui filtre uniquement les étiquettes dynamiques et un autre qui filtre les étiquettes statiques et dynamiques pour renseigner les membres du groupe.
- Assurez-vous que les membres du groupe d'adresses dynamiques sont renseignés sur le pare-feu.
- Utilisez des groupes d'adresses dynamiques dans une politique. Cet exemple utilise deux politiques de sécurité différentes :
  - Une politique de sécurité pour tous les serveurs Linux déployés comme serveurs FTP ; cette règle correspond aux étiquettes enregistrées de manière dynamique.
  - Une politique de sécurité pour tous les serveurs Linux déployés comme serveurs Web ; cette règle correspond à un groupe d'adresses dynamiques qui utilise des étiquettes statiques et dynamiques.
- Assurez-vous que les membres du groupe d'adresses dynamiques sont mis à jour lorsque de nouveaux serveurs FTP ou Web sont déployés. Ainsi, les règles de sécurité sont également appliquées sur ces nouvelles machines virtuelles.

**STEP 1 |** Activez la surveillance des sources de machine virtuelle.

Consultez Activation de la surveillance des machines virtuelles pour suivre les modifications sur le réseau virtuel.

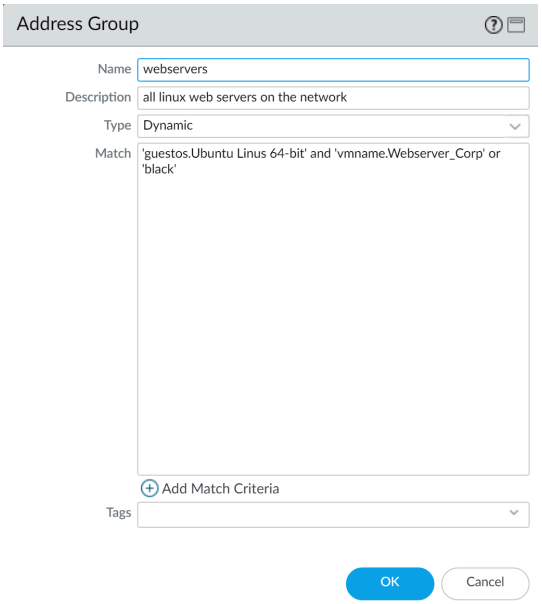
**STEP 2 |** Créez des groupes d'adresses dynamiques sur le pare-feu.

***Consultez le** didacticiel **pour avoir une vue d'ensemble de la fonction.***

1. Connectez-vous à l'interface Web du pare-feu.
2. Sélectionnez **Object (Objet)** > **Address Groups (Groupe d'adresses)**.
3. Cliquez sur **Add (Ajouter)** et saisissez un **Name (nom)** et une **Description (description)** pour identifier le groupe d'adresses.
4. Définissez le **Type (type)** sur **Dynamic (Dynamique)**.
5. Définissez les critères de correspondance. Vous pouvez sélectionner des étiquettes dynamiques et statiques comme critères de correspondance pour renseigner les membres du groupe. Cliquez sur **Add Match Criteria (Ajouter un critère de correspondance)**

et sélectionnez l'opérateur **And (Et)** ou **Or (Ou)**, puis choisissez les attributs que vous souhaitez filtrer ou mettre en correspondance et cliquez sur **OK (OK)**.




6. Cliquez sur **Commit (Valider)**.

**STEP 3 |** Les critères de correspondance pour chaque groupe d'adresses dynamiques dans cet exemple sont les suivants :

ftp_servers : correspond au système d'exploitation invité « Linux 64-bit » et annoté « ftp » (« guestos.Ubuntu Linux 64-bit » et « annotation.ftp »).

web-servers : correspond à deux critères : si le système d'exploitation invité est « Linux 64-bit » et le nom du serveur est « Web_server_Corp » ou l'étiquette « black », (« guestos.Ubuntu Linux 64-bit » et « vmname.WebServer_Corp » ou « black »).

**STEP 4 |** Utilisez des groupes d'adresses dynamiques dans une politique.

*Consultez le didacticiel.*

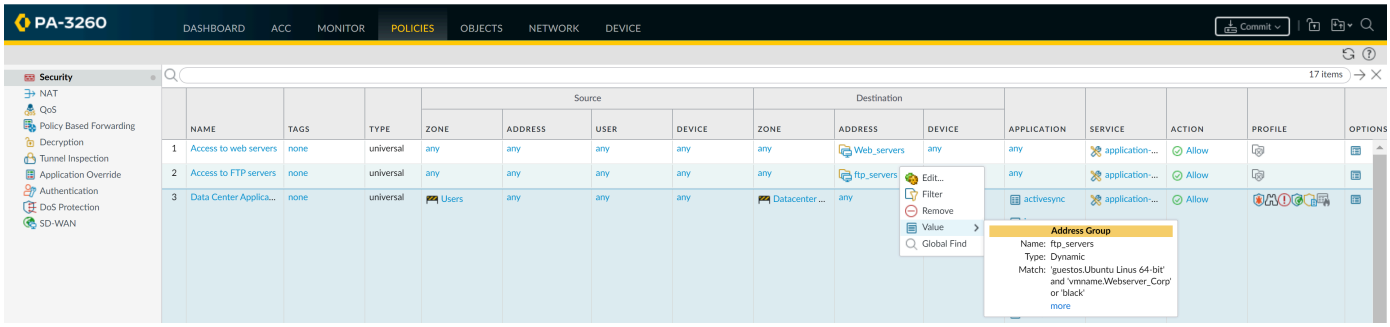
1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
2. Cliquez sur **Add (Ajouter)** et saisissez un **Name (nom)** et une **Description (description)** pour identifier la politique.
3. Ajoutez la **Source Zone (Zone source)** pour indiquer la zone d'où provient le trafic.
4. Ajoutez la **Destination Zone (Zone de destination)** dans laquelle se termine le trafic.
5. Pour **Destination Address (Adresse de destination)**, sélectionnez le groupe d'adresses dynamiques que vous venez de créer.
6. Indiquez l'action (**Allow (Autoriser)** ou **Deny (Refuser)**) pour le trafic, puis associez éventuellement les profils de sécurité par défaut à la règle.
7. Répétez les étapes 1 à 6 pour créer une autre règle de politique.
8. Cliquez sur **Commit (Valider)**.

**STEP 5 |** Cet exemple indique comment créer deux politiques : l'une pour l'accès aux serveurs FTP et l'autre pour l'accès aux serveurs Web.

| | NAME | TAGS | TYPE | Source ZONE | Source ADDRESS | Source USER | Source DEVICE | Destination ZONE | Destination ADDRESS | Destination DEVICE | APPLICATION | SERVICE | ACTION | PROFILE | OPTI |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Access to web servers | none | universal | any | any | any | any | any | Web_servers | any | any | application-... | Allow | | |
| 2 | Access to FTP servers | none | universal | any | any | any | any | any | ftp_servers | any | any | application-... | Allow | | |

**STEP 6 |** Assurez-vous que les membres du groupe d'adresses dynamiques sont renseignés sur le pare-feu.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis choisissez la règle.
2. Cliquez sur la flèche déroulante en regard du lien du groupe d'adresses et sélectionnez **Value (Valeur)**. Vous pouvez également vérifier que les critères de correspondance sont corrects.




3. Cliquez sur le lien **more (Plus)** et vérifiez que la liste des adresses IP enregistrées s'affiche.

   La politique est appliquée à toutes les adresses IP qui appartiennent à ce groupe d'adresses et s'affichent ici.

*Si vous souhaitez supprimer toutes les adresses IP enregistrées, utilisez la commande CLI* ***debug object registered-ip clear all****, puis redémarrez le pare-feu après avoir effacé les étiquettes.*

# Commandes CLI pour les adresses IP dynamiques et les étiquettes

L'interface de ligne de commande sur le pare-feu et Panorama vous donne une vue détaillée des différentes sources à partir desquelles les étiquettes et les adresses IP ont été enregistrées de manière dynamique. Celle-ci vous permet également de contrôler les étiquettes enregistrées et non enregistrées. Les exemples suivants illustrent les fonctionnalités de la CLI.

| Exemple | Commande de la CLI |
|---|---|
| Afficher toutes les adresses IP enregistrées qui correspondent à l'étiquette `state.poweredOn` ou qui ne sont pas identifiées comme `vSwitch0`. | **`show log iptag tag_name equal state.poweredOn`**<br>**`show log iptag tag_name not-equal switch.vSwitch0`** |
| Afficher toutes les adresses IP enregistrées de manière dynamique qui proviennent de la source d'informations de machine virtuelle `vmware1` et qui ont été identifiées comme `poweredOn`. | **`show vm-monitor source source-name vmware1 tag state.poweredOn registered-ip all`**<br>`registered IP Tags`<br>`---------- ----------`<br>`fe80::20c:29ff:fe69:2f76 "state.poweredOn"`<br>`10.1.22.100 "state.poweredOn"`<br>`2001:1890:12f2:11:20c:29ff:fe69:2f76" state.poweredOn"`<br>`fe80::20c:29ff:fe69:2f80 "state.poweredOn"`<br>`192.168.1.102 "state.poweredOn"`<br>`10.1.22.105 "state.poweredOn"`<br>`2001:1890:12f2:11:2cf8:77a9:5435:c0d" state.poweredOn"`<br>`fe80::2cf8:77a9:5435:c0d "state.poweredOn"` |
| Effacer toutes les adresses IP et les étiquettes apprises d'une certaine source de surveillance des machines virtuelles sans déconnecter la source | **`debug vm-monitor clear source-name <name>`** |
| Afficher les adresses IP enregistrées à partir de toutes les sources | **`show object registered-ip all`** |

| Exemple | Commande de la CLI |
| --- | --- |
| Afficher le nombre d'adresses IP enregistrées à partir de toutes les sources | **show object registered-ip all option count** |
| Effacer les adresses IP enregistrées à partir de toutes les sources | **debug object registered-ip clear all** |
| Ajouter ou supprimer des étiquettes pour une adresse IP donnée qui a été enregistrée à l'aide de l'API XML | **debug object registered-ip test [<register/unregister>] <ip/netmask><tag>** |
| Afficher toutes les étiquettes enregistrées à partir d'une certaine source d'informations | **show vm-monitor source source-name vmware1 tag all**<br>vlanId.4095<br>vswitch.vSwitch1<br>host-ip.10.1.5.22<br>portgroup.TOBEUSED<br>hostname.panserver22<br>portgroup.VM Network 2<br>datacenter.ha-datacenter<br>vlanId.0<br>state.poweredOn<br>vswitch.vSwitch0<br>vmname.Ubuntu22-100<br>vmname.win2k8-22-105<br>resource-pool.Resources<br>vswitch.vSwitch2<br>guestos.Ubuntu Linux 32-bit<br>guestos.Microsoft Windows Server 2008 32-bit<br>annotation.<br>version.vmx-08<br>portgroup.VM Network<br>vm-info-source.vmware1<br>uuid.564d362c-11cd-b27f-271f-c361604dfad7<br>uuid.564dd337-677a-eb8d-47db-293bd6692f76<br>Total: 22 |
| Afficher toutes les étiquettes enregistrées à partir d'une certaine source de données, par exemple, à partir de l'agent de surveillance des machines virtuelles sur le pare-feu, de l'API XML, de l'agent User-ID Windows ou de la CLI | • Pour afficher les étiquettes enregistrées à partir de la CLI :<br>**show log iptag datasource_type equal unknown** |

| Exemple | Commande de la CLI |
| --- | --- |
| | • Pour afficher les étiquettes enregistrées à partir de l'API XML :<br>`show log iptag datasource_type equal xml-api`<br>• Pour afficher les étiquettes enregistrées à partir de sources d'informations de machine virtuelle :<br>`show log iptag datasource_type equal vm-monitor`<br>• Pour afficher les étiquettes enregistrées à partir de l'agent User-ID Windows :<br>`show log iptag datasource_type equal xml-api datasource_subtype equal user-id-agent` |
| Afficher toutes les étiquettes enregistrées pour une certaine adresse IP (à partir de toutes les sources) | `debug object registered-ip show tag-source ip ip_address tag all` |

# Application de la politique sur les terminaux et les utilisateurs derrière un périphérique en amont

Si vous disposez d'un périphérique en amont, tel qu'un serveur proxy explicite ou un équilibreur de charge, déployé entre les utilisateurs de votre réseau et le pare-feu, ce dernier peut voir l'adresse IP du périphérique en amont comme l'adresse IP source dans le trafic HTTP/HTTPS que le proxy transmet plutôt que l'adresse IP du client qui a demandé le contenu. Dans de nombreux cas, le périphérique en amont ajoute un en-tête X-Forwarded-For (XFF) aux requêtes HTTP qui incluent l'adresse IPv4 ou IPv6 réelle du client qui a demandé le contenu ou de qui provient la requête.

Dans ces cas, vous pouvez configurer le pare-feu pour extraire l'adresse IP du champ XFF et la faire correspondre à un utilisateur avec son User-ID ou appliquer une politique de sécurité basée sur l'adresse IP.

- **Use X-Forwarded-For Header in User-ID (Utiliser l'en-tête X-Forwarded-For dans User-ID)** : ceci vous permet d'appliquer la politique basée sur les utilisateurs afin d'autoriser vos utilisateurs derrière un serveur proxy à accéder en toute sécurité aux applications Web. De plus, si User-ID arrive à mapper l'adresse IP XFF à un nom d'utilisateur, le pare-feu affiche ce nom d'utilisateur en tant qu'utilisateur source dans les journaux du trafic, des menaces, des envois WildFire et de filtrage des URL afin de vous procurer une visibilité de l'activité Web des utilisateurs derrière le proxy.
- **Use X-Forwarded-For Header in Security Policy (Utilisez l'en-tête X-Forwarded-For dans la politique de sécurité)** : ceci vous permet d'appliquer une politique de sécurité basée sur l'adresse IP source en utilisant l'adresse IP dans le champ XFF de l'en-tête HTTP. En outre, lorsque la politique est appliquée à un trafic qui inclut une adresse IP dans le champ XFF, vous pouvez configurer les journaux de trafic, de menaces, de filtrage des données et de soumission des feux de forêt pour faciliter le dépannage et les mesures correctives.

Pour veiller à ce que les pirates ne puissent lire ni exploiter les valeurs XFF contenues dans les paquets de requêtes Web qui sortent du pare-feu pour récupérer le contenu d'un serveur externe, vous pouvez également configurer le pare-feu pour qu'il extraie les valeurs XFF des paquets sortants. L'utilisation de l'adresse IP XFF pour l'ID utilisateur ou dans la politique et la suppression de la valeur XFF ne sont pas mutuellement exclusives : si vous configurez les deux, le pare-feu supprime les valeurs XFF uniquement après les avoir utilisées dans l'application de la politique et la journalisation.

***Vous ne pouvez pas configurer le pare-feu pour utiliser simultanément l'adresse IP dans le champ XFF de l'ID utilisateur et la politique de sécurité.***

- Utilisation des valeurs XFF pour les politiques et les utilisateurs sources de journalisation
- Utilisation des valeurs d'adresse IP XFF dans la politique de sécurité et la journalisation
- Utiliser l'adresse IP dans l'en-tête XFF pour dépanner des événements

## Utiliser les valeurs XFF pour les politiques basées sur les utilisateurs source

Vous pouvez configurer le pare-feu pour qu'il fasse correspondre l'adresse IP qui se trouve dans l'en-tête XFF à un nom d'utilisateur au moyen d'User-ID. Cela vous procurera une visibilité du trafic Web des utilisateurs derrière un serveur proxy qui, autrement, ne peuvent être identifiés de même qu'un

contrôle des politiques basées sur les utilisateurs. Afin de mapper les adresses IP des en-têtes XFF aux noms d'utilisateurs, vous devez d'abord procéder à l'Activation de User-ID.

Lorsque cette option est activée, le pare-feu utilise l'adresse IP de l'en-tête XFF à des fins de mappage d'utilisateur uniquement. L'adresse IP source que le pare-feu consigne est toujours celle du serveur proxy, et non celle de l'utilisateur source. Lorsque vous voyez un événement de journal attribué à un utilisateur que le pare-feu a mappé et une adresse IP extraite d'un en-tête XFF, il peut être difficile de repérer le périphérique associé à l'événement. Pour simplifier le débogage et le dépannage des événements attribués à des utilisateurs derrière le serveur proxy, vous devez également configurer le pare-feu pour qu'il renseigne la colonne X-Forwarded-For du journal de filtrage des URL en y indiquant l'adresse IP qui se trouve dans l'en-tête XFF afin que vous puissiez repérer le périphérique et l'utilisateur associés à un événement du journal qui corrélés à l'entrée du journal de filtrage des URL.

L'en-tête XFF que votre serveur proxy ajoute doit contenir l'adresse IP source de l'utilisateur final qui a lancé la requête. Si l'en-tête comporte plusieurs adresses IP, le pare-feu utilise la première adresse IP uniquement. Si l'en-tête contient des informations autres que l'adresse IP, le pare-feu ne parviendra pas à effectuer le mappage d'utilisateur.

*En activant l'option permettant aux pare-feu d'utiliser les en-têtes X-Forwarded-For pour procéder au mappage d'utilisateur, vous ne permettez pas au pare-feu d'utiliser l'adresse IP client de l'en-tête XFF en tant qu'adresse source dans les journaux ; les journaux continuent d'afficher l'adresse IP du serveur proxy en tant qu'adresse source. Cependant, pour simplifier le processus de débogage et de dépannage, vous pouvez configurer le pare-feu pour qu'il procède à l'*Ajout de valeurs XFF aux journaux de filtrage des URL *afin que l'adresse IP du client qui figure dans l'en-tête XFF s'affiche dans les journaux de filtrage des URL.*

**STEP 1 |** Autorisez le pare-feu à utiliser les valeurs XFF dans les politiques et dans les champs Utilisateur source des journaux.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Content-ID (Content-ID)** et modifiez les paramètres d'en-tête X-Forwarded-For.
2. Sélectionnez **Use X-Forwarded-For Header in User-ID (Utiliser l'en-tête X-Forwarded-For dans User-ID)**.

**STEP 2 |** Supprimez les valeurs XFF des demandes Web sortantes.

1. Sélectionnez **Strip X-Forwarded-For Header (Enlever l'en-tête X-Forwarded-For)**.
2. Cliquez sur **OK**, puis sur **Commit (Valider)**.

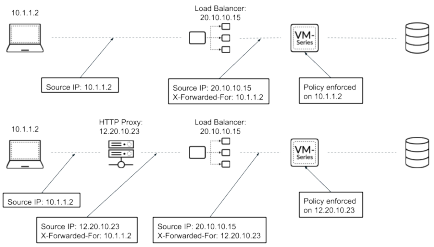
**STEP 3 |** Vérifiez que le pare-feu renseigne les champs Utilisateur source des journaux.

1. Sélectionnez un type de journal qui dispose d'un champ Utilisateur source (par exemple, **Monitor (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)**).
2. Vérifiez que la colonne Utilisateur source affiche les noms d'utilisateur des utilisateurs qui accèdent aux applications Web.

# Utilisation des valeurs d'adresse IP XFF dans la politique de sécurité et la journalisation

Vous pouvez configurer le pare-feu de manière à utiliser l'adresse IP dans le champ X-Forwarded-For (XFF) de l'en-tête HTTP pour appliquer la politique de sécurité. Si le paquet passe par un seul serveur proxy avant d'atteindre le pare-feu, le champ XFF contient l'adresse IP du terminal d'origine et le pare-feu peut utiliser cette adresse IP pour appliquer la politique de sécurité. Toutefois, si le paquet passe par plusieurs périphériques en amont, le pare-feu utilise l'adresse IP la plus récemment ajoutée pour appliquer la politique ou utiliser d'autres fonctionnalités qui reposent sur les informations IP.




- Utiliser les valeurs XFF dans la politique
- Afficher les valeurs XFF dans les journaux
- Afficher les valeurs XFF dans les rapports

## Utiliser les valeurs XFF dans la politique

Suivez la procédure suivante pour utiliser l'adresse IP du client dans l'en-tête XFF lors de l'application de la politique de sécurité.

*Dans Microsoft Azure, par défaut, une passerelle d'application insère l'adresse IP source et le port d'origine dans l'en-tête XFF. Pour utiliser les en-têtes XFF dans la politique de votre pare-feu, vous devez configurer la passerelle d'application de manière à omettre le port de l'en-tête XFF. Pour plus d'informations, consultez la* documentation relative à Azure*.*

**STEP 1 |** Connectez-vous à votre pare-feu.

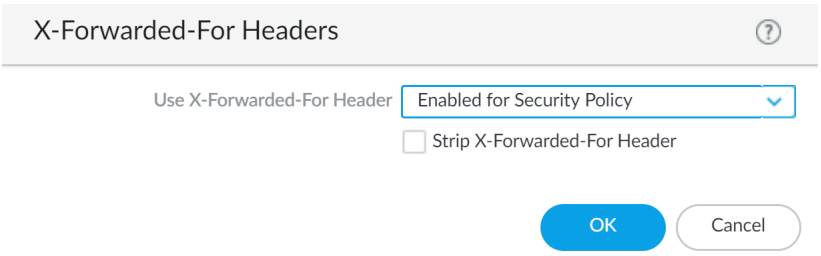
**STEP 2 |** Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Content-ID (ID de contenu)** > **X-Forwarded-For Headers (En-têtes X-Forwarded-For)**.

**STEP 3 |** Cliquez sur l'icône de modification.

**STEP 4 |** Sélectionnez **Enabled for Security Policy (Activé pour la politique de sécurité)** dans la liste déroulante **Use X-Forwarded-For Header (Utiliser l'en-tête X-Forwarded-For)**.

*Vous ne pouvez pas activer Utiliser l'en-tête X-Forwarded-For pour une politique de sécurité et un User-ID en même temps.*




**STEP 5 |** (Facultatif) Sélectionnez **Strip X-Forwarded-For Header (Enlever l'en-tête X-Forwarded-For)**. En sélectionnant cette option, l'en-tête XFF est supprimé avant que le pare-feu ne transmette la demande. Cette option ne désactive pas l'utilisation des en-têtes XFF ; le pare-feu utilise l'en-tête XFF pour l'application des politiques et la journalisation.

**STEP 6 |** Cliquez sur **OK**.

**STEP 7 |** **Commit (Validez)** vos modifications.

## Afficher les valeurs XFF dans les journaux

En plus de l'utilisation de l'en-tête XFF dans la politique de sécurité, vous pouvez consulter l'adresse IP XFF dans divers journaux, rapports et dans l'Application Command Center (Centre de commande des applications - ACC) pour faciliter la surveillance et le dépannage. Vous pouvez ajouter la colonne X-Forwarded-For dans les journaux du trafic, des menaces, de filtrage des données et des envois Wildfire.

Pour afficher l'adresse IP XFF dans vos journaux, suivez les étapes suivantes.

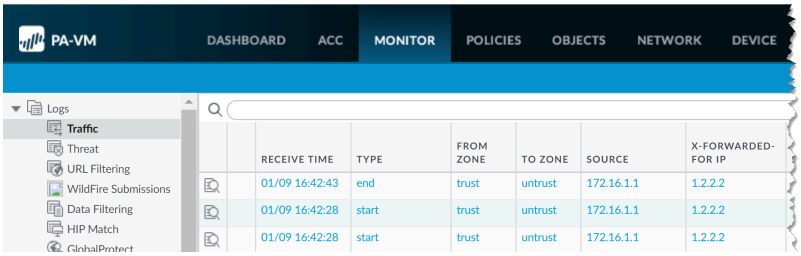
**STEP 1 |** Connectez-vous à votre pare-feu.

**STEP 2 |** Sélectionnez **Monitoring (Surveillance)** > **Logs (Journaux)**.

**STEP 3 |** Sélectionnez **Traffic (Trafic)**, **Threat (Menace)**, **Data Filtering (Filtrage de données)** ou **WildFire Submissions (Envois WildFire)**.

**STEP 4 |** Cliquez sur la flèche qui se trouve à la droite des en-têtes des colonnes, puis sélectionnez **Columns (Colonnes)**.

**STEP 5 |** Sélectionnez **X-Forwarded-For IP** pour afficher l'IP XFF dans votre journal.



## Afficher les valeurs XFF dans les rapports

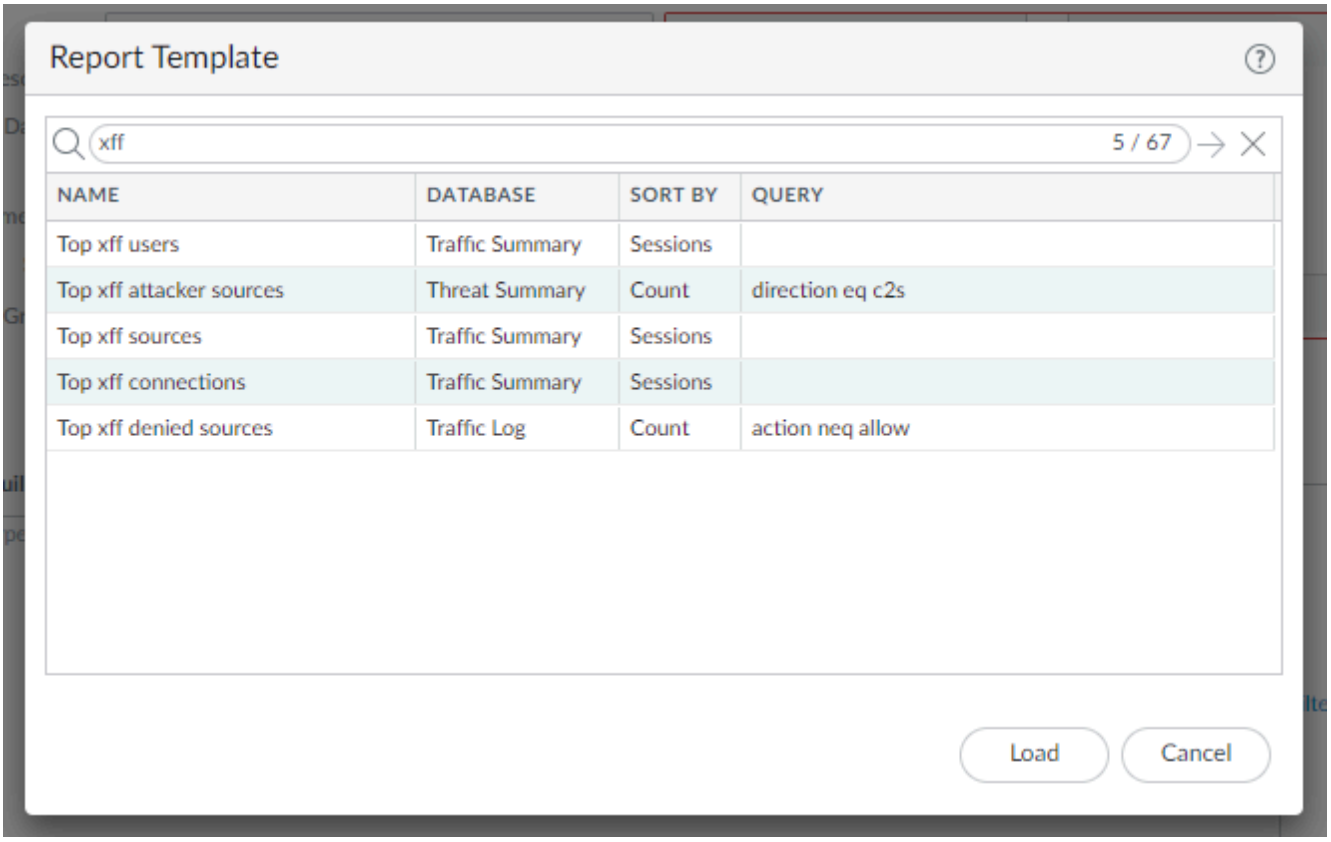
Les rapports prédéfinis générés par le pare-feu ne contiennent pas de valeurs XFF. Pour afficher les adresses IP XFF dans les rapports, le pare-feu comprend des modèles de rapport intégrés qui incluent des informations XFF.

**STEP 1 |** Connectez-vous à votre pare-feu.

**STEP 2 |** Sélectionnez **Monitor (Moniteur)** > **Manage Custom Reports (Gérer les rapports personnalisés)** > **Add (Ajouter)**.

**STEP 3 |** Cliquez sur **Load Template (Charger un modèle)**.

**STEP 4 |** Saisissez XFF dans la barre de recherche et cliquez sur le bouton de recherche pour trouver les modèles de rapport XFF intégrés.




**STEP 5 |** Cliquez sur **Load (Charger)**.

**STEP 6 |** Configurez votre rapport personnalisé **Time Frame (Intervalle de temps)**, **Sort By (Trier par)** et **Group By (Grouper par)** pour afficher les informations XFF de la manière la plus adaptée à vos besoins.

**STEP 7 |** (Facultatif) Cliquez sur **Run Now (Exécuter maintenant)** pour générer votre rapport à la demande au lieu de, ou en plus d'un **Scheduled Time (Temps planifié)**.

# Utiliser l'adresse IP dans l'en-tête XFF pour dépanner des événements

Par défaut, le pare-feu ne journalise pas l'adresse source d'un client derrière un serveur proxy, et ce, même si vous utilisez cette adresse à partir de l'en-tête X-Forwarded-For (XFF) aux fins du mappage d'utilisateur. Par conséquent, bien que vous puissiez identifier l'utilisateur spécifique associé à un événement du journal, vous ne serez pas en mesure de facilement identifier le périphérique source d'où provient l'événement du journal. Pour simplifier le débogage et le dépannage des événements pour les utilisateurs derrière un serveur proxy, vous devez activer l'option X-Forwarded-For dans la journalisation de l'en-tête HTTP dans le profil de filtrage des URL que vous avez associé aux règles de politique de sécurité qui autorisent l'accès aux applications Web. Lorsque cette option est activée, le pare-feu journalise l'adresse IP de l'en-tête XFF en tant qu'adresse source pour tout le trafic qui correspond à la règle.

*En activant l'option permettant au pare-feu d'utiliser l'en-tête XFF en tant qu'adresse source dans les journaux de filtrage des URL, vous n'activez pas le mappage d'utilisateur de l'adresse source. Pour renseigner les champs Utilisateur source, consultez la section* Utilisation des valeurs XFF pour les politiques et les utilisateurs sources de journalisation.

**STEP 1 |** Activez l'option X-forwarded-for de la journalisation de l'en-tête dans le profil de filtrage des URL.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **URL Filtering (Filtrage des URL)**, puis sélectionnez le profil de filtrage des URL que vous souhaitez configurer ou ajoutez-en un nouveau.

   *Vous ne pouvez activer la journalisation XFF dans le profil de filtrage des URL par défaut.*

2. Sélectionnez l'onglet **Settings (Paramètres)** et sélectionnez **X-Forwarded-For (X-Forwarded-For)**.
3. Cliquez sur **OK** pour enregistrer le profil.

**STEP 2 |** Associez le profil de filtrage des URL à la ou aux règles de politique de sécurité qui autorisent l'accès aux applications Web.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis cliquez sur la règle.
2. Sélectionnez l'onglet **Actions (Actions)**, définissez le **Profile Type (Type de profil)** sur **Profiles (Profils)** et sélectionnez le profil de **URL Filtering (Filtrage des URL)** que vous venez de configurer pour la journalisation de l'en-tête HTTP.
3. Cliquez sur **OK**, puis sur **Commit (Valider)**.

**STEP 3 |** Vérifiez que le pare-feu journalise les valeurs XFF.

1. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **URL Filtering (Filtrage des URL)**.
2. Affichez les valeurs XFF de l'une des manières suivantes :
   - Pour afficher la valeur XFF d'un seul journal de filtrage des URL : cliquez sur l'icône loupe pour que le journal affiche ses détails. La section HTTP Headers (En-têtes HTTP) affiche la valeur X-Forwarded-For.
   - Pour afficher les valeurs XFF de tous les journaux de filtrage des URL : ouvrez le menu déroulant de tout en-tête de colonne, sélectionnez **Columns (Colonnes)**, puis **X-Forwarded-For (X-Forwarded-For)**. La page affiche ensuite une colonne X-Forwarded-For.

**STEP 4 |** Utilisez le champ XFF dans le journal de filtrage des URL pour résoudre un événement de journal qui figure dans un journal d'un autre type.

Bien que seuls les journaux de filtrage des URL affichent l'adresse IP de l'utilisateur source dans la colonne X-Forwarded-For des journaux, si vous remarquez la présence d'un événement associé au trafic HTTP/HTTPS, mais qui ne peut identifier l'adresse IP source, car il s'agit de celle du serveur proxy, vous pouvez utiliser la valeur X-Forwarded-For dans un journal de filtrage des URL corrélés pour vous aider à identifier l'adresse source associée à un événement du journal. Pour ce faire :

1. Trouvez un événement sur lequel vous souhaitez enquêter dans des journaux du trafic, des menaces ou des envois WildFire qui indiquent l'adresse IP du serveur proxy en tant qu'adresse source.
2. Cliquez sur l'icône en forme de loupe pour que le journal affiche ses détails, puis cherchez un journal de filtrage des URL associé au bas de la fenêtre du Visualiseur de la vue détaillée du journal.
3. Sélectionnez la ligne d'en-tête, puis sélectionnez **X-Forwarded-For** dans la liste déroulante **Columns (Colonnes)** pour afficher cette valeur. L'adresse IP qui est indiquée dans cette colonne de la colonne X-Forwarded-For représente l'adresse IP de l'utilisateur source derrière le serveur proxy. Utilisez cette adresse IP pour repérer le périphérique qui a déclenché l'événement faisant l'objet de votre enquête.

# Transfert basé sur une politique

Normalement, le pare-feu utilise l'adresse IP de destination dans un paquet pour déterminer l'interface sortante. Le pare-feu utilise la table de routage associée au routeur virtuel auquel l'interface est connectée pour rechercher l'itinéraire. Le transfert basé sur une politique vous permet d'avoir le contrôle prioritaire sur la table de routage et d'indiquer l'interface sortante ou ***de sortie*** en fonction de certains paramètres tels que l'adresse IP source ou de destination ou le type de trafic.

- Transfert basé sur une politique (PBF)
- Création d'une règle de transfert basé sur une politique
- Cas d'utilisation : transfert basé sur une politique pour l'accès sortant avec deux fournisseurs de services Internet

## Transfert basé sur une politique (PBF)

Les règles de transfert basé sur une politique permettent au trafic de prendre un autre chemin que le saut suivant indiqué dans la table de routage. Elles sont généralement utilisées pour spécifier une interface de sortie pour des raisons de sécurité ou de performance. Supposons que votre entreprise dispose de deux liaisons entre le siège social et la succursale : une liaison Internet bon marché et une ligne louée plus coûteuse. La ligne louée est une liaison à large bande et à faible latence. Afin de renforcer la sécurité, vous pouvez utiliser le transfert basé sur une politique pour envoyer des applications qui ne sont pas du trafic crypté, notamment du trafic FTP, sur la ligne privée louée et tout autre trafic sur la liaison Internet. Sinon, afin d'améliorer les performances, vous pouvez choisir d'acheminer les applications essentielles sur la ligne louée et d'envoyer tout autre trafic, tel que la navigation Web, sur la liaison meilleur marché.

- Chemin de sortie et retour symétrique
- Surveillance des chemins pour PBF
- Services et applications dans le transfert basé sur une politique

### Chemin de sortie et retour symétrique

Le transfert basé sur une politique vous permet d'ignorer le trafic, de le diriger vers une interface spécifique sur le pare-feu ou vers un autre système virtuel (sur les périphériques prenant en charge plusieurs systèmes virtuels).

Dans les réseaux dotés d'un routage asymétrique, par exemple, dans un environnement composé de deux fournisseurs de services Internet, des problèmes de connectivité surviennent lorsque le trafic arrive au niveau d'une interface sur le pare-feu et quitte une autre interface. Si le routage est asymétrique, c'est-à-dire dans le cas où les chemins de transfert (paquet SYN) et de retour (SYN/ACK) sont différents, le pare-feu ne peut pas suivre l'état de la session et la connexion échoue. Pour vous assurer que le trafic utilise un chemin symétrique, autrement dit, que le trafic arrive au niveau d'une interface et quitte la même interface sur laquelle la session a été créée, vous pouvez activer l'option ***Retour symétrique***.

Lorsque cette option est sélectionnée, le routeur virtuel a le contrôle prioritaire sur la recherche d'itinéraire du trafic de retour et redirige le flux vers l'adresse MAC de laquelle il a reçu le paquet SYN (ou le premier paquet). Cependant, si l'adresse IP de destination se trouve sur le même sous-réseau que celle de l'interface d'entrée/de sortie, une recherche d'itinéraire est effectuée

et le retour symétrique n'est pas appliqué. Ce comportement permet d'éviter que le trafic soit silencieusement rejeté.

*Afin de déterminer le saut suivant pour des retours symétriques, le pare-feu utilise une table ARP (Address Resolution Protocol). Le nombre maximum d'entrées prises en charge par cette table ARP dépend du modèle de pare-feu. Cette valeur ne peut pas être configurée par l'utilisateur. Afin de déterminer la limite pour votre modèle, utilisez la commande de la CLI suivante :* ***`show pbf return-mac all`***.

## Surveillance des chemins pour PBF

La surveillance des chemins vous permet de vérifier la connexion à une adresse IP de manière à ce que le pare-feu puisse diriger le trafic via un autre itinéraire, si nécessaire. Le pare-feu utilise les requêtes ping ICMP comme ***pulsations*** pour vérifier que l'adresse IP donnée est accessible.

Un profil de surveillance vous permet d'indiquer le nombre maximum de pulsations pour déterminer si l'adresse IP est accessible. Lorsque l'adresse IP surveillée est inaccessible, vous pouvez soit désactiver la règle de transfert basé sur une politique soit indiquer une action ***Basculement*** ou ***En attente de récupération***. La désactivation de la règle de transfert basé sur une politique permet au routeur virtuel de prendre les décisions de routage. Lorsque l'action Basculement ou En attente de récupération est prise, le profil de surveillance continue de surveiller si l'adresse IP cible est accessible et, lorsqu'il récupère, le pare-feu recommence à utiliser l'itinéraire d'origine.

Le tableau suivant répertorie la différence de comportement entre une nouvelle session et une session établie, en cas d'échec de la surveillance des chemins.

| Comportement d'une session en cas d'échec de la surveillance | Si la règle reste activée lorsque l'adresse IP surveillée est inaccessible | Si la règle est désactivée lorsque l'adresse IP surveillée est inaccessible |
|---|---|---|
| **Pour une session établie** | **Wait-recover (En attente de récupération)**: continuez d'utiliser l'interface de sortie indiquée dans la règle de transfert basé sur une politique | **Wait-recover (En attente de récupération)**: continuez d'utiliser l'interface de sortie indiquée dans la règle de transfert basé sur une politique |
| | **Fail-over (Basculement)**: utilisez le chemin déterminé par la table de routage (pas de transfert basé sur une politique) | **Fail-over (Basculement)**: utilisez le chemin déterminé par la table de routage (pas de transfert basé sur une politique) |
| **Pour une nouvelle session** | **Wait-recover (En attente de récupération)**: Utilisez le chemin déterminé par la table de routage (pas de transfert basé sur une politique) | **En attente de récupération** : vérifiez les règles de transfert basé sur une politique restantes. S'il n'y a aucune correspondance, utilisez la table de routage. |
| | **Fail-over (Basculement)**: utilisez le chemin déterminé | **Basculement** : vérifiez les règles de transfert basé sur une politique restantes. S'il n'y a aucune |

| Comportement d'une session en cas d'échec de la surveillance | Si la règle reste activée lorsque l'adresse IP surveillée est inaccessible | Si la règle est désactivée lorsque l'adresse IP surveillée est inaccessible |
|---|---|---|
| | par la table de routage (pas de transfert basé sur une politique) | correspondance, utilisez la table de routage. |

### Services et applications dans le transfert basé sur une politique

Les règles de transfert basé sur une politique sont appliquées au premier paquet (SYN) ou à la première réponse au premier paquet (SYN/ACK). Ainsi, une règle de transfert basé sur une politique peut être appliquée avant que le pare-feu dispose de suffisamment d'informations pour déterminer l'application. Par conséquent, les règles propres à une application ne sont pas recommandées pour être utilisées avec le transfert basé sur une politique. Lorsque cela est possible, utilisez un objet de service, qui est le port de couche 4 (TCP ou UDP) utilisé par le protocole ou l'application.

Toutefois, si vous indiquez une application dans une règle de transfert basé sur une politique, le pare-feu effectue la ***mise en cache App-ID***. Lorsqu'une application passe par le pare-feu pour la première fois, le pare-feu ne dispose pas de suffisamment d'informations pour identifier l'application et ne peut donc pas appliquer la règle de transfert basé sur une politique. À l'arrivée d'autres paquets, le pare-feu détermine l'application et crée une entrée dans le cache App-ID et conserve cet App-ID pour la session. Lorsqu'une nouvelle session est créée avec la même adresse IP de destination, le même port de destination et le même ID de protocole, le pare-feu peut identifier l'application comme identique à la session initiale (selon le cache App-ID) et appliquer la règle de transfert basé sur une politique. Par conséquent, une session qui n'est pas une correspondance exacte et qui n'est pas la même application peut être transférée selon la règle de transfert basé sur une politique.

De plus, les applications ont des dépendances et l'identité de l'application peut changer lorsque le pare-feu reçoit d'autres paquets. Puisque le transfert basé sur une politique prend une décision de routage au début d'une session, le pare-feu ne peut pas appliquer de modification à l'identité de l'application. YouTube, par exemple, commence comme navigation Web, puis change en Flash, RTSP ou YouTube, en fonction des différents liens et vidéos inclus sur la page. Cependant, avec le transfert basé sur une politique, puisque le pare-feu identifie l'application comme navigation Web au début de la session, la modification de l'application n'est pas reconnue par la suite.

***Vous ne pouvez pas utiliser d'applications personnalisées, de filtres d'applications ou de groupes d'applications avec le transfert basé sur une politique.***

## Création d'une règle de transfert basé sur une politique

Utilisez une règle Transfert basé sur une politique (PBF) pour diriger le trafic vers une interface de sortie spécifique sur le pare-feu et remplacer le chemin par défaut du trafic.

**STEP 1 |** Créez une règle Policy-Based Forwarding (transfert basé sur une politique ; PBF).

Lors de la création d'une règle de transfert basé sur une politique, vous devez donner un nom à la règle, puis indiquer une interface ou une zone source et une interface de sortie. Tous les autres composants sont facultatifs ou ont une valeur par défaut.

*Vous pouvez préciser les adresses source et de destination en utilisant une adresse IP, un objet d'adresse ou un FQDN.*

1. Sélectionnez **Policies (Politiques)** > **Policy Based Forwarding (Transfert basé sur une politique)**, puis **Add (Ajoutez)** une règle de politique PBF.
2. Donnez un Name (Nom) descriptif à la règle (**General [Général]**).
3. Sélectionnez **Source**, puis configurez ce qui suit :
   1. Sélectionnez le **Type** (**Zone** ou **Interface**) auquel vous appliquerez la politique de transfert et spécifiez la zone ou l'interface correspondante. Si vous souhaitez appliquer le retour symétrique, vous devez sélectionner une interface source.

      *Seules les interfaces de Couche 3 prennent en charge PBF ; les interfaces en boucle ne prennent pas en charge PBF.*
   2. (Facultatif) Indiquez la **Source Address (Adresse source)** à laquelle la règle PBF s'appliquera, par exemple, une certaine adresse IP ou adresse IP de sous-réseau à partir

de laquelle vous souhaitez transférer le trafic vers l'interface ou la zone indiquée dans cette règle.

> *Cliquez sur **Negate (Refuser)** pour exclure une ou plusieurs **Source Addresses (Adresses IP source)** de la règle de transfert basé sur une politique. Par exemple, si votre règle de transfert basé sur une politique dirige tout le trafic depuis une zone indiquée vers Internet, l'option **Negate (Refuser)** vous permet d'exclure les adresses IP internes de la règle de transfert basé sur une politique.*

L'ordre d'évaluation des règles est de haut en bas. Une correspondance est établie entre un paquet et la première règle répondant aux critères définis. Après avoir déclenché une correspondance, les règles suivantes ne sont pas évaluées.

3. (Facultatif) **Add (Ajoutez)** et sélectionnez le **Source User (Utilisateur source)** ou les groupes d'utilisateurs au(x)quel(s) s'applique la politique.

4. Sélectionnez **Destination/Application/Service**, puis configurez les options suivantes :

   1. **Destination Address (Adresse de destination)** : Par défaut, la règle s'applique à **Any (Toute)** adresse IP. Cliquez sur **Negate (Refuser)** pour exclure une ou plusieurs adresses IP de destination de la règle de transfert basé sur une politique.
   2. **Add (Ajoutez)** toute **Application**ou tout **Service** que vous souhaitez contrôler à l'aide du transfert basé sur une politique.

   > *Nous ne recommandons pas l'utilisation des règles propres à une application avec le transfert basé sur une politique (PBF), car les règles de transfert basé sur une politique peuvent être appliquées avant que le pare-feu dispose de suffisamment d'information pour déterminer l'application. Lorsque cela est possible, utilisez un objet de service, qui est le port de couche 4 (TCP ou UDP) utilisé par le protocole ou l'application. Pour plus d'informations, reportez-vous à la section* Services et applications dans le transfert basé sur une politique.

**STEP 2 |** Indiquez comment transférer les paquets correspondant à la règle.

> *Si vous configurez le PBF dans un environnement à plusieurs systèmes virtuels, vous devez créer des règles PBF distinctes pour chaque système virtuel (et créez les règles de politique de sécurité appropriées pour autoriser le trafic).*

1. Sélectionnez **Forwarding (Transfert)**.
2. Définissez l'**action** à prendre lorsque de la mise en correspondance d'un paquet :
   - **Forward (Transférer)** : dirige le paquet vers l'**Egress Interface (Interface de sortie)** spécifiée.
   - **Forward to VSYS (Transférer vers un VSYS)** : (sur un pare-feu prenant en charge plusieurs systèmes virtuels) : sélectionnez le système virtuel vers lequel transférer le paquet.
   - **Discard (Supprimer)** : abandonne le paquet.
   - **No PBF (Pas de transfert basé sur une politique)** : exclut les paquets qui correspondent aux critères de la source, de la destination, de l'application ou du service définis dans

la règle. Les paquets correspondants utilisent la table de routage au lieu du transfert basé sur une politique ; le pare-feu utilise la table de routage pour exclure le trafic correspondant du port redirigé.

3. Pour déclencher l'**Action** indiquée à une fréquence quotidienne, hebdomadaire ou non récurrente, créez et associez un **Schedule (Calendrier)**.
4. Sous **Next Hop (Saut suivant)**, sélectionnez l'une des options suivantes :
   - **IP Address (Adresse IP)** : saisissez une adresse IP, ou sélectionnez un objet d'adresse de type masque réseau IP, à laquelle le pare-feu transfère les paquets mis en correspondance. Un objet d'adresse IPv4 doit comporter un masque réseau /32 et un objet d'adresse IPv6 doit comporter un masque réseau /128.
   - **FQDN** : saisissez un FQDN (ou sélectionnez ou créez un objet d'adresse de type FQDN) auquel le pare-feu transfère les paquets mis en correspondance. Le FQDN peut se résoudre en une adresse IPv4, une adresse IPv6, ou les deux. Si le FQDN se résout en une adresse IPv4 et une adresse IPv6, la règle PBF a alors deux sauts suivants : une adresse IPv4 et une adresse IPv6. Vous pouvez utiliser la même règle PBF pour le trafic IPv4 et IPv6. Le trafic IPv4 est transmis au saut suivant IPv46 et le trafic IPv6, au saut suivant IPv6.

     *Ce FQDN doit se résoudre en une adresse IP qui appartient au même sous-réseau comme l'interface que vous avez configurée pour PBF. Sinon, le pare-feu rejette la résolution et le FQDN demeure non résolu.*

     *Le pare-feu n'utilise qu'une seule adresse IP (de chaque type de famille IPv4 ou IPv6) de la résolution DNS du FQDN. Si la résolution FQDN donne plus d'une adresse, le pare-feu utilise l'adresse IP privilégiée qui correspond au type de famille IP (Ipv4 ou IPv6) configuré pour le saut suivant. L'adresse IP privilégiée est la première adresse que le serveur DNS retourne dans sa réponse initiale. Le pare-feu conserve cette adresse en tant que privilégiée tant que l'adresse apparaît dans les réponses subséquentes, peu importe l'ordre.*
   - **None (Aucun)** : en l'absence d'un saut suivant, l'adresse IP de destination du paquet est utilisée comme saut suivant. Le transfert échoue si l'adresse IP de destination n'est pas dans le même sous-réseau que l'interface de sortie.
5. (Facultatif) Activez la surveillance pour vérifier la connexion à une adresse IP cible ou à l'adresse IP de **Next Hop (Saut suivant)** si aucune adresse IP n'est spécifiée. Sélectionnez **Monitor (Surveillance)** et associez un **Profile (Profil)** de surveillance (par défaut ou personnalisé) qui indique l'action lorsque l'adresse surveillée est inaccessible.
   - Vous pouvez **Disable this rule if nexthop/monitor ip is unreachable (Désactiver cette règle si l'adresse IP de surveillance/le saut suivant est inaccessible)**.
   - Saisissez une **IP Address (Adresse IP)** cible à surveiller.

   La **Egress Interface (Interfaces de sortie)** peut comporter des adresses IPv4 et IPv6, et le FQDN de **Next Hop (Saut suivant)** peut se résoudre en des adresses IPv4 et IPv6. Dans ce cas :

   **1.** Si l'interface de sortie contient des adresses IPv4 et IPv6 et que le FQDN de saut suivant se résout uniquement en un type de famille d'adresses, le pare-feu surveille l'adresse IP résolue. Si le FQDN se résout en deux adresses IPv4 et IPv6, mais que

l'interface de sortie contient un seul type de famille d'adresses, le pare-feu surveille l'adresse de saut suivant résolue qui correspond à la famille d'adresses de l'interface de sortie.

2. Si l'interface de sortie et le FQDN de saut suivant possèdent des adresses IPv4 et IPv6, le pare-feu surveille l'adresse de saut suivant IPv4.
3. Si l'interface de sortie contient une seule famille d'adresses et que le FQDN de saut suivant se résout en un autre type de famille d'adresses, le pare-feu ne surveille rien du tout.

6. (Obligatoire pour les environnements de routage asymétrique ; autrement, facultatif) **Enforce Symmetric Return (Appliquez le retour symétrique)**, puis **Add (Ajoutez)** une ou plusieurs adresses IP dans la **Next Hop Address List (Liste d'adresses du saut suivant)**. Vous pouvez ajouter un maximum de huit adresses IP de saut suivant ; les interfaces de tunnel et PPoE ne sont pas disponibles en tant qu'adresse IP de saut suivant.

   L'activation du retour symétrique permet de s'assurer que le trafic de retour (par exemple, depuis la zone approuvée sur le réseau local vers Internet) est transféré via la même interface que celle au niveau de laquelle le trafic arrive d'Internet.

**STEP 3 |** **Commit (Validez)** vos modifications. La règle de transfert basé sur une politique est effective.

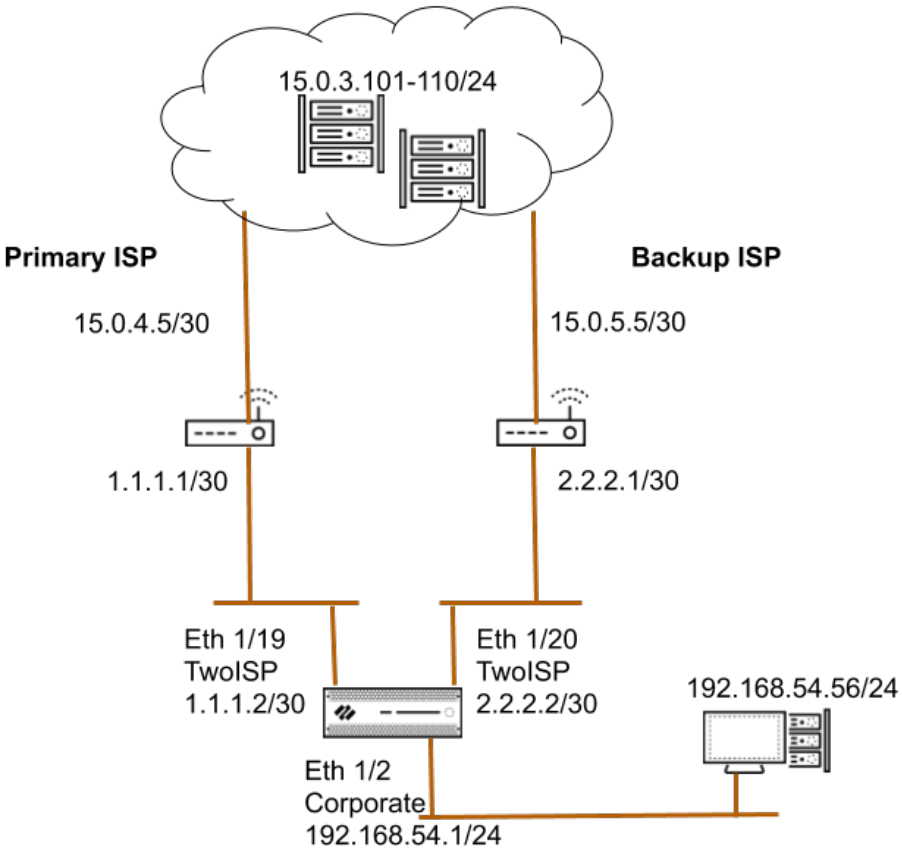
| | Source | | | Destination | | | Forwarding | | | Monitoring | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| NAME | ZONE/INTERFACE | ADDRESS | USER | ADDRESS | SERVICE | ACTION | EGRESS I/F | NEXT HOP | ENFORCE SYMMETRIC RETURN | PROFILE | DISABLE IF UNREACHABL |
| pdf2 | ethernet1/3 | any | any | HQ-subnet | service-http | forward | ethernet1/1.100 | 192.168.100.2 | false | none | false |

# Cas d'utilisation : transfert basé sur une politique pour l'accès sortant avec deux fournisseurs de services Internet

Dans ce cas pratique, la succursale dispose d'une configuration à deux fournisseurs de services Internet et implémente le transfert basé sur une politique pour un accès Internet redondant. Le fournisseur de services Internet de secours est l'itinéraire par défaut du trafic depuis le client vers les serveurs Web. Afin de permettre un accès Internet redondant sans utiliser de protocole inter-réseau, tel que BGP, utilisez le transfert basé sur une politique avec une traduction NAT source basée sur l'interface de destination et des itinéraires statiques, puis configurez le pare-feu comme suit :

- Activez une règle de transfert basé sur une politique qui achemine le trafic vers le fournisseur de services Internet principal et associez un profil de surveillance à la règle. Le profil de surveillance indique au pare-feu d'utiliser l'itinéraire par défaut via le fournisseur de services Internet de secours, lorsque le fournisseur de services Internet principal n'est pas disponible.
- Définissez des règles NAT source pour les fournisseurs de services Internet principal et de secours qui indiquent au pare-feu d'utiliser l'adresse IP source associée à l'interface de sortie du fournisseur de services Internet correspondant. Le trafic sortant dispose ainsi de la bonne adresse IP source.
- Ajoutez un itinéraire statique au fournisseur de services Internet de secours de manière à ce que, lorsque le fournisseur de services Internet principal n'est pas disponible, l'itinéraire par défaut soit effectif et le trafic soit dirigé vers le fournisseur de services Internet de secours.



**STEP 1 |** Configurez les interfaces d'entrée et de sortie sur le pare-feu.

Les interfaces de sortie peuvent se trouver dans la même zone.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** et choisissez l'interface que vous voulez configurer.

   Les configurations d'interface sur le pare-feu utilisé dans cet exemple sont les suivantes :

   - Ethernet 1/19 connectée à l'ISP principal :
     - Zone : DeuxISP
     - IP address: 1.1.1.2/30
     - Routeur virtuel : Default (Par défaut)
   - Ethernet 1/20 connectée à l'ISP secours :
     - Zone : DeuxISP
     - IP address: 2.2.2.2/30
     - Routeur virtuel : Default (Par défaut)
   - Ethernet 1/2 est l'interface d'entrée, utilisée par les clients réseau pour se connecter à Internet :
     - Zone : Entreprise
     - IP address: 192.168. 54.1/24
     - Routeur virtuel : Default (Par défaut)
2. Pour enregistrer la configuration de l'interface, cliquez sur **OK**.

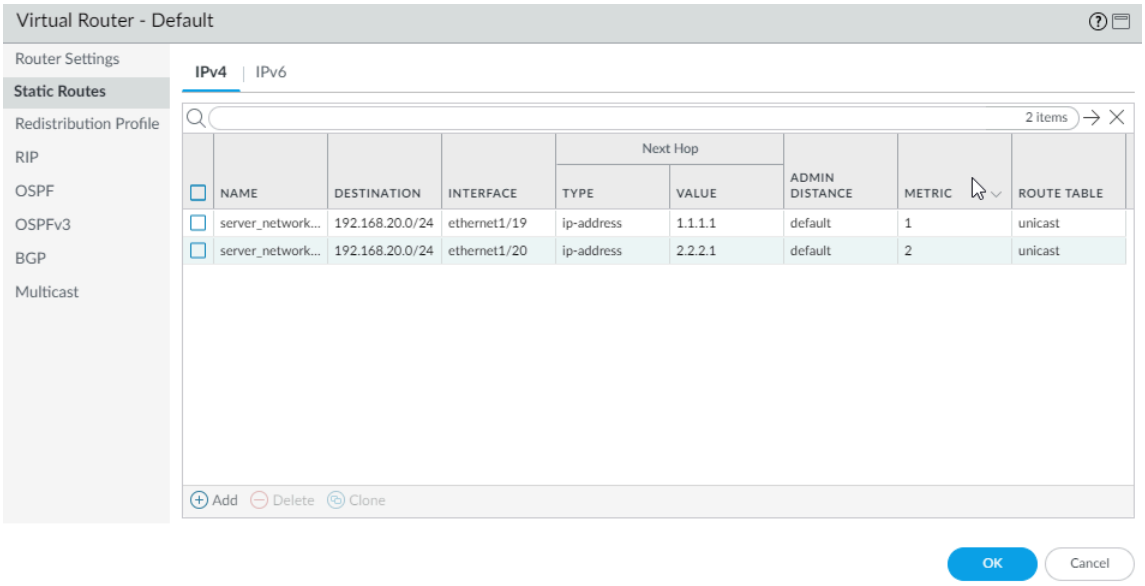
**STEP 2 |** Sur le routeur virtuel, ajoutez un itinéraire statique au fournisseur de services Internet de secours.

1. Sélectionnez **Network (Réseau)** > **Virtual Router (Routeur virtuel)**, puis sélectionnez le lien **default (par défaut)** pour ouvrir la boîte de dialogue Routeur virtuel.
2. Sélectionnez **Static Routes (Itinéraires statiques)** et cliquez sur **Add (Ajouter)**. Donnez un **Name (nom)** à l'itinéraire et indiquez l'adresse IP de **Destination (destination)** pour laquelle

vous définissez l'itinéraire statique. Dans cet exemple, 0.0.0.0/0 est utilisé pour tout le trafic.

3. Sélectionnez la case d'option **IP Address (Adresse IP)** et définissez l'adresse IP de **Next Hop (Saut suivant)** du routeur qui se connecte à la passerelle Internet de secours (vous ne pouvez pas utiliser un nom de domaine pour le saut suivant). Dans cet exemple, 2.2.2.1.
4. Indiquez une mesure de coût pour l'itinéraire.




5. Cliquez deux fois sur **OK (OK)** pour enregistrer la configuration du routeur virtuel.

**STEP 3 |** Créez une règle de transfert basé sur une politique qui dirige le trafic vers l'interface qui est connectée au fournisseur de services Internet principal.

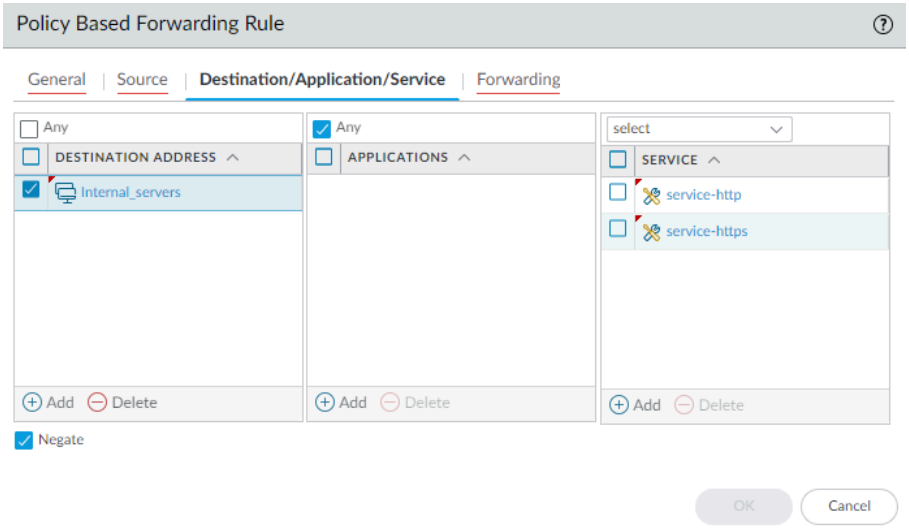
Assurez-vous d'exclure le trafic destiné aux serveurs/adresses IP internes du transfert basé sur une politique. Définissez une règle de refus de manière à ce que le trafic destiné aux adresses IP internes ne soit pas acheminé via l'interface de sortie indiquée dans la règle de transfert basé sur une politique.

1. Sélectionnez **Policies (Politiques)** > **Policy Based Forwarding (Transfert basé sur une politique)**, puis cliquez sur **Add (Ajouter)**.
2. Dans l'onglet **General (Général)**, donnez un **Name (Nom)** descriptif à la règle.
3. Dans l'onglet **Source**, définissez la **Source Zone (Zone source)** ; dans cet exemple, la zone est Corporate.
4. Dans l'onglet **Destination/Application/Service**, définissez les options suivantes :
   1. Dans la section Adresse de destination, **Add (ajoutez)** les adresses IP ou la plage d'adresses IP des serveurs sur le réseau interne ou créez un objet d'adresse pour vos serveurs internes. Sélectionnez **Negate (Refuser)** pour exclure les adresses IP ou l'objet d'adresse répertorié ci-dessus de cette règle.

2. Dans la section Service, **Add (ajoutez)** les services **service-http** et **service-https** pour autoriser le trafic HTTP et HTTPS à utiliser les ports par défaut. L'itinéraire par défaut sera utilisé pour tout autre trafic autorisé par la politique de sécurité.

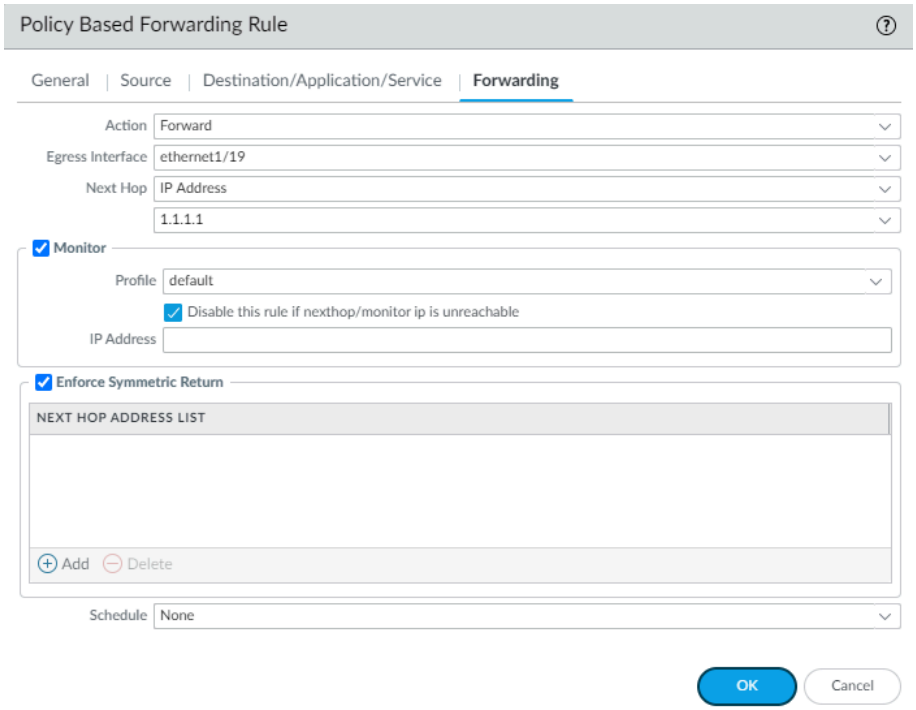
   *Pour transférer tout le trafic à l'aide du transfert basé sur une politique, définissez le service sur **Any (Indifférent)**.*




**STEP 4 |** Spécifiez la destination de transfert du trafic.

1. Dans l'onglet **Forwarding (Transfert)**, indiquez l'interface vers laquelle vous souhaitez transférer le trafic et activer la surveillance des chemins.
2. Pour transférer le trafic, définissez l'**Action (Action)** sur **Forward (Transférer)**, puis sélectionnez l'**Egress Interface (Interface de sortie)** et indiquez le **Next Hop (Saut**

**suivant)**. Dans cet exemple, l'interface de sortie est ethernet1/19 et l'adresse IP de saut suivant est 1.1.1.1 (vous ne pouvez pas utiliser un FQDN pour le saut suivant).




3. Activez la **Monitor (surveillance)** et associez le profil de surveillance par défaut pour déclencher un basculement vers le fournisseur de services Internet de secours. Dans cet exemple, aucune adresse IP cible à surveiller n'est indiquée. Le pare-feu surveillera l'adresse IP de saut suivant ; si cette adresse IP est inaccessible, le pare-feu dirigera le trafic vers l'itinéraire par défaut indiqué sur le routeur virtuel.
4. (Requis si vous disposez d'un routage asymétrique) Sélectionnez **Enforce Symmetric Return (Appliquer le retour symétrique)** pour vous assurer que le trafic de retour depuis la zone approuvée vers Internet est transféré sur la même interface que celle au niveau de laquelle le trafic arrive d'Internet.
5. La traduction NAT garantit que le trafic provenant d'Internet est renvoyé vers la bonne interface/adresse IP sur le pare-feu.
6. Cliquez sur **OK (OK)** pour enregistrer les modifications.

| | | Source | | | Destination | | | | Forwarding | | | Monitoring | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | NAME | ZONE/INTERFACE | ADDRESS | USER | ADDRESS | APPLICATION | SERVICE | ACTION | EGRESS I/F | NEXT HOP | ENFORCE SYMMETRIC RETURN | PROFILE | TARGET | DISABLE IF UNR |
| 1 | pbf_rule_source_zone | Corporate | 192.168.10.2 | any | any | any | service-http<br>service-https | forward | ethernet1/19 | 1.1.1.1 | true | default | none | true |

**STEP 5 |** Créez des règles NAT basées sur l'interface de sortie et le fournisseur de services Internet. Ces règles s'assurent que la bonne adresse IP source est utilisée pour les connexions sortantes.

1. Sélectionnez **Policies (Politiques)** > **NAT (NAT)**, puis cliquez sur **Add (Ajouter)**.
2. Dans cet exemple, la règle NAT créée pour chaque fournisseur de services Internet est la suivante :

   **Règle NAT pour le fournisseur de services Internet principal**

   Dans l'onglet **Original Packet (Paquet d'origine)**,

   **Zone source** : Entreprise

   **Destination Zone (Zone de destination)** : DeuxISP

   Dans l'onglet **Translated Packet (Paquet traduit)**, sous Traduction de l'adresse source,

   **Translation Type (Type de traduction)** : port et IP dynamiques

   **Address Type (Type d'adresse)** : Adresse de l'interface

   **Interface** : ethernet1/19

   **IP Address (Adresse IP)** : 1.1.1.2/30

   **Règle NAT pour le fournisseur de services Internet de secours**

   Dans l'onglet **Original Packet (Paquet d'origine)**,

   **Zone source** : Entreprise

   **Destination Zone (Zone de destination)** : DeuxISP

   Dans l'onglet **Translated Packet (Paquet traduit)**, sous Traduction de l'adresse source,

   **Translation Type (Type de traduction)** : port et IP dynamiques

   **Address Type (Type d'adresse)** : Adresse de l'interface

   **Interface** : ethernet1/20

   **IP Address (Adresse IP)** : 2.2.2.2/30

| | | | Original Packet | | | | | | Translated Packet | |
|---|---|---|---|---|---|---|---|---|---|---|
| | NAME | TAGS | SOURCE ZONE | DESTINATION ZONE | DESTINATION INTERFACE | SOURCE ADDRESS | DESTINATION ADDRESS | SERVICE | SOURCE TRANSLATION | DESTINATION TRANSL |
| 1 | NAT for Primary ISP | none | Corporate | TwoISP | any | any | any | any | dynamic-ip-and-port<br>ethernet1/19<br>1.1.1.2/30 | none |
| 2 | NAT for Backup ISP | none | Corporate | TwoISP | any | any | any | any | dynamic-ip-and-port<br>ethernet1/20<br>2.2.2.2/30 | none |

**STEP 6 |** Créez une politique de sécurité pour autoriser l'accès sortant à Internet.

Pour activer en toute sécurité les applications, créez une simple règle qui autorise l'accès à Internet et associez les profils de sécurité disponibles sur le pare-feu.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et cliquez sur **Add (Ajouter)**.
2. Dans l'onglet **General (Général)**, donnez un **Name (Nom)** descriptif à la règle.
3. Dans l'onglet **Source**, réglez la **Source Zone (Zone Source)** sur Corporate (Entreprise).
4. Dans l'onglet **Destination**, définissez la **Zone de destination** sur TwoISP.
5. Dans l'onglet **Service/ URL Category (Catégorie de service/d'URL)**, laissez l'option par défaut **application-default (Par défaut de l'application)**.
6. Dans l'onglet **Actions**, exécutez les tâches suivantes :
   1. Définissez l'**Action Setting (Paramètre d'action)** sur **Allow (Autoriser)**.
   2. Joignez les profils par défaut pour l'antivirus, l'antispyware, la protection contre les vulnérabilités et le filtrage des URL, sous **Profile Setting. (Paramètre du profil)**.
7. Sous **Options**, vérifiez que la journalisation est activée à la fin d'une session. Seul le trafic qui correspond à une règle de sécurité est consigné.

| | NAME | TAGS | TYPE | Source | | | | Destination | | | APPLICATION | SERVICE | ACTION |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS | DEVICE | | | |
| 1 | Copr2ISP | none | universal | Corporate | any | any | any | TwoISP | any | any | any | any | Allow |

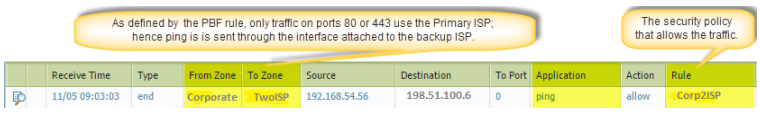
**STEP 7 |** Sauvegardez les politiques dans la configuration en cours d'exécution sur le pare-feu.

Cliquez sur **Commit (Valider)**.

**STEP 8 |** Vérifiez que la règle de transfert basé sur une politique est active et que le fournisseur de services Internet principal est utilisé pour l'accès Internet.

1. Ouvrez votre navigateur Web et accédez au serveur Web. Sur le pare-feu, recherchez l'activité de navigation Web dans le journal du trafic.
2. À partir d'un client sur le réseau, utilisez l'utilitaire ping pour vérifier la connexion à un serveur Web sur Internet et consultez le journal du trafic sur le pare-feu.

```
C:\Users\pm-user1>ping 198.51.100.6
Pinging 198.51.100.6 with 32 bytes of data:
Reply from 198.51.100.6: bytes=32 time=34ms TTL=117
Reply from 198.51.100.6: bytes=32 time=13ms TTL=117
Reply from 198.51.100.6: bytes=32 time=25ms TTL=117
Reply from 198.51.100.6: bytes=32 time=3ms TTL=117
Ping statistics for 198.51.100.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milliseconds:
    Minimum = 3ms, Maximum = 34ms, Average = 18ms
```



3. Pour confirmer que la règle PBF est active, utilisez la commande CLI suivante :

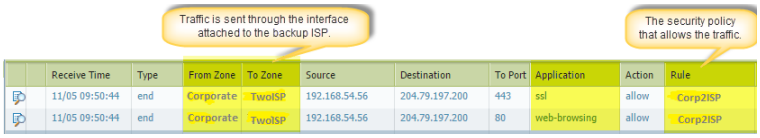
```
admin@PA-NGFW> show pbf rule all
Rule       ID    Rule State Action   Egress IF/VSYS  NextHop
========== === ========== ====== ==============
Use ISP-Pr 1 Active     Forward ethernet1/1 1.1.1.1
```

**STEP 9 |** Vérifiez que le basculement vers le fournisseur de services Internet de secours est effectué et que la traduction NAT source est correctement appliquée.

1. Déconnectez le fournisseur de services Internet principal.
2. Confirmez que la règle PBF est inactive avec la commande CLI suivante :

```
admin@PA-NGFW> show pbf rule all
Rule       ID    Rule State Action   Egress IF/VSYS  NextHop
========== === ========== ====== ============== ===
Use ISP-Pr 1 Disabled Forward ethernet1/19     1.1.1.1
```

3. Accédez à un serveur Web et consultez le journal du trafic pour vérifier que le trafic est transféré via le fournisseur de services Internet de secours.




4. Affichez les détails de la session pour vérifier que la règle NAT fonctionne correctement.

```
admin@PA-NGFW> show session all
--------------------------------------------------------------
ID Application    State   Type Flag Src[Sport]/Zone/Proto
 (translated IP[Port]) Vsys Dst[Dport]/Zone (translated
 IP[Port])
--------------------------------------------------------------
87212 ssl ACTIVE  FLOW  NS   192.168.54.56[53236]/Corporate/6
  (2.2.2.2[12896]) vsys1 204.79.197.200[443]/TwoISP
 (204.79.197.200[443])
```

5. Obtenez le numéro d'identification de la session dans le résultat et affichez les détails de la session.

*La règle de transfert basé sur une politique n'est pas utilisée et n'est donc pas répertoriée dans le résultat.*

```
admin@PA-NGFW> show session id 87212
Session           87212
c2s flow:
                source:      192.168.54.56 [Corporate]
                dst:         204.79.197.200
                proto:       6
                sport:       53236           dport:      443
                state:       ACTIVE          type:       FLOW
                src user:    unknown
```

```
                dst user:    unknown
s2c flow:
                source:      204.79.197.200 [TwoISP]
                dst:         2.2.2.2
                proto:       6
                sport:       443             dport:
 12896
                state:       ACTIVE          type:       FLOW
                src user:    unknown
                dst user:    unknown
start time                    : Wed Nov5 11:16:10 2014
        timeout                          : 1800 sec
        time to live                     : 1757 sec
        total byte count(c2s)            : 1918
        total byte count(s2c)            : 4333
        layer7 packet count(c2s)         : 10
        layer7 packet count(s2c)         : 7
        vsys                             : vsys1
        application                      : ssl
        rule                             : Corp2ISP
        session to be logged at end      : True
        session in session ager          : True
        session synced from HA peer      : False
        address/port translation         : source
        nat-rule                         : NAT-Backup ISP(vsys1)
        layer7 processing                : enabled
        URL filtering enabled            : True
        URL category                     : search-engines
        session via syn-cookies          : False
        session terminated on host       : False
        session traverses tunnel         : False
        authentication portal session        : False
        ingress interface                : ethernet1/2
        egress interface                 : ethernet1/20
        session QoS rule                 : N/A (class 4)
```

# Test des règles de politique

Testez les règles de politique dans votre configuration active pour veiller à ce que vos politiques autorisent et refusent comme il se doit le trafic et l'accès aux applications et aux sites Web, dans le respect de vos besoins et de vos exigences d'affaires. Vous pouvez tester et vérifier que vos règles de politique autorisent et refusent le bon trafic en exécutant les tests de correspondance de la politique pour vos pare-feu directement à partir de l'interface Web.

**STEP 1 |** Lancement de l'interface Web.

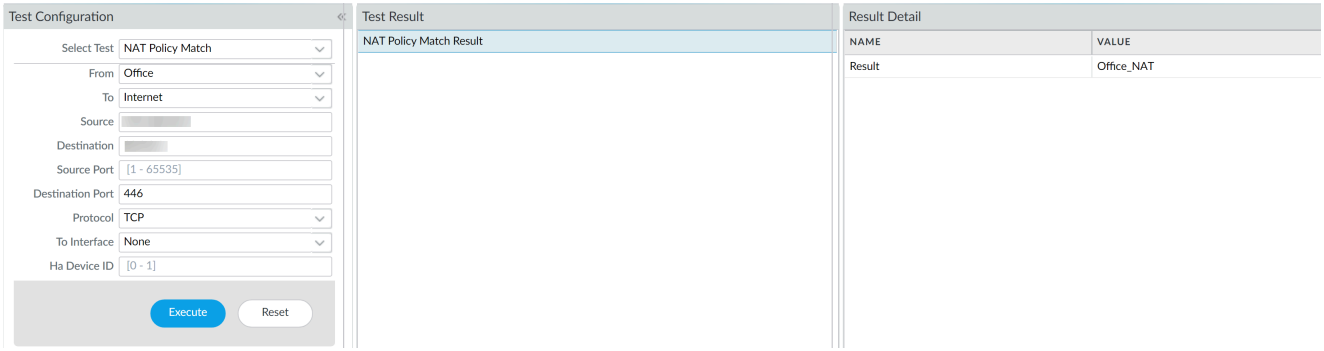
**STEP 2 |** Sélectionnez **Device (Périphérique)** > **Troubleshooting (Résolution des problèmes)** pour effectuer un test de connectivité ou de correspondance de la politique.

**STEP 3 |** Saisissez les informations requises pour effectuer le test de correspondance de la politique. Dans cet exemple, nous exécutons un tests de correspondance de la politique NAT.

1. **Select Test (Sélectionner le test)** : sélectionnez **NAT Policy Match (Correspondance de la politique NAT)**.
2. **From (Depuis)** : sélectionnez la zone d'où le trafic provient.
3. **To (Vers)** : sélectionnez la zone cible du trafic.
4. **Source** : saisissez l'adresse IP de laquelle provient le trafic.
5. **Destination** : saisissez l'adresse IP du périphérique cible pour le trafic.
6. **Destination Port (Port de destination)** : saisissez le port utilisé pour le trafic. Ce port varie selon le protocole IP utilisé à l'étape suivante.
7. **Protocol (Protocole)** : saisissez le protocole IP utilisé pour le trafic.
8. Au besoin, saisissez les informations complémentaires pertinente pour le test de votre règle de politique NAT.

**STEP 4 |** **Execute (Exécutez)** le test de correspondance de la politique de NAT.

**STEP 5 |** Passez en revue le **NAT Policy Match Result (Résultat de la correspondance de la politique NAT)** pour voir les règles de politique qui correspondent aux critères du test.



# Systèmes virtuels

Cette rubrique décrit les systèmes virtuels, leurs avantages, les cas pratiques typiques et comment les configurer. Elle fournit également des liens vers d'autres rubriques dans lesquelles les systèmes virtuels sont décrits lorsqu'ils sont combinés à d'autres fonctionnalités.

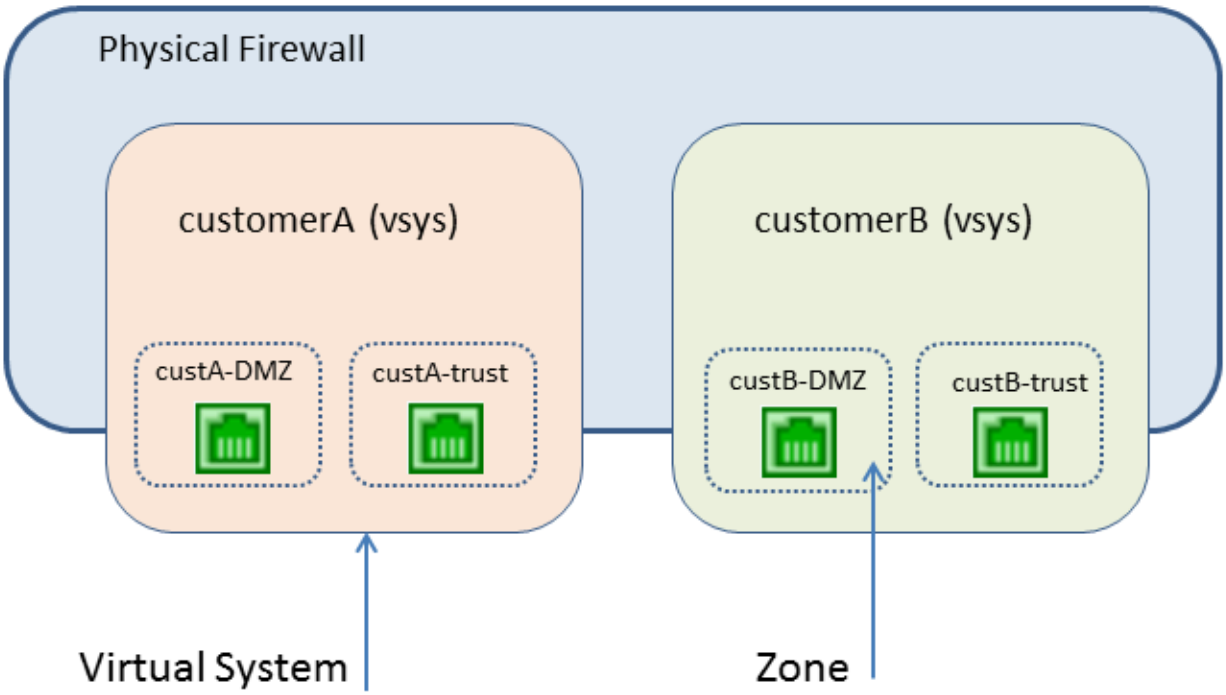
# Présentation des systèmes virtuels

Les systèmes virtuels sont des instances de pare-feu logiques et distinctes dans un pare-feu Palo Alto Networks physique unique. Plutôt que d'utiliser plusieurs pare-feu, les fournisseurs de services gérés et les entreprises peuvent utiliser une paire de pare-feu (pour la haute disponibilité) et y activer des systèmes virtuels. Chaque système virtuel (vsys) est un pare-feu indépendant et géré séparément dont le trafic est tenu à l'écart du trafic des autres systèmes virtuels.

- Composants d'un système virtuel et segmentation
- Avantages des systèmes virtuels
- Cas pratiques de systèmes virtuels
- Prise en charge et licence de plateforme des systèmes virtuels
- Rôles administrateur des systèmes virtuels
- Objets partagés des systèmes virtuels

## Composants d'un système virtuel et segmentation

Un système virtuel est un objet qui crée une limite administrative, comme illustré dans la figure suivante.




Un système virtuel est constitué d'un ensemble d'interfaces et de sous-interfaces physiques et logiques (notamment les VLAN et câbles virtuels), des routeurs virtuels et des zones de sécurité. Vous choisissez le ou les modes de déploiement (toute combinaison de câble virtuel, de Couche 2 ou de Couche 3) de chaque système virtuel. Grâce aux systèmes virtuels, vous pouvez segmenter l'un des éléments suivants :

- Accès administrateur

- La gestion de toutes les politiques (sécurité, NAT, QoS, policy-based forwarding (transfert basé sur une politique - PBF), décryptage, contrôle prioritaire sur l'application, inspection des tunnels, authentification et protection DoS)
- Tous les objets (comme des objets d'adresse, groupes et filtres d'applications, listes dynamiques externes, profils de sécurité, profils de décryptage, objets personnalisés, etc.)
- User-id
- Gestion des certificats
- Profils de serveur
- Journalisation, génération de rapports et fonctions de visibilité

Les systèmes virtuels affectent les fonctions de sécurité du pare-feu, mais ils n'affectent pas les fonctions de mise en réseau comme le routage statique ou dynamique. Vous pouvez segmenter le routage de chaque système virtuel en créant un ou plusieurs routeurs virtuels pour chaque système virtuel, comme dans les cas pratiques suivants :

- Si vous disposez de systèmes virtuels pour les services d'une entreprise et que l'ensemble du trafic réseau de tous les services se trouve dans un réseau commun, vous pouvez créer un routeur virtuel pour plusieurs systèmes virtuels.
- Si vous souhaitez segmenter le routage et que le trafic de chaque système virtuel soit isolé des autres systèmes virtuels, vous pouvez créer un ou plusieurs routeurs virtuels par système virtuel.
- Si vous souhaitez segmenter les mappages d'utilisateur pour éviter que tous les mappages soient partagés sur l'ensemble des systèmes virtuels, vous pouvez configurer les sources User-ID sur un système virtuel qui n'est pas un pôle User-ID. Reportez-vous à la section Partage des mappages User-ID sur l'ensemble des systèmes virtuels.

## Avantages des systèmes virtuels

Les systèmes virtuels offrent les mêmes fonctions de base qu'un pare-feu physique, plus les avantages supplémentaires suivants :

- **Administration segmentée** : différentes entreprises (ou clients, ou unités commerciales) peuvent contrôler (et surveiller) une instance de pare-feu distincte. Elles peuvent ainsi contrôler leur propre trafic sans interférer avec le trafic ou les politiques d'une autre instance de pare-feu sur le même pare-feu physique.
- **Évolutivité** : une fois le pare-feu physique configuré, l'ajout ou la suppression de clients ou d'unités commerciales peut être réalisé efficacement. Un ISP, un fournisseur de services de sécurité gérés ou une entreprise peut proposer des services de sécurité différents à chaque client.
- **Dépenses d'investissement et d'exploitation réduites** : avec les systèmes virtuels, il n'est plus nécessaire de disposer de plusieurs pare-feu physiques à un emplacement car les systèmes virtuels coexistent sur un même pare-feu. N'ayant pas besoin d'acheter plusieurs pare-feu, une entreprise peut réaliser des économies sur les dépenses de matériel, les factures d'électricité et l'encombrement, et peut réduire ses dépenses de maintenance et de gestion.
- **Capacité de partager les informations de mappage adresse IP/nom d'utilisateur** : En faisant d'un système virtuel un pôle User-ID, vous pouvez partager les mappages d'adresse IP/nom d'utilisateur sur l'ensemble des systèmes virtuels afin d'exploiter la pleine capacité User-ID du pare-feu et de réduire la complexité opérationnelle.

## Cas pratiques de systèmes virtuels

Les systèmes virtuels peuvent être utilisés de nombreuses manières dans un réseau. Un cas pratique courant consiste, pour un ISP ou un Managed Security Service Provider (fournisseur de services de sécurité gérés - MSSP), à fournir ses services à plusieurs clients via à un seul et même pare-feu. Les clients ont le choix parmi une large gamme de services qu'ils peuvent facilement activer ou désactiver. L'administration basée sur le rôle du pare-feu permet à l'ISP ou au MSSP de contrôler l'accès de chaque client à une fonctionnalité (la journalisation et la génération de rapports par exemple) tout en masquant ou en proposant d'autres fonctions en lecture seule.

Un autre cas pratique courant concerne une grande entreprise qui a besoin de différentes instances de pare-feu en raison des différentes exigences techniques ou de confidentialité des nombreux services. Comme dans le premier cas, différents groupes peuvent avoir des niveaux d'accès différents alors que le service informatique gère, quant à lui, le pare-feu. Les services peuvent être suivis et/ou facturés aux services, permettant ainsi d'appliquer une comptabilité distincte dans une entreprise.

## Prise en charge et licence de plateforme des systèmes virtuels

Les systèmes virtuels sont pris en charge sur les pare-feu PA-3200, PA-5200 et PA-7000 Series. Chaque série de pare-feu prend en charge un nombre de systèmes virtuels de base, qui varie selon la plateforme. Une licence Systèmes virtuels est requise pour prendre en charge plusieurs systèmes virtuels sur les pare-feux PA-3200 Series et pour créer un plus grand nombre de systèmes virtuels que le nombre en charge par une plateforme.

Pour plus d'informations sur la licence, reportez-vous à la section Abonnements. Pour le nombre de base et maximum de systèmes virtuels pris en charge, reportez-vous à l'outil Comparer des pare-feu.

Plusieurs systèmes virtuels ne sont pas pris en charge sur les pare-feu PA-220, PA-800 Series, ou VM-Series.

*La valeur par défaut est **vsys1**. Vous ne pouvez supprimer vys1, car il est nécessaire pour la hiérarchie interne du pare-feu; vsys1 apparaît même sur les modèles de pare-feu qui ne supporte pas de multiples systèmes virtuels*

Vous pouvez limiter les allocations de ressources pour les sessions, règles et tunnels VPN autorisés pour le système virtuel et, par le fait même, contrôler les ressources du pare-feu. Chaque paramètre de ressource affiche la plage de valeurs valide; qui varie selon le modèle de pare-feu. Le paramètres par défaut est fixé sur 0, ce qui signifie que la limite du système virtuel est la limite du modèle de pare-feu. Cependant, la limite d'un paramètre spécifique n'est pas reproduite pour chaque système virtuel. Par exemple, si un pare-feu dispose de quatre systèmes virtuels, chaque système virtuel ne peut disposer du nombre total de règles de décryptage autorisées par pare-feu. Une fois que le nombre total de règles de décryptage pour tous les systèmes virtuels atteint la limite du pare-feu, vous ne pouvez en ajouter plus.

## Rôles administrateur des systèmes virtuels

Un administrateur **Superuser (super utilisateur)** peut créer des systèmes virtuels et ajouter un **Device administrator (Administrateur de périphérique)**, **vsysadmin (vsysadmin)** ou **vsysreader (vsysreader)**. Un **Device administrator (Administrateur de périphérique)** peut accéder à tous les systèmes virtuels, mais ne peut pas ajouter d'administrateurs. Lorsque vous créez un profil de rôle administrateur et que vous sélectionnez **Virtual System (Système virtuel)** en tant que rôle, le rôle

s'applique à des systèmes virtuels spécifiques du pare-feu. Dans l'onglet **Command Line (Ligne de commande)**, les deux types de rôles administrateur des systèmes virtuels sont les suivants :

- **vsysadmin** : a accès aux systèmes virtuels spécifiques du pare-feu pour créer et gérer des aspects particuliers des systèmes virtuels. Un administrateur de systèmes virtuels n'a pas accès aux interfaces de réseau, aux VLAN, aux câbles virtuels, aux routeurs virtuels, aux tunnels IPSec, aux tunnels GRE, à DHCP, au proxy Dns, à QoS, à LLDP ou aux profils réseaux. Les utilisateurs disposant de l'autorisation vsysadmin peuvent valider les configurations des systèmes virtuels qui leur sont attribués uniquement.
- **vsysreader** : a un accès en lecture seule aux systèmes virtuels spécifiques du pare-feu et aux aspects particuliers des systèmes virtuels. Un lecteur de systèmes virtuels n'a pas accès aux interfaces de réseau, aux VLAN, aux câbles virtuels, aux routeurs virtuels, aux tunnels IPSec, aux tunnels GRE, à DHCP, au proxy Dns, à QoS, à LLDP ou aux profils réseaux.

Un administrateur de système virtuel peut consulter les journaux des systèmes virtuels qui lui sont attribués uniquement. Un **Superuser (Superutilisateur)** ou un **Device administrator (Administrateur du périphérique)** peut voir tous les journaux, sélectionner un système virtuel à afficher ou configurer un système virtuel en tant que pôle User-ID.

## Objets partagés des systèmes virtuels

Si votre compte d'administrateur couvre plusieurs systèmes virtuels, vous pouvez décider de configurer des objets (comme un objet d'adresse) et des politiques pour un système virtuel spécifique ou en tant qu'objets partagés qui s'appliquent à tous les systèmes virtuels sur le pare-feu. Si vous tentez de créer un objet partagé avec les mêmes noms et types qu'un objet existant d'un système virtuel, l'objet du système virtuel est utilisé.

# Communication entre systèmes virtuels

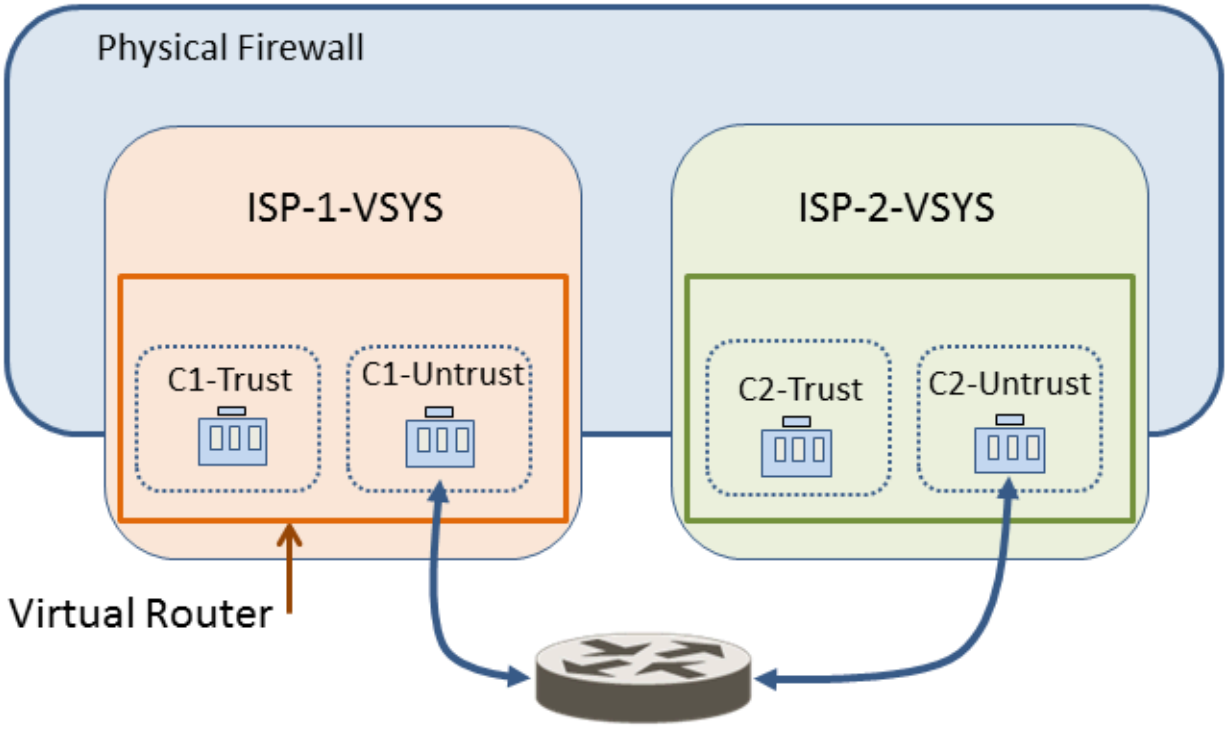
Deux scénarios typiques dans lesquels une communication entre systèmes virtuels (trafic inter-vsys) est souhaitable sont possibles. Dans un environnement à plusieurs clients, la communication entre systèmes virtuels peut être possible en laissant le trafic quitter le pare-feu, passer par Internet, puis revenir au pare-feu. Dans un environnement à une seule entreprise, la communication entre systèmes virtuels peut rester à l'intérieur du pare-feu. Cette section décrit les deux scénarios.

- Le trafic inter-VSYS doit quitter le pare-feu
- Le trafic inter-VSYS reste à l'intérieur du pare-feu
- La communication inter-VSYS utilise deux sessions

## Le trafic inter-VSYS doit quitter le pare-feu

Un ISP disposant de plusieurs clients sur un pare-feu (également appelé multi-clients) peut utiliser un système virtuel pour chaque client et permettre ainsi à chaque client de contrôler sa configuration de système virtuel. L'ISP accorde l'autorisation **vsysadmin (vsysadmin)** à ses clients. Le trafic et la gestion de chaque client sont isolés des autres. Chaque système virtuel doit être configuré avec une adresse IP propre et un ou plusieurs routeurs virtuels pour gérer le trafic et sa propre connexion à Internet.

Si les systèmes virtuels doivent communiquer entre eux, le trafic quitte le pare-feu vers un autre périphérique de routage de Couche 3 puis revient vers le pare-feu, même si les systèmes virtuels se trouvent sur le même pare-feu physique, comme illustré dans la figure suivante.



# Le trafic inter-VSYS reste à l'intérieur du pare-feu

Contrairement au scénario multi-clients ci-dessus, les systèmes virtuels d'un pare-feu peuvent être contrôlés par une seule et même entreprise. L'entreprise souhaite isoler le trafic entre les systèmes virtuels et autoriser les communications entre systèmes virtuels. Ce cas pratique courant se produit lorsque l'entreprise souhaite distinguer les services tout en leur permettant de communiquer les uns avec les autres ou de se connecter au ou aux mêmes réseaux. Dans ce scénario, le trafic inter-vsys reste à l'intérieur du pare-feu, comme décrit dans les rubriques suivantes :

- Zone externe
- Zones externes et politiques de sécurité pour le trafic dans un pare-feu

## Zone externe

La communication souhaitée dans le cas pratique ci-dessus est obtenue en configurant des politiques de sécurité qui pointent vers ou depuis une zone ***externe***. Une zone externe est un objet de sécurité associé à un système virtuel qu'il peut atteindre ; la zone est externe au système virtuel. Un système virtuel ne peut inclure qu'une seule zone externe, quel que soit le nombre de zones de sécurité contenues dans le système virtuel. Des zones externes sont requises pour autoriser le trafic entre les zones de différents systèmes virtuels sans que le trafic ne sorte du pare-feu.

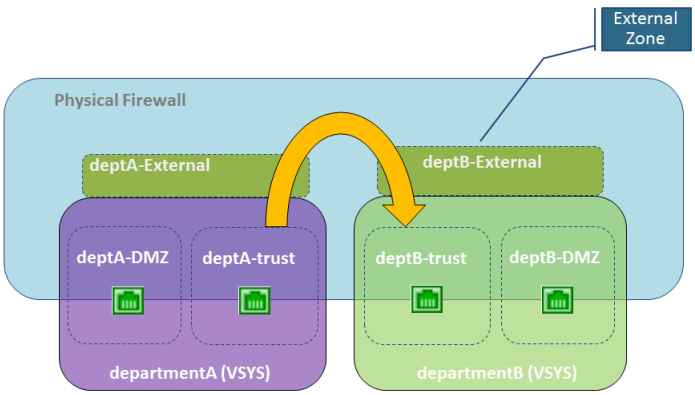
L'administrateur de système virtuel configure les politiques de sécurité nécessaires pour autoriser le trafic entre deux systèmes virtuels. Contrairement aux zones de sécurité, une zone externe n'est pas associée à une interface ; elle est associée à un système virtuel. La politique de sécurité autorise ou refuse le trafic entre la zone de sécurité (interne) et la zone externe.

Aucune interface ou adresse IP n'étant associée aux zones externes, certains profils de protection de zone ne sont pas pris en charge sur les zones externes.

N'oubliez pas que chaque système virtuel est une instance distincte d'un pare-feu, ce qui signifie que chaque paquet passant d'un système virtuel à un autre est inspecté pour l'évaluation de la politique de sécurité et de l'App-ID.

## Zones externes et politiques de sécurité pour le trafic dans un pare-feu

Dans l'exemple suivant, une entreprise comporte deux groupes administratifs distincts : les systèmes virtuels du serviceA et du serviceB. La figure suivante illustre la zone externe associée à chaque système virtuel, ainsi que le trafic entre une zone approuvée, en sortie d'une zone externe, et une zone externe d'un autre système virtuel, puis dans sa zone approuvée.



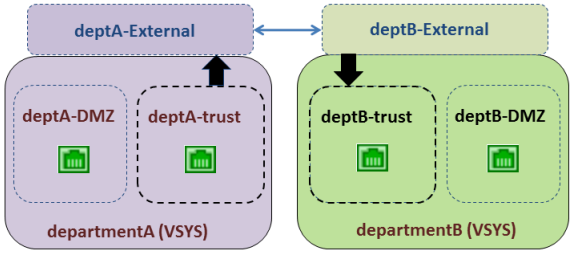
Pour pouvoir créer des zones externes, l'administrateur de pare-feu doit configurer les systèmes virtuels de sorte qu'ils soient mutuellement ***visibles***. Les zones externes n'incluent pas de politiques de sécurité entre elles car leurs systèmes virtuels sont visibles.

Pour permettre une communication entre systèmes virtuels, les interfaces d'entrée et de sortie du pare-feu sont soit associées à un routeur virtuel unique, soit connectées à l'aide d'itinéraires statiques entre routeurs virtuels. La plus simple de ces deux approches consiste à associer tous les systèmes virtuels qui doivent communiquer à un seul et même routeur virtuel.

Pour une quelconque raison, les systèmes virtuels devront peut-être disposer d'un routeur virtuel propre, s'ils utilisent des plages d'adresses IP se chevauchant par exemple. Le trafic peut être acheminé entre les systèmes virtuels, mais chaque routeur virtuel doit comprendre des itinéraires statiques qui pointent vers le ou les autres routeurs virtuels comme saut suivant.

Comme illustré dans le scénario sur la figure ci-dessus, une entreprise comporte deux groupes administratifs : serviceA et serviceB. Le groupe serviceA gère le réseau local et les ressources DMZ. Le groupe serviceB gère le trafic vers et depuis le segment commercial du réseau. L'ensemble du trafic se trouve sur un réseau local ; un seul routeur virtuel est donc utilisé. Deux zones externes sont configurées pour la communication entre deux systèmes virtuels. Le système virtuel de serviceA compte trois zones utilisées pour la politique de sécurité : servA-DMZ, servA-trust (approuvé) et servA-Externe. Le système virtuel de serviceB compte également trois zones : servB-DMZ, servB-trust (approuvé) et servB-Externe. Les deux groupes peuvent contrôler le trafic traversant leurs systèmes virtuels.

Pour autoriser le trafic de servA-trust (approuvé) vers servB-trust (approuvé), deux politiques de sécurité sont nécessaires. Dans la figure suivante, les deux flèches verticales indiquent où les politiques de sécurité (décrites sous la figure) contrôlent le trafic.




- Politique de sécurité 1 : Dans la figure ci-dessus, le trafic est destiné à la zone servB-trust (approuvé). Le trafic quitte la zone servA-trust (approuvé) et est transmis à la zone servA-Externe. Une politique de sécurité doit autoriser le trafic entre la zone source (servA-trust) et la zone de destination (servA-Externe). Un système virtuel autorise l'utilisation de tout type de politique pour ce trafic, NAT inclus.

  Aucune politique n'est nécessaire entre les zones externes car le trafic envoyé à une zone externe apparaît et dispose d'un accès automatique aux autres zones externes visibles pour la zone externe d'origine.
- Politique de Sécurité 2 : Dans la figure ci-dessus, le trafic provenant de servB-Externe est toujours destiné à la zone servB-trust (approuvé), et une politique de sécurité doit être configurée pour l'autoriser. La politique de sécurité doit autoriser le trafic entre la zone source (servB-Externe) et la zone de destination (servB-trust).

Le système virtuel de serviceB peut être configuré pour bloquer le trafic du système virtuel de serviceA, et vice-versa. Comme le trafic de toute autre zone, le trafic provenant de zones externes

doit être explicitement autorisé par une politique pour pouvoir parvenir à d'autres zones d'un système virtuel.

***Outre les zones externes nécessaires au trafic entre systèmes virtuels ne quittant pas le pare-feu, des zones externes sont également nécessaires si vous configurez une** passerelle partagée**, auquel cas le trafic est censé quitter le pare-feu.***

## La communication inter-VSYS utilise deux sessions

Il est utile de bien comprendre que la communication entre deux systèmes virtuels utilise deux sessions, contrairement à une seule session utilisée pour un seul système virtuel. Comparons les scénarios.

Scénario 1 : Vsys1 comporte deux zones : trust1 et untrust1. Un hôte dans la zone trust1 initie le trafic lorsqu'il doit communiquer avec un périphérique dans la zone untrust1. L'hôte envoie le trafic au pare-feu, et le pare-feu crée une nouvelle session pour la zone source trust1 vers la zone de destination untrust1. Une seule session est nécessaire pour ce trafic.

Scénario 2 : Un hôte de vsys1 doit accéder à un serveur sur vsys2. Un hôte dans la zone trust1 initie le trafic au pare-feu, et le pare-feu crée la première session : de la zone source trust1 vers la zone de destination untrust1. Le trafic est acheminé vers vsys2, en interne ou en externe. Le pare-feu crée ensuite une seconde session : zone source untrust2 vers la zone de destination trust2. Deux sessions sont nécessaires pour ce trafic entre systèmes virtuels.

# Passerelle partagée

Cette rubrique inclut les informations suivantes sur les passerelles partagées :

- Zones externes et passerelle partagée
- Remarques relatives à la mise en réseau d'une passerelle partagée

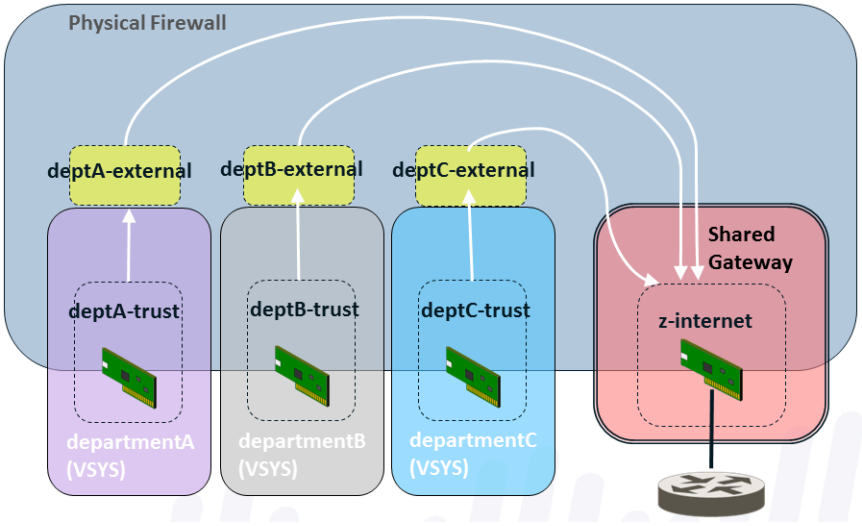
## Zones externes et passerelle partagée

Une passerelle partagée est une interface partagée par plusieurs systèmes virtuels pour communiquer via Internet. Chaque système virtuel requiert une Zone externe qui agit comme un intermédiaire pour configurer des politiques qui autorisent ou refusent le trafic de la zone interne du système virtuel vers la passerelle partagée.

La passerelle partagée utilise un routeur virtuel unique pour acheminer le trafic de tous les systèmes virtuels. Une passerelle partagée est utilisée lorsqu'une interface n'a pas besoin d'une limite administrative complète, ou lorsque plusieurs systèmes virtuels doivent partager une même connexion Internet. Ce second cas survient si un ISP ne fournit à une entreprise qu'une seule adresse IP (interface), mais où plusieurs systèmes virtuels ont besoin d'une communication externe.

Contrairement au comportement entre les systèmes virtuels, les évaluations de la politique de sécurité et de l'App-ID ne sont pas réalisées entre un système virtuel et une passerelle partagée. C'est pourquoi l'utilisation d'une passerelle partagée pour accéder à Internet implique moins de surcharge que la création d'un autre système virtuel.

Dans la figure suivante, trois clients partagent un pare-feu, mais une seule interface a accès à Internet. La création d'un autre système virtuel ajouterait une surcharge d'évaluation de l'App-ID et de la politique de sécurité pour le trafic envoyé à l'interface via le système virtuel ajouté. Pour ne pas avoir à ajouter un autre système virtuel, la solution consiste à configurer une passerelle partagée, comme illustré dans le diagramme suivant.




La passerelle partagée a une adresse IP pouvant être acheminée au niveau mondial et utilisée pour communiquer avec le monde extérieur. Les interfaces des systèmes virtuels ont également des adresses IP, mais il peut s'agir d'adresses IP privées et ne pouvant pas être acheminées.

Rappelez-vous qu'un administrateur doit spécifier si un système virtuel est visible pour les autres systèmes virtuels. Contrairement à un système virtuel, une passerelle partagée est toujours visible pour tous les systèmes virtuels du pare-feu.

Le numéro d'identifiant d'une passerelle partagée apparaît sous la forme **sg<ID>** sur l'interface Web. Il est recommandé de donner un nom à votre passerelle partagée qui inclut son numéro d'identifiant.

Lorsque vous ajoutez des objets, comme des zones et des interfaces, à une passerelle partagée, cette dernière apparaît comme un système virtuel disponible dans le menu des systèmes virtuels.

Une passerelle partagée est une version limitée d'un système virtuel ; elle prend en charge les politiques NAT, Policy-Based Forwarding (transfert basé sur une politique - PBF) et DoS, mais ne prend pas en charge les politiques de sécurité, QoS, décryptage, contrôle prioritaire sur l'application et authentification.

## Remarques relatives à la mise en réseau d'une passerelle partagée

Respectez les consignes suivantes lorsque vous configurez une passerelle partagée :

- Les systèmes virtuels dans un scénario de passerelle partagée accèdent à Internet via l'interface physique de la passerelle partagée à l'aide d'une adresse IP unique. Si les adresses IP des systèmes virtuels ne peuvent pas être acheminées au niveau mondial, configurez un NAT source pour convertir ces adresses en adresses IP pouvant être acheminées au niveau mondial.
- Un routeur virtuel achemine le trafic de tous les systèmes virtuels via la passerelle partagée.
- L'itinéraire par défaut des systèmes virtuels doit pointer vers la passerelle partagée.
- Des politiques de sécurité doivent être configurées pour chaque système virtuel pour autoriser le trafic entre la zone interne et la zone externe, qui est visible pour la passerelle partagée.
- Un administrateur de pare-feu doit contrôler le routeur virtuel de sorte qu'aucun membre d'un système virtuel n'affecte le trafic des autres systèmes virtuels.
- Dans un pare-feu Palo Alto Networks, un paquet peut passer d'un système virtuel à un autre ou à une passerelle partagée. Un paquet ne peut pas traverser plus de deux systèmes virtuels ou passerelles partagées. Par exemple, un paquet ne peut passer du système virtuel 1 au système virtuel 2 au système virtuel 3, ou du système virtuel 1 au système virtuel 2 à la passerelle partagée 1. Les deux exemples reposent sur plus de deux systèmes virtuels, ce qui n'est pas permis.

Pour gagner du temps et des efforts de configuration, prenez en compte les avantages suivants d'une passerelle partagée :

- Plutôt que de configurer NAT pour plusieurs systèmes virtuels associés à une passerelle partagée, vous pouvez configurer NAT pour la passerelle partagée.
- Plutôt que de configurer un routage basé sur une politique (PBR) pour plusieurs systèmes virtuels associés à une passerelle partagée, vous pouvez configurer PBR pour la passerelle partagée.

# Configuration de systèmes virtuels

La création d'un système virtuel nécessite que vous ayez ce qui suit à disposition :

- Un rôle administrateur **superuser (superutilisateur)**.
- Une interface configurée.
- Une licence Systèmes virtuels si vous créez plus que le nombre de base de systèmes virtuels pris en charge par la plate-forme. Reportez-vous à la section Prise en charge et licence de plate-forme des systèmes virtuels.

**STEP 1 |** Activez des systèmes virtuels.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les **General Settings (Paramètres généraux)**.
2. Cochez la case **Multi Virtual System Capability (Fonction de systèmes virtuels multiples)**, puis cliquez sur **OK (OK)**. Cette action entraîne une validation si vous la confirmez.

   Une fois les systèmes virtuels activés seulement, l'onglet **Device (Périphérique)** affiche les options **Virtual Systems (Systèmes virtuels)** et **Shared Gateways (Passerelles partagées)**.

**STEP 2 |** Créez un système virtuel.

1. Sélectionnez **Device (Périphérique)** > **Virtual Systems (Systèmes virtuels)**, cliquez sur **Add (Ajouter)**, et saisissez un **ID (ID)** pour le système virtuel, qui vient s'ajouter à « vsys » (plage comprise entre 1 et 255).

   *La valeur par défaut est **vsys1**. Vous ne pouvez supprimer vys1, car il est nécessaire pour la hiérarchie interne du pare-feu; vsys1 apparaît même sur les modèles de pare-feu qui ne supporte pas de multiples systèmes virtuels*
2. Sélectionnez **Allow forwarding of decrypted content (Autoriser le transfert de contenu crypté)** si vous souhaitez permettre au pare-feu de transférer du contenu décrypté à un service externe. Par exemple, vous devez activer cette option pour que le pare-feu puisse envoyer du contenu décrypté à WildFire pour analyse.
3. Donnez un **Name (Nom)** descriptif au système virtuel. Un maximum de 31 caractères alphanumériques, espace et trait de soulignement est autorisé.

**STEP 3 |** Associez des interfaces au système virtuel.

Les routeurs virtuels, les câbles virtuels ou les VLAN peuvent être déjà configurés ou vous pouvez les configurer ultérieurement, auquel cas vous spécifiez le système virtuel qui est associé à chacun.

1. Dans l'onglet **General (Général)**, sélectionnez un objet **DNS Proxy (Proxy DNS)** si vous souhaitez appliquer des règles de proxy DNS à l'interface.
2. Dans le champ **Interfaces (Interfaces)**, cliquez sur **Add (Ajouter)** pour saisir les interfaces ou sous-interfaces à associer au système virtuel. Une interface ne peut appartenir qu'à un seul système virtuel.
3. Suivez l'une des procédures suivantes en fonction du ou des types de déploiement dont vous avez besoin dans le système virtuel :
   - Dans le champ **VLAN (VLAN)**, cliquez sur **Add (Ajouter)** pour saisir le ou les VLAN à associer au système virtuel.
   - Dans le champ **Virtual Wires (Câbles virtuels)**, cliquez sur **Add (Ajouter)** pour saisir le ou les câbles virtuels à associer au système virtuel.
   - Dans le champ **Virtual Routers (Routeurs virtuels)**, cliquez sur **Add (Ajouter)** pour saisir le ou les routeurs virtuels à associer au système virtuel.
4. Dans le champ **Visible Virtual System (Système virtuel visible)**, vérifiez tous les systèmes virtuels qui doivent être visibles pour le système virtuel en cours de configuration. Ceci est nécessaire pour les systèmes virtuels qui doivent communiquer les uns avec les autres.

   Dans un scénario à plusieurs clients où des limites administratives strictes sont nécessaires, aucun système virtuel ne doit être vérifié.
5. Cliquez sur **OK**.

**STEP 4 |** (Facultatif) Limitez les allocations de ressources pour les sessions, règles et tunnels VPN autorisés pour le système virtuel. La possibilité de pouvoir allouer des limites par système virtuel vous permet de contrôler efficacement des ressources de pare-feu.

1. Dans l'onglet **Resource (Ressource)**, définissez éventuellement des limites pour un système virtuel. Chaque champ affiche la plage de valeurs valide; qui varie selon le modèle de pare-feu. Le paramètres par défaut est fixé sur 0, ce qui signifie que la limite du système virtuel est la limite du modèle de pare-feu. Cependant, la limite d'un paramètre spécifique n'est pas reproduite pour chaque système virtuel. Par exemple, si un pare-feu dispose de quatre systèmes virtuels, chaque système virtuel ne peut disposer du nombre total de règles de

décryptage autorisées par pare-feu. Une fois que le nombre total de règles de décryptage pour tous les systèmes virtuels atteint la limite du pare-feu, vous ne pouvez en ajouter plus.

- **Limite des sessions**

  *Si vous utilisez la commande show session meter de la CLI, vous obtenez le nombre maximal de sessions autorisé par plan de données, le nombre de sessions actuelles qui sont utilisées par le système virtuel et le nombre limité de session par système virtuel. Sur un pare-feu PA-5200 ou PA-7000 Series, le nombre de sessions actuelles qui sont utilisées peut être supérieur au nombre maximal de sessions configuré, puisque chaque système virtuel comporte plusieurs plans de données. La limite des sessions que vous avez configurée sur un pare-feu PA-5200 Series ou PA-7000 Series s'applique à chaque plan de données ; le nombre maximal par système virtuel sera donc supérieur.*

- **Règles de sécurité**
- **Règles NAT**
- **Règles de décryptage**
- **Règles de QoS**
- **Règles de contrôle prioritaire sur l'application**
- **Règles de transfert basées sur les politiques**
- **Règles d'authentification**
- **Règles de protection DoS**
- **Tunnels VPN de site à site**
- **Tunnels VPN SSL simultanés**

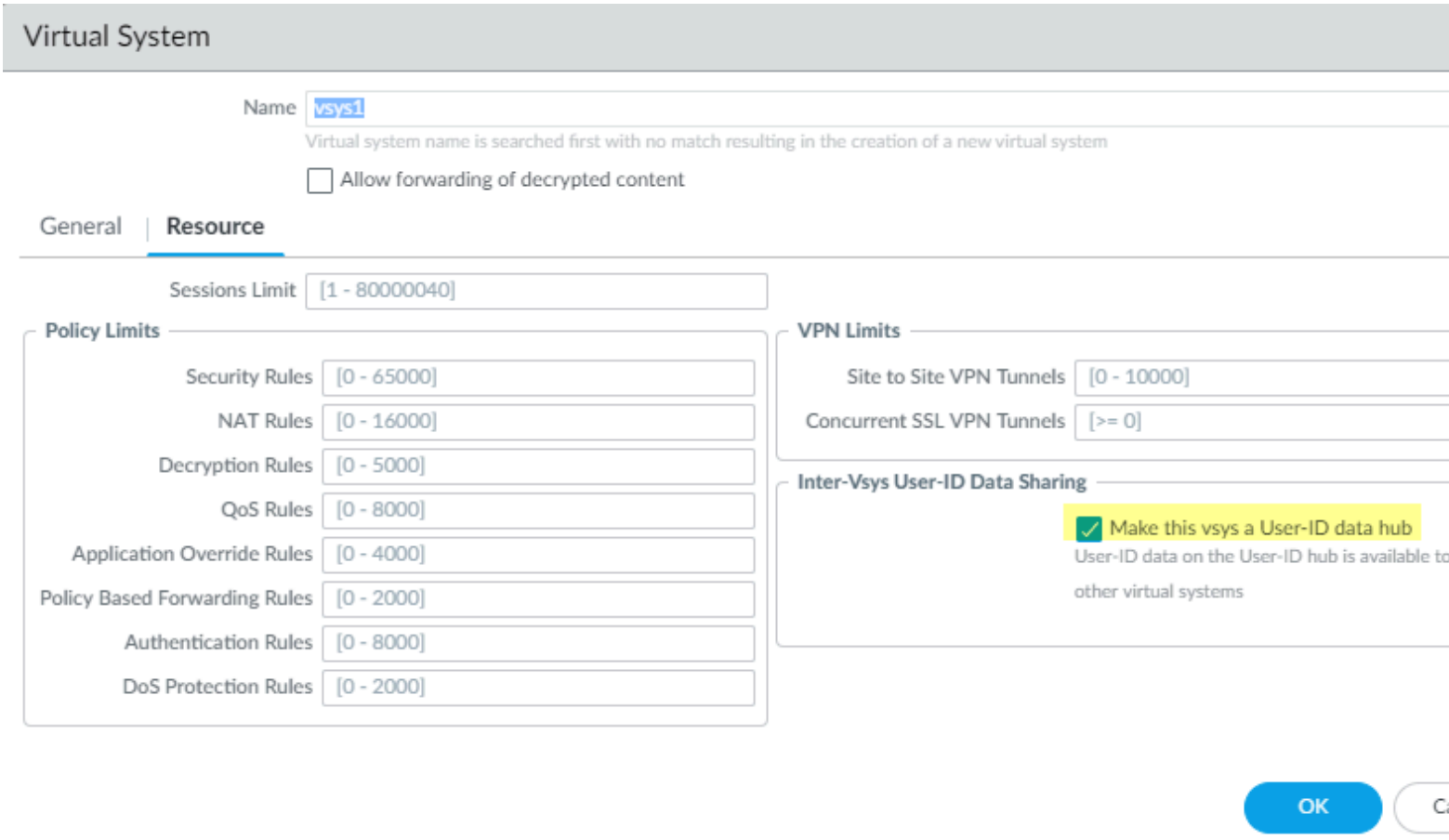
2. Cliquez sur **OK**.

**STEP 5 |** (Facultatif) Configurez un système virtuel en tant que pôle User-ID afin de Partage des mappages User-ID sur l'ensemble des systèmes virtuels.

*Les informations de mappage adresse IP et port/nom d'utilisateur obtenues auprès des agents Terminal Server et les données de mappage de groupe ne sont pas partagées entre le système virtuel faisant office de pôle et les systèmes virtuels connectés.*

1. Pour les systèmes virtuels existants, transférez la configuration des sources User-ID que vous souhaitez partager (comme les serveurs surveillés et les agents User-ID) au système virtuel qui fera office de pôle.
2. À l'onglet **Resource (Ressource)**, sélectionnez **Make this vsys a User-ID data hub (Faire de ce système virtuel un centre de données User-ID)**.

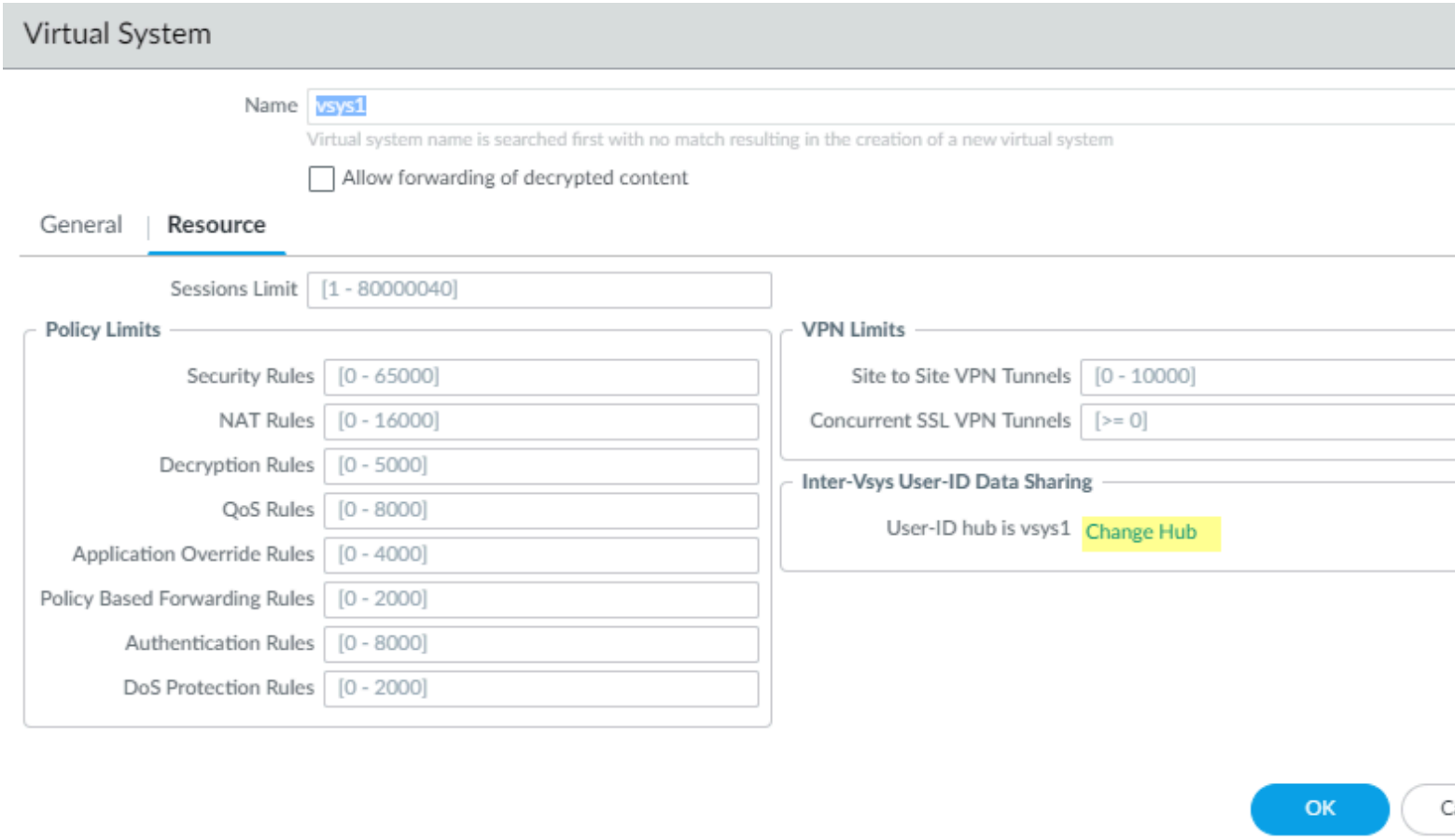



3. Cliquez sur **Yes (Oui)** pour confirmer, puis cliquez sur **OK**.

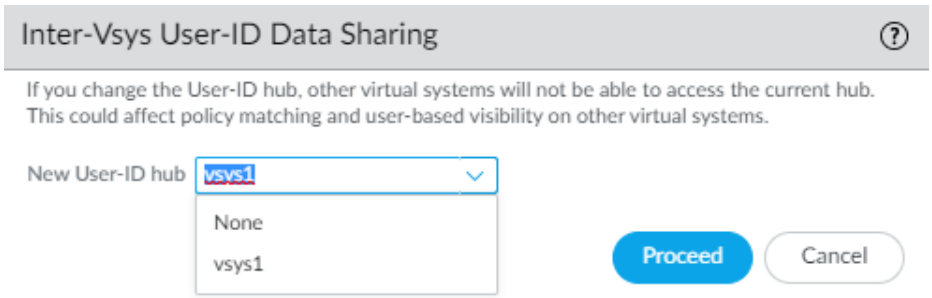
   Si vous souhaitez modifier le pôle User-ID If en spécifiant un autre système virtuel ou que vous souhaitez le désactiver, sélectionnez le système virtuel actuellement configuré en

tant que pôle User-ID, puis sélectionnez **Resource (Ressource)** > **Change Hub (Modifier le pôle)**.




Sélectionnez le **New User-ID hub (Nouveau pôle User-ID)** dans la liste, ou sélectionnez **none (aucun)** pour désactiver le pôle User-ID et cesser de partager les mappages sur l'ensemble des systèmes virtuels.




Cliquez sur **Proceed (Poursuivre)** pour confirmer, puis validez vos modifications.

**STEP 6 |** Commit (Validez) la configuration.

Cliquez sur **Commit (Valider)**. Le système virtuel est désormais un objet accessible dans l'onglet **Objects (Objets)**.

**STEP 7 |** Créez au moins un routeur virtuel pour le système virtuel pour que ce dernier puisse utiliser les fonctions de mise en réseau comme le routage statique ou dynamique.

Votre système virtuel peut également utiliser un VLAN ou un câble virtuel en fonction de votre déploiement.

1. Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et **Add (Ajoutez)** un routeur virtuel par **Name (Nom)**.
2. Pour **Interfaces (Interfaces)**, cliquez sur **Add (Ajouter)** puis sélectionnez les interfaces appartenant au routeur virtuel.
3. Cliquez sur **OK**.

**STEP 8 |** Configurez une zone de sécurité pour chaque interface du système virtuel.

Pour au moins une interface, créez une zone de sécurité de Couche 3. Reportez-vous à la section Configuration des interfaces et des zones.

**STEP 9 |** Configurez les règles de politique de sécurité autorisant ou refusant le trafic vers et depuis les zones du système virtuel.

Reportez-vous à la section Création d'une règle de politique de sécurité.

**STEP 10 |** Commit (Validez) la configuration.

Cliquez sur **Commit (Valider)**.

*Après avoir créé un système virtuel, vous pouvez utiliser la CLI pour valider une configuration pour un système virtuel spécifique uniquement :*

```
commit partial vsys <id-système virtuel>
```

**STEP 11 |** (Facultatif) Affichez les politiques de sécurité configurées pour un système virtuel.

Ouvrez une session SSH pour utiliser la CLI. Pour afficher les politiques de sécurité d'un système virtuel, en mode Opérationnel, utilisez les commandes suivantes :

```
set system setting target-vsys <id-système virtuel>
show running security-policy
```

# Configuration de la communication entre systèmes virtuels à l'intérieur du pare-feu

Effectuez cette tâche si vous disposez d'un cas pratique, dans une entreprise par exemple où vous souhaitez que les systèmes virtuels puissent communiquer entre eux à l'intérieur du pare-feu. Un tel scénario est décrit dans le document trafic entre des systèmes virtuels qui reste à l'intérieur du pare-feu. Cette tâche suppose que :

- vous avez effectué la tâche Configuration de systèmes virtuels.
- Lors de la configuration des systèmes virtuels, dans le champ **Visible Virtual System (Système virtuel visible)**, vous avez coché les cases de tous les systèmes virtuels qui doivent communiquer entre eux pour être visibles.

**STEP 1 |** Configurez une zone externe pour chaque système virtuel.

1. Sélectionnez **Network (Réseau)** > **Zones (Zones)** et cliquez sur **Add (Ajouter)** pour ajouter une nouvelle zone par **Name (Nom)**.
2. Pour **Location (Emplacement)**, sélectionnez le système virtuel pour lequel vous créez une zone externe.
3. Pour le **Type (Type)**, sélectionnez **External (Externe)**.
4. Pour **Virtual Systems (Systèmes virtuels)**, cliquez sur **Add (Ajouter)** et saisissez le système virtuel accessible à la zone externe.
5. (Facultatif) Sélectionnez un **Zone Protection Profile (Profil de protection de zone)** (ou configurez-en un ultérieurement) qui offre une protection contre la saturation, la reconnaissance ou les attaques basées sur le paquet.
6. (Facultatif) Sous **Log Setting (Paramètre de journal)**, sélectionnez un profil de transfert des journaux pour transférer les journaux de protection de zone vers un système externe.
7. (Facultatif) Cochez la case **Enable User Identification (Activer l'identification de l'utilisateur)** pour activer User-ID pour la zone externe.
8. Cliquez sur **OK**.

**STEP 2 |** Configurez les règles de politique de sécurité pour autoriser ou refuser le trafic des zones internes vers la zone externe du système virtuel, et vice-versa.

- Reportez-vous à la section Création d'une règle de politique de sécurité.
- Reportez-vous à la section Trafic inter-VSYS restant à l'intérieur du pare-feu.

**STEP 3 |** Validez vos modifications.

Cliquez sur **Commit (Valider)**.

# Configuration d'une passerelle partagée

Effectuez cette tâche si plusieurs systèmes virtuels doivent partager une interface (une passerelle partagée) vers Internet. Cette tâche suppose que :

- Vous avez configuré une interface avec une adresse IP pouvant être acheminée au niveau mondial, qui sera la passerelle partagée.
- Vous avez effectué la tâche précédente : Configuration de systèmes virtuels. Pour l'interface, vous avez choisi l'interface orientée vers l'extérieur avec l'adresse IP pouvant être acheminée au niveau mondial.
- Lors de la configuration des systèmes virtuels, dans le champ **Visible Virtual System (Système virtuel visible)**, vous avez coché les cases de tous les systèmes virtuels qui doivent communiquer pour être visibles entre eux.

**STEP 1 |** Configurez une passerelle partagée.

1. Sélectionnez **Device (Périphérique)** > **Shared Gateway (Passerelle partagée)**, cliquez sur **Add (Ajouter)** et saisissez un **ID (ID)**.
2. Donnez un **Name (Nom)** explicite, qui inclut de préférence l'**ID (ID)** de la passerelle.
3. Dans le champ **DNS Proxy (Proxy DNS)**, sélectionnez un objet de proxy DNS si vous souhaitez appliquer des règles de proxy DNS à l'interface.
4. **Add (Ajoutez)** une **Interface (Interface)** connectée au monde extérieur.
5. Cliquez sur **OK**.

**STEP 2 |** Configurez la zone pour la passerelle partagée.

*Lors de l'ajout d'objets, comme des zones ou des interfaces, à une passerelle partagée, cette dernière apparaît comme un système virtuel disponible dans le menu **VSYS (VSYS)**.*

1. Sélectionnez **Network (Réseau)** > **Zones (Zones)** et cliquez sur **Add (Ajouter)** pour ajouter une nouvelle zone par **Name (Nom)**.
2. Pour **Location (Emplacement)**, sélectionnez la passerelle partagée pour laquelle vous créez une zone externe.
3. Pour le **Type (Type)**, sélectionnez **Layer3 (Couche 3)**.
4. (Facultatif) Sélectionnez un **Zone Protection Profile (Profil de protection de zone)** (ou configurez-en un ultérieurement) qui offre une protection contre la saturation, la reconnaissance ou les attaques basées sur le paquet.
5. (Facultatif) Sous **Log Setting (Paramètre de journal)**, sélectionnez un profil de transfert des journaux pour transférer les journaux de protection de zone vers un système externe.
6. (Facultatif) Sélectionnez **Enable User Identification (Activer l'identification de l'utilisateur)** pour activer User-ID pour la passerelle partagée.
7. Cliquez sur **OK**.

**STEP 3 |** Validez vos modifications.

Cliquez sur **Commit (Valider)**.

# Personnalisation d'itinéraires de service pour un système virtuel

Lorsque plusieurs systèmes virtuels sont activés sur un pare-feu, les systèmes virtuels héritent des paramètres de service et d'itinéraire de service globaux du pare-feu. Par exemple, le pare-feu peut utiliser un serveur de messagerie partagé pour envoyer des alertes par e-mail à tous les systèmes virtuels. Dans certains cas, vous aimeriez pouvoir créer des itinéraires de service différents pour chaque système virtuel.

Un cas pratique de configuration d'itinéraires de service au niveau du système virtuel est si vous êtes un ISP qui doit prendre en charge plusieurs locataires individuels sur un même pare-feu Palo Alto Networks. Chaque locataire a besoin d'itinéraires de service personnalisés pour accéder à des services comme DNS, Kerberos, LDAP, NetFlow, RADIUS, TACACS+, authentification à facteurs multiples, courrier électronique, piège SNMP, Syslog, HTTP, agent User-ID, VM Monitor et Panorama (déploiement des mises à jour logicielles et de contenu). Un autre cas pratique est une entreprise informatique souhaitant offrir une autonomie totale aux groupes qui définissent des serveurs pour des services. Chaque groupe peut disposer d'un serveur virtuel et définir ses propres itinéraires de service.

***Vous pouvez sélectionner un routeur virtuel pour un itinéraire de service dans un système virtuel ; vous ne pouvez pas sélectionner l'interface de sortie. Après avoir sélectionné le routeur virtuel et que le pare-feu a envoyé le paquet du routeur virtuel, le pare-feu sélectionne l'interface de sortie en fonction de l'adresse IP de destination. Ainsi, si un système virtuel comporte plusieurs routeurs virtuels, les paquets vers tous les serveurs d'un service ne doivent provenir que d'un seul routeur virtuel. Un paquet avec une adresse source d'interface peut provenir d'une autre interface, mais le trafic de retour se trouvera sur l'interface avec l'adresse IP source, générant ainsi un trafic asymétrique.***

- Personnalisation d'itinéraires de service vers des services pour systèmes virtuels
- Configuration d'un pare-feu PA-7000 Series pour la journalisation par système virtuel
- Configuration de l'accès administratif par système virtuel ou pare-feu

## Personnalisation d'itinéraires de service vers des services pour systèmes virtuels

Lorsque vous activez l'option Multi Virtual System Capability (Fonction de systèmes virtuels multiples), tout système virtuel pour lequel aucun itinéraire de service spécifique n'est configuré hérite des paramètres de service et d'itinéraire de service globaux du pare-feu. Vous pourriez plutôt choisir de configurer un système virtuel pour qu'il utilise un itinéraire de service différent, comme le décrit le flux de travail suivant.

Un pare-feu avec plusieurs systèmes virtuels doit comporter des interfaces et sous-interfaces avec des adresses IP qui ne se chevauchent pas. Un itinéraire de service par système virtuel pour les pièges SNMP ou pour Kerberos s'applique à IPv4 uniquement.

L'itinéraire d'un service suit strictement la manière dont vous avez configuré le profil de serveur du service :

- Si vous définissez un profil de serveur (**Device (Périphérique)** > **Server Profiles (Profils de serveur)**) pour l'emplacement partagé, le pare-feu utilise l'itinéraire de service global pour ce service.
- Si vous définissez un profil de serveur pour un système virtuel donné, le pare-feu utilise l'itinéraire de service propre au système virtuel pour ce service.
- Si vous définissez un profil de serveur pour un système virtuel donné, mais que l'itinéraire de service propre à ce système virtuel n'est pas configuré, le pare-feu utilise l'itinéraire de service global pour ce service.

*Le pare-feu prend en charge le transfert des messages Syslog par système virtuel. Lorsque plusieurs systèmes virtuels d'un pare-feu se connectent à un serveur Syslog via SSL, le pare-feu ne peut générer qu'un seul certificat pour la communication sécurisée. Le pare-feu ne prend pas en charge chaque système virtuel disposant d'un certificat propre.*

**STEP 1 |** Personnalisez des itinéraires de service pour un système virtuel.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Services (Services)** > **Virtual Systems (Systèmes virtuels)** et choisissez le système virtuel que vous souhaitez configurer.
2. Cliquez sur le lien **Service Route Configuration (Configuration de l'itinéraire de service)**.
3. Sélectionnez parmi les choix suivants :
   - **Inherit Global Service Route Configuration (Hériter de la configuration d'itinéraire de service globale)** : le système virtuel hérite des paramètres de l'itinéraire de service global correspondant à un système virtuel. Si vous sélectionnez cette option, sautez l'étape consacrée à la personnalisation.
   - **Customize (Personnaliser)** : vous permet de spécifier une adresse source pour chaque service.
4. Si vous avez choisi **Customize (Personnaliser)**, sélectionnez l'onglet **IPv4 (IPv4)** ou **IPv6 (IPv6)**, en fonction du type d'adressage proposé par le serveur utilisé par le service. Vous pouvez spécifier des adresses IPv4 et IPv6 pour un service. Cliquez sur un service. (Seuls les services associés à un système virtuel sont disponibles.)

   *Pour facilement utiliser la même adresse source pour plusieurs services, cochez la case des services, cliquez sur **Set Selected Routes (Définir les itinéraires sélectionnés)**, puis continuez.*

   - Pour restreindre la liste Source Address (Adresse source), sélectionnez une **Source Interface (Interface source)**, puis sélectionnez une adresse source (de cette interface) en tant qu'itinéraire de service. Si vous sélectionnez **Any (Indifférent)** pour Source Interface (Interface source), toutes les adresses IP de toutes les interfaces du système virtuel seront disponibles dans la liste Source Address (Adresse source) à partir de laquelle vous sélectionnez une adresse. Vous pouvez sélectionner **Inherit Global Setting (Hériter des paramètres généraux)**.
   - La **Source Address (Adresse source)** indiquera **Inherited (Hérité)** si vous avez sélectionné **Inherit Global Setting (Hériter des paramètres généraux)** pour la **Source Interface (Interface source)** ou indiquera l'adresse source sélectionnée. Si vous avez sélectionné **Any (Indifférent)** pour **Source Interface (Interface source)**, sélectionnez

une adresse IP (au format IPv4 ou IPv6 correspondant à l'onglet sélectionné) pour spécifier l'adresse source qui sera utilisée dans les paquets envoyés au service externe.

- Si vous modifiez un objet d'adresse et si le type de famille d'adresses IP (IPv4/IPv6) change, **Commit (Valider)** est nécessaire pour mettre à jour la famille d'itinéraires de service à utiliser.

5. Cliquez sur **OK**.
6. Répétez les étapes précédentes pour configurer les adresses sources d'autres services externes.
7. Cliquez sur **OK**.

**STEP 2 |** Validez vos modifications.

Cliquez sur **Commit (Valider)** puis sur **OK (OK)**.

Si vous configurez des itinéraires de service par système virtuel pour des services de journalisation d'un pare-feu PA-7000 Series, procédez à la Configuration d'un pare-feu PA-7000 Series pour la journalisation par système virtuel.

## Configuration d'un pare-feu PA-7000 Series pour la journalisation par système virtuel

Pour les types de journaux Trafic, Correspondance HIP, Menaces et WildFire, le pare-feu PA-7000 Series n'utilise pas d'itinéraires de service pour les pièges SNMP, Syslog et la messagerie. Quant au pare-feu PA-7000 Series, il prend en charge une carte de journalisation.

Selon la configuration de votre pare-feu, vous pourriez disposer de l'un des types de cartes suivants :

- **Log Processing Card (carte de traitement des journaux - LPC)** : prend en charge des chemins spécifiques au système virtuel de sous-interfaces LPC vers un commutateur sur site en direction du service correspondant sur un serveur. Pour les journaux système et de configuration, le pare-feu PA-7000 Series utilise des itinéraires de service globaux, et non la LPC. Si une LPC est installée sur votre pare-feu, vous devez configurer un port de carte de traitement des journaux.
- **Log Forwarding Card (carte de transfert des journaux ; LFC)** : prend en charge le transfert haute vitesse des journaux de tous les journaux de plans de données vers un collecteur de journaux externe (par exemple, Panorama et serveurs Syslog). Vous pouvez créer et configuration des sous-interfaces pour les systèmes virtuels. Si une LFC est installée sur votre pare-feu, vous n'avez pas à configurer de port de carte de traitement des journaux.

Dans d'autres modèles Palo Alto Networks, le plan de données envoie le trafic d'itinéraire de service de journalisation au plan de gestion, qui transmet le trafic à des serveurs de journalisation. Dans un pare-feu PA-7000 Series, la LPC ou la LFC ne comporte qu'une seule interface, et les plans de données des différents systèmes virtuels envoient le trafic du serveur de journalisation (des types indiqués ci-dessus) à la carte de journalisation du pare-feu PA-7000 Series. La carte de journalisation est configurée avec plusieurs sous-interfaces, auxquelles la plate-forme envoie le trafic de service de journalisation à partir d'un commutateur du client, qui peut être connecté à plusieurs serveurs de journalisation.

Chaque sous-interface peut être configurée avec un nom de sous-interface et un numéro de sous-interface à points. La sous-interface est affectée à un système virtuel qui est configuré pour les services de journalisation. Les autres itinéraires de service sur un pare-feu PA-7000 Series fonctionnent comme les itinéraires de service sur d'autres plates-formes Palo Alto Networks. Pour

plus d'informations sur la LPC ou la LFC, reportez-vous au Guide de référence du matériel PA-7000 Series.

- Configuration de la LPC d'un pare-feu PA-7000 Series pour la journalisation par système virtuel
- Configuration de la LFC d'un pare-feu PA-7000 Series pour la journalisation par système virtuel

## Configuration de la LPC d'un pare-feu PA-7000 Series pour la journalisation par système virtuel

Si vous avez activé la fonction de systèmes virtuels multiples sur un pare-feu PA-7000 sur lequel une Log Processing Card (carte de traitement des journaux ; LPC) est installée, vous pouvez configurer la connexion à différents systèmes virtuels, comme l'illustre le flux de travail suivant.

**STEP 1 |** Créez une sous-interface de carte de journal.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)** et choisissez l'interface qui fera office d'interface de carte de journal.
2. Saisissez le **Interface Name (Nom de l'interface)**.
3. Sous **Interface Type (Type d'interface)**, sélectionnez **Log Card (Carte de journal)**.
4. Cliquez sur **OK**.

**STEP 2 |** Ajoutez une sous-interface pour chaque locataire sur l'interface physique de la LPC.

1. Mettez en évidence l'interface Ethernet dont le type est Carte de journal, puis cliquez sur **Add Subinterface (Ajouter une sous-interface)**.
2. Pour **Interface Name (Nom de l'interface)**, après le point, saisissez la sous-interface associée au système virtuel du locataire.
3. Pour **Tag (Étiquette)**, saisissez une valeur d'étiquette VLAN.

   *Donnez à l'étiquette le même numéro que la sous-interface pour simplifier l'utilisation, mais vous pouvez lui donner un autre numéro.*
4. (Facultatif) Saisissez un **Comment (Commentaire)**.
5. Dans l'onglet **Config (Configuration)**, dans le champ **Assign Interface to Virtual System (Associer l'interface au système virtuel)**, sélectionnez le système virtuel auquel la sous-interface LPC est associée. Vous pouvez également cliquer sur **Virtual Systems (Systèmes virtuels)** pour ajouter un nouveau système virtuel.
6. Cliquez sur **OK**.

**STEP 3 |** Saisissez l'adresse associée à la sous-interface, puis configurez la passerelle par défaut.

1. Dans l'onglet **Log Card Forwarding (Transfert de la carte de journal)**, effectuez l'une des deux actions suivantes ou les deux :
   - Dans la section IPv4, saisissez l'**IP Address (Adresse IP)** et le **Netmask (Masque réseau)** affectés à la sous-interface. Saisissez la **Default Gateway (Passerelle par défaut)** (le saut suivant où les paquets sans adresse de saut suivant connue dans la Routing Information Base (base d'informations de routage ; RIB) seront envoyés).
   - Dans la section IPv6, saisissez la **IPv6 Address (Adresse IPv6)** associée à la sous-interface. Saisissez la **IPv6 Default Gateway (Adresse IPv6 de passerelle par défaut)**.
2. Cliquez sur **OK**.

**STEP 4 |** Validez vos modifications.

Cliquez sur **OK**, puis sur **Commit (Valider)**.

**STEP 5 |** Si vous ne l'avez pas déjà fait, configurez les autres itinéraires de service du système virtuel.

Personnalisation d'itinéraires de service pour un système virtuel.

## Configuration de la LFC d'un pare-feu PA-7000 Series pour la journalisation par système virtuel

Si vous avez activé la fonction de systèmes virtuels multiples (multi-vsys) sur un pare-feu PA-7000 sur lequel une Log Forwarding Card (carte de transfert des journaux ; LFC) est installée, vous pouvez configurer la connexion à différents systèmes virtuels.

*Vous pouvez choisir de configurer uniquement l'interface physique. Si vous ne créez pas de sous-interfaces, chaque système virtuel utilise l'interface physique unique non balisée.*

Pour configurer une sous-interface distincte pour chaque système virtuel, ajoutez des sous-interfaces à l'interface physique et affectez la balise nécessaire pour segmenter le trafic de sous-interface.

*Pour un pare-feu de la série PA-7000 géré par un serveur d'administration Panorama, vous ne pouvez pas remplacer ou rétablir la configuration LFC localement sur le pare-feu si la configuration LFC est poussée à partir de Panorama. Pour remplacer la configuration LFC poussée à partir de Panorama, vous devez vous* log in to the firewall CLI (connecter à l'interface de ligne de commande) *du pare-feu et supprimer la configuration poussée de Panorama.*

```
admin> configure
```

```
admin# delete deviceconfig log-fwd-card
```

```
admin# commit
```

*Après avoir supprimé avec succès la configuration LFC poussée à partir de Panorama,* log in to the firewall web interface (connectez-vous à l'interface Web du pare-feu) *et continuez avec les étapes décrites ci-dessous.*

**STEP 1 |** Créez une sous-interface de carte de transfert des journaux.

1. Sélectionnez **Device (Périphérique)** > **Log Forwarding Card (Carte de transfert des journaux)** et ajoutez un sous-interface.
2. Pour **Interface Name (Nom de l'interface)**, après le point, saisissez la sous-interface associée au système virtuel du locataire.
3. (Facultatif) Saisissez un **Comment (Commentaire)**.
4. Pour **Tag (Étiquette)**, saisissez une valeur d'étiquette VLAN.

   *Donnez à l'étiquette le même numéro que la sous-interface pour simplifier l'utilisation, mais vous pouvez lui donner un autre numéro.*
5. Dans l'onglet **Config (Configuration)**, dans le champ **Assign Interface to Virtual System (Associer l'interface au système virtuel)**, sélectionnez le système virtuel auquel la sous-interface LFC est associée. Vous pouvez également cliquer sur **Virtual Systems (Systèmes virtuels)** pour ajouter un nouveau système virtuel.
6. Cliquez sur **OK**.

**STEP 2 |** (Facultatif) Saisissez l'adresse associée à la sous-interface, puis configurez la passerelle par défaut.

1. Dans l'onglet **Network (Réseau)**, effectuez l'une des deux actions suivantes ou les deux :
   - Dans la section IPv4, saisissez l'**IP Address (Adresse IP)** et le **Netmask (Masque réseau)** affectés à la sous-interface. Saisissez la **Default Gateway (Passerelle par défaut)** (le saut suivant où les paquets sans adresse de saut suivant connue dans la Routing Information Base (base d'informations de routage ; RIB) seront envoyés).
   - Dans la section IPv6, saisissez la **IPv6 Address (Adresse IPv6)** associée à la sous-interface. Saisissez la **IPv6 Default Gateway (Adresse IPv6 de passerelle par défaut)**.
2. Cliquez sur **OK**.

**STEP 3 |** Validez vos modifications.

Cliquez sur **OK**, puis sur **Commit (Valider)**.

## Configuration de l'accès administratif par système virtuel ou pare-feu

Si vous disposez d'un compte administratif super utilisateur, vous pouvez créer et configurer des autorisations granulaires pour un rôle vsysadmin ou device admin.

**STEP 1 |** Créez un profil de rôle administrateur qui active ou désactive l'autorisation pour un administrateur de configuration ou de lecture seule de différentes zones de l'interface Web.

1. Sélectionnez **Device (Périphérique)** > **Admin Roles (Rôles administrateur)** et cliquez sur **Add (Ajouter)** pour ajouter un **Admin Role Profile (Profil de rôle administrateur)**.
2. Saisissez un **Name (Nom)** et une **Description (Description)** (facultatif) pour le profil.
3. Pour **Role (Rôle)**, spécifiez le niveau de contrôle appliqué par le profil :
   - **Device (Périphérique)** : le profil permet de gérer les paramètres généraux et tous les systèmes virtuels.
   - **Virtual System (Système virtuel)** : le profil permet de ne gérer que le(s) système(s) virtuel(s) affecté(s) au(x) administrateur(s) ayant ce profil. (L'administrateur aura accès à

**Device (Périphérique)** > **Setup (Configuration)** > **Services (Services)** > **Virtual Systems (Systèmes virtuels)**, mais pas à l'onglet **Global**.)

4. Dans l'onglet **Web UI (IU Web)** du profil de rôle administrateur, faites défiler vers le bas pour accéder à **Device (Périphérique)** et laissez la coche verte (Activer).
   - Sous **Device (Périphérique)**, cochez **Setup (Configuration)** . Sous **Setup (Configuration)**, cochez les zones pour lesquelles ce profil accorde l'autorisation de configuration à l'administrateur, comme illustré ci-dessous. (L'icône de verrouillage Lecture seule apparaît dans le bouton à bascule Activer/Désactiver si Lecture seule est autorisé pour ce paramètre.)
     - **Management (Gestion)** : autorise un administrateur ayant ce profil à configurer des paramètres de l'onglet **Management (Gestion)**.
     - **Operations (Opérations)** : autorise un administrateur ayant ce profil à configurer des paramètres de l'onglet **Operations (Opérations)**.
     - **Services (Services)** : autorise un administrateur ayant ce profil à configurer des paramètres de l'onglet **Services (Services)**. **Services (Services)** doit être coché pour qu'un administrateur puisse accéder à l'onglet **Device (Périphérique)** > **Setup Services (Services de configuration)** > **Virtual Systems (Systèmes virtuels)**. Si **Role (Rôle)** a été défini sur **Virtual System (Système virtuel)** à l'étape précédente, **Services (Services)** est le seul paramètre pouvant être activé sous **Device (Périphérique)** > **Setup (Configuration)**.
     - **Content-ID (Content-ID)** : autorise un administrateur ayant ce profil à configurer des paramètres de l'onglet **Content-ID (Content-ID)**.
     - **WildFire (WildFire)** : autorise un administrateur ayant ce profil à configurer des paramètres de l'onglet **WildFire (WildFire)**.
     - **Session (Session)** : autorise un administrateur ayant ce profil à configurer des paramètres de l'onglet **Session (Session)**.
     - **HSM (HSM)** : autorise un administrateur ayant ce profil à configurer des paramètres de l'onglet **HSM (HSM)**.
5. Cliquez sur **OK**.
6. (Facultatif) Répétez l'ensemble de l'étape pour créer un autre profil de rôle administrateur avec d'autres autorisations, si nécessaire.

**STEP 2 |** Appliquez le profil de rôle Administrateur à un administrateur.

1. Sélectionnez **Device (Périphérique)** > **Administrators (Administrateurs)**, cliquez sur **Add (Ajouter)**, et saisissez un **Name (Nom)** pour ajouter un Administrateur.
2. (Facultatif) Sélectionnez un **Authentication Profile (Profil d'authentification)**.
3. (Facultatif) Sélectionnez **Use only client certificate authentication (Web) (Utiliser uniquement l'authentification du certificat client (Web))** pour disposer de l'authentification bidirectionnelle afin d'atteindre le serveur pour authentifier le client.
4. Saisissez un **Password (Mot de passe)** et **Confirm Password (Confirmez le mot de passe)**.
5. (Facultatif) Sélectionnez **Use Public Key Authentication (SSH) (Utiliser l'authentification de clé publique (SSH))** si vous souhaitez utiliser une méthode d'authentification renforcée basée sur une clé à l'aide d'une clé publique SSH au lieu d'un seul mot de passe.
6. Pour **Administrator Type (Type d'administrateur)**, sélectionnez **Role Based (Basé sur le rôle)**.
7. Pour **Profile (Profil)**, sélectionnez le profil que vous venez de créer.
8. (Facultatif) Sélectionnez un **Password Profile (Profil de mot de passe)**.
9. Cliquez sur **OK**.

**STEP 3 |** Commit (Validez) la configuration.

Cliquez sur **Commit (Valider)**.

# Compatibilité du système virtuel avec d'autres fonctionnalités

De nombreuses fonctionnalités et fonctions du pare-feu peuvent être configurées, affichées, consignées ou rapportées par système virtuel. Les systèmes virtuels sont donc mentionnés à d'autres endroits pertinents de la documentation et ces informations ne sont pas reprises ici. Certains des chapitres spécifiques sont les suivants :

- Si vous configurez la HA active/passive, les deux pare-feu doivent comporter la même capacité de systèmes virtuels (un ou plusieurs systèmes virtuels). Reportez-vous à la section Haute disponibilité.
- Pour configurer la QoS pour les systèmes virtuels, reportez-vous à la section Configuration de la QoS pour un système virtuel.
- Pour plus d'informations sur la configuration d'un pare-feu avec des systèmes virtuels dans un déploiement filaire virtuel utilisant des sous-interfaces (et des étiquettes VLAN), reportez-vous à la section Virtual Wire Interfaces (interfaces virtuelles Wire).
- Si vous avez configuré User-ID et plusieurs systèmes virtuels, vous pouvez partager les mappages d'utilisateurs sur l'ensemble des systèmes virtuels. Reportez-vous à la section Partage des mappages User-ID sur l'ensemble des systèmes virtuels.

# Protection de zone et protection DoS

La segmentation du réseau en zones fonctionnelles et organisationnelles réduit la surface d'attaque du réseau (la portion du réseau exposée aux agresseurs éventuels). La protection de zone défend les zones de votre réseau contre les attaques par saturation, les tentatives de reconnaissance, les attaques basées sur les paquets et les attaques qui utilisent des protocoles non-IP. Personnalisez un profil de protection de zone pour protéger chaque zone (vous pouvez appliquer le même profil à des zones similaires). La protection Denial-Of-Service (déni de service - DoS) défend des systèmes critiques spécifique contre les attaques par saturation, tout particulièrement les périphériques auxquels l'utilisateur accède depuis l'Internet, comme les serveurs Web et les serveurs de base de données, et protège les ressources des attaques par saturation de session. Personnalisez des règles de politique et des profils de protection DoS pour protéger chaque ensemble de périphériques critiques. Visitez le portail de la documentation sur les pratiques exemplaires pour obtenir une liste de vérification des pratiques exemplaires relatives à la protection DoS et à la protection de zone.

*Vérifiez et surveillez la consommation CPU du plan de données du pare-feu afin de vous assurer que chaque pare-feu est correctement dimensionné pour soutenir la protection DoS et la protection de la Zone et d'autres fonctions qui consomment les cycles CPU, telles que le déchiffrement. Si vous utilisez Panorama pour gérer vos pare-feu, utilisez la surveillance des périphériques (**Panorama** > **Managed Devices (Périphériques gérés)** > **Health (Santé)**) pour vérifier et surveiller la consommation du processeur de tous les pare-feu gérés d'une seule fois.*

# Segmentation du réseau à l'aide de Zones

Plus votre réseau est vaste, plus il est difficile à protéger. Un réseau vaste et non segmenté possède une grande surface d'attaque qui peut être difficile à gérer et à protéger. Puisque le trafic et les applications ont accès à la totalité du réseau, lorsqu'un pirate parvient à accéder à un réseau, celui-ci peut se déplacer latéralement à l'échelle du réseau pour accéder à des données essentielles. Un vaste réseau est également plus difficile à surveiller et à contrôler. La segmentation du réseau restreint la capacité du pirate à se déplacer dans le réseau en empêchant les déplacements latéraux entre les zones.

Une zone de sécurité est un groupe qui se compose de une ou plusieurs interfaces de pare-feu physiques ou virtuelles et des segments de réseau qui sont connectés aux interfaces de la zone. Vous contrôlez la protection de chaque zone de manière individuelle. Ainsi, chaque zone reçoit la protection particulière dont elle a besoin. Par exemple, il se peut qu'une zone dédiée au service des finances n'ait pas à autoriser toutes les applications qu'une zone propre au service des technologies de l'information autorise.

Pour protéger pleinement votre réseau, tout le trafic doit transiter par le pare-feu. Procédez à la Configuration des interfaces et des zones pour créer des zones distinctes pour des secteurs fonctionnels différents, comme la passerelle Internet, le stockage de données de nature délicate et les applications d'entreprise, et pour des groupes organisationnels différents, comme les finances, les technologies de l'information, le marketing et l'ingénierie. Lorsqu'il y a une division logique d'une fonctionnalité, de l'utilisation d'une application ou des privilèges d'accès des utilisateurs, vous pouvez créer une zone distincte pour isoler et protéger la zone et appliquer des règles de politique de sécurité pour empêcher l'accès non nécessaire aux données et aux applications auxquels un seul un ou certains des groupes doivent avoir accès. Plus les zones sont granulaires, plus vous avez une grande visibilité et un grand contrôle du trafic du réseau. La division de votre réseau en zones vous aide à créer une architecture Confiance Zéro qui respecte une philosophie de sécurité selon laquelle la confiance n'est accordée à aucun utilisateur, à aucun périphérique, à aucune application ou à aucun paquet, et tout doit être vérifié. L'objectif ultime consiste à créer un réseau qui n'autorise l'accès qu'aux utilisateurs, aux périphériques et aux applications qui ont des besoins d'entreprise légitimes, et à refuser tout autre trafic.

La façon de restreindre et d'autoriser de manière appropriée l'accès aux zones dépend de l'environnement réseau. Par exemple, les environnements tels que les ateliers de fabrication de semi-conducteurs ou les ateliers d'assemblage robotisés, où les postes de travail contrôlent des équipements de fabrication sensibles ou bien des zones d'accès très restreintes, peuvent nécessiter une segmentation physique qui ne donne pas l' accès aux périphériques externes (pas d'accès aux périphériques mobiles).

Dans un environnement où les utilisateurs peuvent accéder au réseau avec des périphériques mobiles, l'activation des User-ID et App-ID conjointement à la segmentation du réseau en zones garantit que les utilisateurs reçoivent les privilèges d'accès appropriés, quel que soit le lieu où ils accèdent au réseau, car les privilèges d'accès sont liés à un utilisateur ou à un groupe d'utilisateurs plutôt qu'à un périphérique dans une zone particulière.

Les exigences de protection des diverses zones fonctionnelles et des divers groupes peuvent également varier. Par exemple, une zone qui gère une grande quantité de trafic peut exiger des seuils de protection contre la saturation différents de ceux d'une zone qui gère normalement moins de trafic. La capacité de définir une protection appropriée pour chaque zone est une autre raison pour

laquelle segmenter le réseau. Ce qui constitue une protection appropriée dépend de l'architecture de votre réseau, de ce que vous voulez protéger et du trafic que vous voulez autoriser et refuser.

# Comment les zones protègent-elles le réseau?

Les zones ne protègent pas uniquement votre réseau en le segmentant en des zones plus petites et plus faciles à gérer, elles protègent également le réseau, car vous pouvez contrôler l'accès aux zones et le mouvement du trafic entre les zones.

Les zones empêchent le trafic non contrôlé d'entrer sur votre réseau par les interfaces du pare-feu, parce que les interfaces du pare-feu ne peuvent traiter le trafic si vous ne les affectez pas à des zones. Le pare-feu applique la protection de zone sur les interfaces d'entrée, là où le trafic entre dans le pare-feu dans le sens du flux allant du client d'origine vers le serveur répondant (c2s), afin de filtrer le trafic avant qu'il ne pénètre dans une zone.

Le type d'interface du pare-feu et le type de zone (tap, câble virtuel, couche 2, couche 3, tunnel ou externe) doivent correspondre ; cela permet de protéger le réseau contre l'admission de trafic qui n'appartient pas à une zone. Par exemple, vous pouvez affecter une interface de couche 2 à une zone de couche 2 ou une interface de couche 3 à une zone de couche 3, mais vous ne pouvez pas affecter une interface de couche 2 à une zone de couche 3.

De plus, une interface du pare-feu ne peut appartenir qu'à une seule zone. Le trafic destiné à diverses zones ne peut se servir de la même interface, ce qui empêche le trafic inapproprié d'entrer dans une zone et vous permet de configurer la protection qui convient à chacune des zones. Vous pouvez connecter plus d'une interface du pare-feu à une zone dans le but d'augmenter la bande passante. Toutefois, chaque interface ne peut se connecter qu'à une seule zone.

Une fois que le pare-feu a autorisé le trafic à entrer dans une zone, le trafic circule librement dans cette zone et n'est pas journalisé. Plus vous créez des zones granulaires, plus votre contrôle sur le trafic qui accède à chacune des zones est grand et plus les logiciels malveillants ont de la difficulté à se propager latéralement d'une zone à l'autre du réseau. Le trafic ne peut circuler entre des zones sans l'existence d'une règle de politique de sécurité qui l'autorise et sans que les zones soient du même type (tap, câble virtuel, couche 2, couche 3, tunnel ou externe). Par exemple, une règle de politique de sécurité peut autoriser le trafic entre deux zones de couche 3, mais pas entre une zone de couche 2 et une zone de couche 2. Le pare-feu journalise le trafic qui circule entre les zones lorsqu'une règle de politique de sécurité autorise le trafic inter-zone.

Par défaut, les règles de politique de sécurité empêchent la propagation latérale du trafic entre les zones. Ainsi, les logiciels malveillants ne peuvent accéder à une zone, puis se déplacer librement dans le réseau afin d'atteindre d'autres cibles.

***Les zones de tunnel sont applicables aux tunnels non chiffrés. Vous pouvez appliquer diverses règles de politique de sécurité au contenu de tunnel et à la zone du tunnel extérieur, comme décrit dans la section*** Aperçu de l'inspection du contenu du tunnel**.**

# Défense de zone

Un profil de protection de zone offre une protection contre les attaques par saturation et reconnaissance, les attaques basées sur les paquets et les attaques non basées sur des protocoles IP. Les profils de protection DoS utilisés dans les règles de politique de protection DoS défendent des périphériques essentiels donnés contre les attaques par saturation et basées sur les ressources ciblées. Une attaque DoS surcharge le réseau ou des systèmes essentiels ciblés avec de grandes quantités de trafic indésirable pour tenter de perturber les services réseau.

Planifiez de défendre votre réseau contre les différents types d'attaques DoS :

- **Attaques basées sur des applications**—Elles ciblent les vulnérabilités dans une application spécifique et tentent d'épuiser ses ressources afin que des utilisateurs légitimes ne puissent pas l'utiliser. Un exemple de ce type d'attaque, est une attaque Slowloris.
- **Attaques fondées sur les protocoles** : également connues sous le nom d'attaques par épuisement d'état, ces attaquent ciblent les faiblesses d'un protocole. Parmi elles, on compte l'attaque SYN flood très répandue.
- **Attaques volumineuses** : des attaques volumineuses qui tentent de surcharger les ressources disponibles d'un réseau, particulièrement la bande passante, et de provoquer l'effondrement de la cible afin d'empêcher les utilisateurs légitimes d'accéder à ces ressources. Un exemple de ce type d'attaque, est une attaque par saturation UDP.

Il n'y a pas de profils de protection de zone ou de profils de protection DoS avec règles de politique de protection DoS par défaut. Configurez et appliquez une protection de zones en fonction des caractéristiques du trafic de chaque zone et configurez une protection DoS fondée sur les systèmes essentiels individuels que vous souhaitez protéger dans chaque zone.

- Outils de défense de zone
- Comment les outils de protection des zones fonctionnent-ils ?
- Positionnement du pare-feu en vue de la protection DoS
- Profils de protection de zone
- Protection de la mémoire tampon des paquets
- Règles de politique et profils de protection DoS

## Outils de défense de zone

Pour vous défendre efficacement contre les attaques DoS, vous avez besoin d'une approche en couches. La première couche de défense devrait être un périphérique de protection contre les attaques DDoS haut volume dédié qui se trouve au périmètre du réseau Internet et un routeur de périmètre, un commutateur ou un autre périphérique de transfert de paquets matériel disposant de listes de contrôle d'accès appropriées pour assurer une défense contre les attaques volumineuses que le pare-feu basé sur la session n'est pas conçu pour gérer. Le pare-feu ajoute des couches de défense plus granulaires contre les attaques par déni de service et une visibilité sur le trafic applicatif que les périphériques DDoS dédiés ne fournissent pas.

Les pare-feu Palo Alto Networks fournissent quatre outils complémentaires pour la protection DoS de vos zones réseau et de vos périphériques critiques :

- **Profils de protection de zone** défendre le bord de la zone d'entrée contre les attaques par inondation IP, les analyses de port de reconnaissance et les balayages d'hôte, les attaques basées sur des paquets IP et les attaques utilisant un protocole non IP. La zone d'entrée est là où le trafic entre dans le pare-feu dans la direction du flux du client vers le serveur (c2s), où le client est à l'origine du flux et où le serveur est le répondeur. Les profils de protection de zone fournissent une deuxième couche de défense générale contre les attaques par déni de service, selon le trafic total entrant dans la zone, en restreignent le nombre de nouvelles connexions par seconde (CPS) à la zone. Les profils de protection de zone ne prennent pas en compte les périphériques individuels (adresses IP) car ils s'appliquent au trafic global entrant dans la zone.

  Les profils de protection de zone défendent le réseau lorsque la session est formée, avant que le pare-feu exécute la politique de protection DoS et les recherches de règles de politique de sécurité, et consomment moins de cycles CPU qu'une recherche de politique de protection DoS ou de règle de politique de sécurité. Si un profil de protection de zone refuse le trafic, le pare-feu ne dépense pas de cycles CPU sur les recherches de règles de politique.

  Appliquez des profils de protection de zone à chaque zone, qu'elle soit interne ou interne à Internet.
- Les **profils de protection DoS et règles de stratégie** défendent des points de terminaison et des ressources spécifiques contre les attaques par saturation, en particulier les cibles de grande valeur auxquelles les utilisateurs ont accès à partir d'Internet. Tandis qu'un profil de protection de zone protège la zone des attaques par inondation, une règle de stratégie de protection DoS avec un profil de protection DoS approprié protège des systèmes individuels critiques dans une zone contre les attaques par saturation ciblées, fournissant ainsi une troisième couche de défense granulaire contre les attaques par DoS.

  ***Comme la protection DoS a pour objectif de défendre les périphériques critiques et qu'elle consomme des ressources, la protection DoS protège uniquement les périphériques spécifiés dans une règle de politique de protection DoS. Aucun autre périphérique n'est protégé.***

  Les profils de protection DoS définissent des seuils de protection contre la saturations (limites de nouvelles connexions par seconde) pour des périphériques ou des groupes de périphériques individuels, des seuils de protection des ressources (limites de session pour les terminaux et les ressources spécifiés) et si le profil s'applique au trafic regroupé ou classé. Les règles de stratégie de protection DoS spécifient les critères de correspondance (source, destination, ports de service), l'action à exécuter lorsque le trafic correspond à la règle et les profils de protection DoS regroupés et classés associés à chaque règle.

  Les règles de stratégie de protection DoS ***regroupées*** appliquent les seuils CPS définis dans un profil de protection DoS global au trafic combiné de tous les périphériques répondant aux critères de correspondance des règles de stratégie de protection DoS. Par exemple, si vous configurez le profil de protection DoS global pour limiter le taux de CPS à 20 000, la limite de 20 000 CPS s'applique au nombre total de connexions du groupe dans son ensemble. Dans ce cas, un périphérique pourrait recevoir la majorité des connexions autorisées.

  Les règles de la politique de protection DoS ***classées*** appliquent les seuils de CPS définis dans un profil de protection DoS classé à chaque périphérique individuel qui correspond à la règle de la politique. Par exemple, si vous configurez le profil de protection DoS classé pour qu'il limite le

taux de CPS à 4 000, aucun périphérique du groupe ne peut accepter plus de 4 000 CPS. Une politique de protection DoS peut comporter un profil regroupé et un profil classé.

> ***Les profils classés peuvent classer les connexions par IP source, IP de destination ou les deux. Pour les zones orientées Internet, classifiez par IP de destination uniquement, car le pare-feu ne peut pas se développer pour contenir la table de routage Internet.***

Appliquez la protection DoS uniquement aux périphériques critiques, en particulier aux cibles d'attaque courantes auxquelles les utilisateurs accèdent depuis Internet, tels que les serveurs Web et les serveurs de base de données.

- Pour les sessions existantes, la **protection de la mémoire tampon de paquets** protège le pare-feu (et donc la zone) contre les attaques DoS à session unique qui tentent de saturer la mémoire tampon des paquets du pare-feu, en utilisant des seuils et des minuteries pour atténuer les sessions abusives. Vous configurez les paramètres de protection des tampons et les appliquez par zone.
- **Les règles de la Politique de sécurité** ont une incidence sur les entrées et les sorties d'une session. Pour établir une session, le trafic entrant doit correspondre à une règle de politique de sécurité existante. En absence de correspondance, le pare-feu abandonne le paquet. Une politique de sécurité autorise ou refuse le trafic entre les zones (interzone) et à l'intérieur des zones (intrazone) en utilisant des critères comme les zones, les adresses IP, les utilisateurs, les applications, les services et les catégories d'URL.

  > ***Appliquez le** profil de protection contre les vulnérabilités exemplaire **à chaque règle de politique de sécurité pour aider à vous défendre contre les attaques DoS.***

  Les règles de politique de sécurité par défaut n'autorisent pas la circulation du trafic entre les zones. Vous devez donc configurer une règle de sécurité si vous voulez autoriser le trafic interzone. Tout le trafic intrazone est autorisé par défaut. Vous pouvez configurer des règles de politique de sécurité et contrôler le trafic intrazone, interzone et universel (intrazone et interzone).

  > ***Les profils de protection de zone, règles de politique/profils de protection DoS et règles de politique de sécurité affectent uniquement le trafic de plan de données sur le pare-feu. Le trafic provenant de l'interface de gestion du pare-feu ne traverse pas le plan de données. Ainsi, le pare-feu ne fait pas correspondre le trafic de gestion à ces profils ou règles de politique.***
- Vous pouvez également rechercher la chambre forte des menaces Palo Alto Networks (nécessite un compte de support valide et une connexion) pour les menaces par hachage, CVE, ID de signature, nom de domaine, URL ou adresse IP.

## Comment les outils de protection des zones fonctionnent-ils ?

Lorsqu'un paquet arrive au pare-feu, le pare-feu tente de mettre le paquet en correspondance avec une session existante, selon la zone d'entrée, la zone de sortie, l'adresse IP source, l'adresse IP de destination, le protocole et l'application dérivés de l'en-tête du paquet. Si le pare-feu trouve une correspondance, le paquet utilise alors les règles de politique de sécurité qui contrôlent déjà la session. Si le paquet n'est mis en correspondance avec aucune session, le pare-feu utilise les profils de protection de zone, les règles de politique et les profils de protection DoS ainsi que les règles de politique de sécurité pour déterminer s'il faut établir une session ou supprimer le paquet et pour décider du niveau d'accès que le paquet reçoit.

Une fois que le trafic est passé par votre périphérique DDoS dédié du côté réseau orienté vers l'Internet, la première protection que le pare-feu applique est la défense vaste du profil de protection de zone, si un profil est associé à la zone. Le pare-feu détermine la zone de l'interface sur laquelle le paquet arrive (chaque interface n'est affectée qu'à une seule zone et toutes les interfaces qui acheminent les trafic doivent appartenir à une zone). Si le profil de protection de zone refuse le paquet, le pare-feu rejette le paquet et épargne les ressources en n'ayant pas besoin de chercher la politique de protection DoS ni la politique de sécurité. Le pare-feu applique les profils de protection de zone uniquement aux nouvelles sessions (paquets qui ne correspondent pas à une session existante). Une fois que le pare-feu a établi une session, le pare-feu contourne la recherche de profil de protection de zone pour les paquets qui réussissent dans cette session.

Si le profil de protection de zone n'abandonne pas le paquet, la deuxième protection que le pare-feu applique est une règle de politique de protection DoS. Si un profil de protection de zone autorise un paquet en fonction du volume total cumulé de trafic entrant dans la zone, une règle de politique de protection DoS pourrait refuser le paquet s'il se dirige vers une destination donnée ou qu'il provient d'une source donnée qui a dépassé les paramètres de protection des ressources ou de protection contre la saturation définis dans le profil de protection DoS de la règle. Si le paquet correspond à une règle de politique de protection DoS, le pare-feu applique la règle au paquet. Si la règle refuse l'accès, le pare-feu rejette le paquet et n'effectue aucune recherche de politiques de sécurité. Si la règle autorise l'accès, le pare-feu effectuer une recherche de politiques de sécurité. Tout comme le profil de protection de zone, le pare-feu applique la politique de protection DoS seulement aux nouvelles sessions.

La troisième protection appliquée par le pare-feu est une recherche de politiques de sécurité, laquelle n'a lieu que si le profil de protection de zone et les règles de politique de protection DoS autorisent le paquet. Si le pare-feu ne trouve aucune règle de politique de sécurité qui correspond au paquet, le pare-feu rejette le paquet. Si le pare-feu trouve une règle de politique de sécurité correspondante, il l'applique au paquet. Le pare-feu applique la règle de politique de sécurité dans les deux sens (c2s et s2c) pour la durée de vie de la session. Appliquez le Profil de protection contre les vulnérabilités exemplaire à toutes les règles de politique de sécurité pour contribuer à défendre les attaques DoS.

La quatrième protection que le pare-feu applique est la protection de la mémoire tampon des paquets, que vous appliquez globalement pour protéger le périphérique et que vous pouvez également appliquer individuellement à des zones pour éviter les attaques DoS sur une session unique qui tentent de surcharger la mémoire tampon des paquets du pare-feu. Pour une protection globale, le pare-feu a utilisé le Random Early Drop (Abandon anticipé aléatoire ; RED) pour abandonner les paquets (et non pas les sessions) lorsque le niveau de trafic traverse les seuils de protection. Pour une protection par zone, le pare-feu bloque l'adresse IP source si elle enfreint les seuils de mémoire tampon des paquets. Contrairement à la protection DoS et à la protection de la zone, la protection de la mémoire tampon des paquets s'applique à toutes les sessions existantes.

## Positionnement du pare-feu en vue de la protection DoS

Le pare-feu est un périphérique basé sur des sessions qui n'est pas conçu pour s'adapter à des millions de connections-per-second (connexions par seconde ; CPS) pour se défendre contre de larges attaques DoS volumétriques. Le pare-feu traite chaque flux unique (basé sur la zone d'entrée et sur la zone de sortie, sur l'adresse IP source et l'adresse IP de destination, sur le protocole et sur l'application) en tant que session, dépense les cycles CPU sur l'inspection de paquets au niveau du port et de l'adresse IP dans le but de fournir une visibilité du trafic de l'application et doit compter

chaque session dans le seuil de saturation ; le positionnement du pare-feu est donc critique si l'on souhaite éviter la saturation du pare-feu.

Pour bénéficier de la meilleure protection DoS qui soit, ***positionnez les pare-feu le plus près possible des ressources que vous protégez.*** Ce faisant, vous réduisez le nombre de sessions que le pare-feu a besoin de gérer et, par le fait même, la quantité de ressources du pare-feu nécessaires pour fournir la protection contre les attaques DoS.

Au périmètre orienté Internet, ***évitez*** de placer les pare-feu que vous utilisez pour la protection DoS ou la protection de zones devant les périphériques DDos et les routeurs et les commutateurs du périmètre. Faites de ces périphériques haut volume votre première ligne de défense pour atténuer les attaques par saturation volumétriques. Pour la protection de zones et DoS au périmètre, utilisez des pare-feu haute capacité et positionnez-les ***derrière*** les périphériques haut volume. Règle générale, plus un pare-feu est près du périmètre, plus sa capacité doit être grande pour gérer le volume de trafic.

La manière dont vous segmentez votre réseau en zones peut contribuer à l'atténuation des attaques DoS internes. De plus petites zones procurent une plus grande visibilité du trafic et permettent de mieux empêcher le mouvement latéral des fichiers malveillants, car un plus grand volume de trafic doit traverser la zone. Pour autoriser le trafic interzone, vous devez créer une règle de politique de sécurité particulière (tout le trafic intrazone est autorisé par défaut). Songez à revoir votre approche à l'égard de la segmentation si votre réseau est relativement peu segmenté.

# Mesures CPS de référence pour établir les seuils de saturation

Les seuils de protection contre les inondations déterminent le nombre de nouvelles connexions par seconde (CPS) à autoriser pour une zone (profil de protection de zone), pour un groupe de périphériques dans une zone (stratégie de protection DoS globale) ou pour des périphériques individuels dans une zone ( politique de protection DoS classée), quand limiter les nouvelles connexions pour commencer à atténuer une possible attaque par saturation et quand abandonner toutes les nouvelles connexions. Les seuils de protection contre la saturation par défaut du profil de protection de zone et du profil de protection DoS ne conviennent pas à la plupart des réseaux, car chaque réseau est unique. Vous devez comprendre les CPS normaux et maximaux cumulés pour chaque zone pour définir des seuils efficaces pour le profil de protection de zone. De même, vous voulez défendre les systèmes critiques individuels en définissant des seuils de profil de protection DoS efficaces qui, par mégarde, ne définissent pas des seuils trop élevés ni ne permettent des attaques par saturation ou définissent des seuils trop faible et ralentissent le trafic.

- Mesures des connexions par secondes à prendre
- Comment mesurer les CPS

## Mesures des connexions par secondes à prendre

Mesurez le trafic CPS moyen et maximal pendant au moins cinq jours ou jusqu'à ce que vous ayez la conviction que les mesures reflètent les tendances habituelles du réseau en matière de trafic ; une plus longue période de mesure vous permettra d'obtenir des résultats plus précis. Tenez compte des événements spéciaux, des événements trimestriels et des événements annuels qui se produisent sur le compte, lesquels pourraient entraîner une hausse du nombre de CPS que devez prendre en charge. Vous devrez peut-être ajuster les profils de protection de la zone et prévoir des règles de stratégie de protection DoS ajustées pour tenir compte de ces types d'événements si vos pare-feu ont la capacité de gérer du trafic supplémentaire. Prenez les mesures de référence suivantes :

- Pour les profil de protection de zone, mesurez les CPS moyens et maximaux qui entrent dans chaque zone.
- Pour les profils de protection DoS regroupés, mesurez les CPS moyens et maximaux pour chaque groupe de périphériques que vous souhaitez protéger.
- Pour les profils de protection DoS classés, mesurez les CPS moyens et maximaux pour les périphériques individuels que vous souhaitez protéger.

Vous devez également comprendre la capacité de vos pare-feu et l'incidence que des fonctions consommant les ressources, comme le déchiffrement, ont sur le nombre de connexions que chaque pare-feu peut contrôler. En règle générale, plus un pare-feu est près du périmètre, plus il doit disposer d'une grande capacité, car il gère plus de trafic. La fiche technique de chaque modèle de pare-feu comprend le nombre total de nouvelles sessions par seconde (CPS) que le pare-feu peut prend en charge et l'outil de comparaison de pare-feu vous permet de comparer le CPS (et d'autres mesures) entre différents modèles de pare-feu.

## Comment mesurer les CPS

On peut mesure les CPS de diverses manières :

- Si vous utilisez Panorama pour gérer vos pare-feu, utilisez la surveillance des périphériques pour mesurer les CPS qui entrent dans un pare-feu (**Panorama** > **Managed Devices (Périphériques gérés)** > **Health (Santé)** > **All Devices (Tous les périphériques)**). La surveillance des périphériques peut également vous montrer une ligne de tendance de la consommation CUP moyenne et de l'utilisation maximale sur 90 jours pour vous aider à comprendre la capacité disponible de chaque pare-feu.
- Exécutez la commande CLI opérationnelle **`show session info`**.

  *La commande CLI opérationnelle **`show counter interface`** affiche deux fois la valeur réelle du CPS. Si vous utilisez cette commande, divisez la valeur CPS par deux pour obtenir la valeur CPS réelle.*
- Pour définir des seuils de profil de protection DoS appropriés, travaillez avec les équipes d'applications pour comprendre les CPS normaux et maximaux de leurs serveurs et les CPS maximaux que ces serveurs peuvent prendre en charge.

  En outre, vous pouvez filtrer les journaux du trafic et les journaux des menaces pour les adresses IP de destination des périphériques essentiels que vous souhaitez protéger afin d'obtenir des informations sur les activités de session normales et maximales.
- Utilisez des outils tiers tels que Wireshark ou NetFlow pour recueillir des données relatives au trafic réseau et les analyser.
- Utilisez des scripts pour automatiser la collecte d'informations sur les CPS et pour en effectuer la surveillance continue, de même que pour extraire des informations des journaux.
- Configurez chaque règle de politique de sécurité sur le pare-feu pour qu'elle **Log at Session End (Journalise à la fin de la session)**. Si vous ne disposez d'aucun outil de surveillance comme NetFlow ou Wireshark, et que vous ne pouvez obtenir ou développer des scripts automatisés, la **Log at Session End (Journalisation à la fin de la session)** recueille le nombre de connexions à la fin de la session. Bien qu'elle ne fournisse pas d'informations sur la CPS, elle vous indique le nombre de sessions se terminant dans la durée sélectionnée et vous pouvez faire un calcul approximatif des sessions par seconde à partir de ces informations.

*Pour préserver les ressources, le pare-feu mesure les CPS cumulées à des intervalles de dix secondes. C'est pourquoi les mesures que vous voyez sur le pare-feu peuvent ne pas capter les rafales dans l'intervalle de dix secondes. Bien que les mesures moyennes de la CPS ne soient pas affectées, les mesures de la CPS de pointe peuvent ne pas être précises. Par exemple, si les journaux du pare-feu signalent une moyenne de 5 000 CPS dans un intervalle de dix secondes, il se peut que 4 000 CPS se sont produits lors d'une rafale d'une seconde et que les autres 1 000 CPS étaient répartis sur les neuf secondes suivantes.*

Pour recueillir des données CPS historiques dans le temps, si vous utilisez un serveur SNMP, vous pouvez utiliser vos propres outils de gestion pour interroger les MIB SNMP. Cependant, il est important de comprendre que les mesures du CPS dans les MIB indiquent deux fois la valeur réelle du CPS (par exemple, si la mesure réelle du CPS est de 10 000, les MIB indiquent 20 000 comme valeur). Vous pouvez toujours voir les tendances des MIB et vous pouvez diviser les valeurs du CPS par deux pour en déduire les vraies valeurs. Les OID de MIB SNMP sont : PanZoneActiveTcpCps, PanZoneActiveUdpCps, et PanZoneOtherIpCps. Comme le pare-feu ne prend des mesures et ne met à jour le serveur SNMP que toutes les 10 secondes, le sondage est effectué toutes les 10 secondes.

De plus, créez des profils de transfert des journaux distincts pour les événements de saturation afin que l'administrateur approprié reçoive des messages électroniques qui contiennent uniquement des événements de saturation (attaque DoS éventuelle). Définissez le transfert des journaux pour les événements de protection de zone et les événements de protection DoS.

*Après avoir mis en œuvre la protection DoS et la protection de la zone, utilisez ces méthodes pour surveiller le déploiement. Ainsi, au fur et à mesure de l'évolution de votre réseau et des modèles de trafic, vous devez ajuster les seuils de protection contre la saturation.*

# Profils de protection de zone

Appliquez un profil de protection de zone à chaque zone pour la défendre en fonction du trafic regroupé entrant dans la zone d'entrée.

*En plus de configurer la protection DoS et la protection de zone, appliquez le profil de protection contre les vulnérabilités exemplaire à chaque règle de politique de sécurité pour vous aider à vous défendre contre les attaques DoS.*

- Protection contre la saturation
- Protection contre la reconnaissance
- Protection contre les attaques basées sur des paquets
- Protection du protocole
- Protection SGT Ethernet

## Protection contre la saturation

Un profil de protection de zone pour lequel la protection contre la saturation a été configurée défend une zone d'entrée entière contre les attaques par saturation SYN, ICMP, ICMPv6, UDP et autres attaques basées sur des adresses IP. Le pare-feu mesure la quantité agrégée de chaque type d'attaque par saturation qui entre dans la zone en nouvelles connexions par seconde et compare le total aux seuils que vous configurez dans le profil de protection de zone. (Vous protégez des

périphériques individuels essentiels au sein d'une zone grâce aux profils de protection DoS et règles de politique.)

*Mesurez et surveillez la consommation CPU du plan de données du pare-feu afin de vous assurer que chaque pare-feu est correctement dimensionné pour soutenir la protection DoS et la protection de la Zone et d'autres fonctions qui consomment les cycles CPU, telles que le déchiffrement. Si vous utilisez Panorama pour gérer vos pare-feu, la* surveillance des pare-feu *(**Panorama > Managed Devices (Périphériques gérés) > Health (Santé) > All Devices (Tous les périphériques)**) vous montre la consommation CPU et mémoire de chaque pare-feu géré. Elle peut également vous montrer une ligne de tendance de la consommation CUP moyenne et de l'utilisation maximale sur 90 jours pour vous aider à comprendre la capacité disponible de chaque pare-feu.*

Pour chaque type de saturation, vous définissez des seuils pour les nouveaux CPS entrant dans la zone, et vous pouvez définir l'autre **action** pour les attaques par saturation SYN. Si vous connaissez les CPS de référence pour la zone, utilisez ces lignes directrices pour définir les seuils initiaux, puis surveillez et ajustez les seuils au besoin.

- **Taux d'alarme** : le nouveau seuil de CPS pour déclencher une alarme. Visez l'établissent d'un **Alarm Rate (Taux d'alarme)** se situant de 15 à 20 % au-dessus du taux des CPS moyen pour la zone, afin d'éviter que les fluctuations normales ne causent des alertes.
- **Taux d'activation** : le seuil des nouvelles CPS pour activer le mécanisme de protection contre la saturation et pour commencer à abandonner des nouvelles connexions. Pour les attaques ICMP, ICMPv6, UDP et les autres attaques par saturation IP, le mécanisme de protection est le Random Early Drop ((Abandon anticipé aléatoire ; RED) également connu sous le nom de détection précoce aléatoire). Pour les attaques par saturation SYN uniquement, vous pouvez définir l'**Action** d'abandon sur cookies SYN ou RED. Visez l'établissement d'un taux **Activate (d'activation)** légèrement supérieur au taux de CPS maximal pour la zone afin de commencer à atténuer les attaques par saturation éventuelles.
- **Maximum** : le nombre de connexions par seconde devant être atteint pour abandonner les paquets entrants lorsque le RED est le mécanisme de protection utilisé. Visez l'établissement d'un taux **Maximum** représentant environ de 80 à 90 % de la capacité du pare-feu, en tenant compte des autres fonctionnalités qui consomment des ressources du pare-feu.

Si vous ne connaissez pas les taux de CPS de référence pour la zone, commencez par définir un taux de CPS **Maximum** d'environ 80 à 90 % de la capacité du pare-feu et utilisez-le pour dériver les taux d'activation et d'alarme pour atténuer la saturation et la ramener à un niveau raisonnable. Définissez le **Alarm Rate (Taux d'alarme)** et le taux **Activate (d'activation)** en fonction du taux maximal. Par exemple, vous pourriez définir le **Alarm Rate (Taux d'alarme)** à la moitié du taux **Maximum**, puis l'ajuster selon le nombre d'alarmes que vous recevez et des ressources du pare-feu consommées. Soyez prudent lors de l'établissement du **Activate Rate (Taux d'activation)**, car il commence à abandonner les connexions. Puisque le volume de trafic normal peut fluctuer, il vaut mieux ne pas abandonner les connexions trop brusquement. Conservez un taux à la hausse, puis ajustez-le si les ressources du pare-feu sont touchées.

*La protection contre la saturation SYN est la seule pour laquelle vous définirez l'**Action** d'abandon. Commencez par définir l'**Action** sur **SYN Cookies (Cookies SYN)**. Les cookies SYN traitent le trafic légitime équitablement et n'abandonnent que le trafic qui échoue l'établissement de liaison SYN, tandis que l'utilisation du Random Early Drop (Abandon anticipé aléatoire ; RED) permet d'abandonner le trafic de manière aléatoire, ce qui veut dire que RED pourrait affecter le trafic légitime. Cependant, les cookies SYN exigent une consommation plus grande de ressources, parce que le pare-feu fait office de proxy pour le serveur cible et gère l'établissement de la connexion en trois étapes pour le serveur. La solution de compromis consiste à ne pas abandonner le trafic légitime (cookies SYN) pour préserver les ressources du pare-feu (RED). Surveillez le pare-feu, et si les cookies SYN consomment un trop grand nombre de ressources, passez au RED. Si vous ne disposez pas d'un périphérique de prévention DDoS dédié devant le pare-feu, utilisez toujours le RED comme mécanisme d'abandon.*

*Lorsque **SYN Cookies (cookies SYN)** sont activés, le pare-feu n'honore pas les options TCP envoyées par le serveur car il ne connaît pas ces valeurs au moment où il effectue le proxy SYN/ACK. Par conséquent, des valeurs telles que la taille de la fenêtre du serveur TCP et les valeurs MSS ne peuvent pas être négociées pendant la négociation TCP et le pare-feu utilisera ses propres valeurs par défaut. Dans le scénario où le MSS du chemin d'accès au serveur est plus petit que la valeur MSS par défaut du pare-feu, le paquet devra être fragmenté.*

Les valeurs de seuil par défaut sont élevées pour que l'activation d'un profil de protection de zone n'abandonne pas soudainement le trafic légitime. Ajustez les seuils des valeurs d'une façon appropriée pour le trafic votre réseau. La meilleure façon de comprendre ce que vous devez faire pour définir des seuils de saturation raisonnables consiste à prendre des mesures de base des CPS moyennes et maximales pour chaque type de saturation afin de déterminer les conditions de trafic normales de chaque zone et de comprendre la capacité du pare-feu, y compris l'incidence d'autres fonctionnalités consommant beaucoup de ressources, comme le déchiffrement. Surveillez et ajustez les seuils de saturation, au besoin, et au fur et à mesure de l'évolution de votre réseau.

*Les pare-feux équipés de processeurs à multiples plans de données (DPs) répartissent les connexions à travers les DPs. Habituellement, le pare-feu partage équitablement les réglages de seuils des CPS à travers ses DPs. Par exemple, si un pare-feu possède cinq DP et que vous définissez le **Alarm Rate (Taux d'alarme)** sur 20 000 CPS, chaque DP a un **Alarm Rate (Taux d'alarme)** de 4 000 CPS (20 000 / 5 = 4 000). S'il y a plus de 4 000 nouvelles sessions sur un DP, le **Alarm Rate (Taux d'alarme)** pour ce DP est alors déclenché.*

## Protection contre la reconnaissance

La reconnaissance en matière de sécurité des réseaux, tout comme la reconnaissance militaire, correspond aux tentatives des agresseurs d'obtenir des informations sur les vulnérabilités de vos réseaux en les sondant secrètement pour y trouver des failles. Les activités de reconnaissance préfigurent bien souvent une attaque du réseau. *Enable Reconnaissance Protection on all zones (Activez la protection contre la reconnaissance sur toutes les zones)* pour vous défendre contre les balayes de ports et les balayages d'hôtes :

- **Les balayages de ports** permettent de découvrir des ports ouverts sur un réseau. Un outil de balayage de ports lance des requêtes client sur une plage de numéros de ports sur un hôte

distant, avec pour objectif de trouver un port actif à exploiter lors d'une attaque. Les profils de protection de zones protègent aussi bien des balayages de ports sur protocole TCP que sur protocole UDP.

- **Les balayages d'hôtes distants** examinent de multiples hôtes pour déterminer si un port spécifique est ouvert et s'il est vulnérable.

Vous pouvez utiliser des outils de reconnaissance à des fins légitimes, par exemple pour tester la sécurité d'un réseau ou la solidité d'un pare-feu. Vous pouvez spécifier jusqu'à 20 adresses IP ou objets avec des masques de sous-réseau à exclure des protections contre la reconnaissance pour que votre département informatique interne puisse mener des tests pour chercher et corriger les vulnérabilités du réseau.

Vous pouvez choisir quelle action effectuer lorsque des activités de reconnaissance (hors trafic de test) dépassent le seuil configuré quand vous Configuration de la protection contre la reconnaissance. Conservez le **Interval (Intervalle)** et le **Threshold (Seuil)** par le défaut pour journaliser quelques paquets pour analyse avant de bloquer l'opération de reconnaissance.

## Protection contre les attaques basées sur des paquets

Les attaques basées sur des paquets prennent de nombreuses formes. Les profils de protection de zone vérifient les en-têtes de paquet IP, TCP, ICMP, IPv6 et ICMPv6 et protègent une zone en :

- Laissant tomber les paquets avec des caractéristiques indésirables.
- Enlevant les options indésirables des paquets avant de les admettre dans la zone.

Sélectionnez les caractéristiques d'abandon de chaque type de paquet lorsque vous Configuration de la protection contre les attaques basées sur les paquets. Voici les pratiques exemplaires de chaque protocole IP :

- **IP Drop**—Abandonnez les paquets **Unknown (Inconnus)** et **Malformed (Malformés)**. Abandonne également le **Strict Source Routing (Routage source strict)** et le **Loose Source Routing (Routage source vague)**, car en autorisant ces options, vous autorisez les adversaires à contourner les règles de politique de sécurité qui utilisent l'adresse IP de destination en tant que critère de correspondance. Pour les zones internes uniquement, vérifiez la **Spoofed IP Address (Adresse IP usurpée)** pour que seul le trafic possédant une adresse source qui est mise en correspondance avec la table de routage du pare-feu puisse accéder la zone.
- **TCP Drop (Abandon TCP)** : conservez les abandons **TCP SYN with Data (paquets TCP SYN contenant des données)** et **TCP SYNACK with Data (paquets TCP SYN-ACK contenant des données)**, abandonnez les paquets **Mismatched overlapping TCP segment (Segment TCP non**

**concordant et se chevauchant)** et **Split Handshake (Établissement de liaison de segmentation)**, et supprimez les **TCP Timestamp (horodatagesTCP)** des paquets.

> *L'activation de l'option **Rematch Sessions (Revérifier les sessions)** (**Device (Périphérique) > Setup (Configuration) > Session > Session Settings (Paramètres de session)**) est une bonne pratique qui applique les règles de politique de sécurité modifiées ou nouvellement configurées aux sessions existantes. Cependant, si vous configurez l'inspection du contenu du tunnel sur une zone et que la **Rematch Sessions (Revérification des sessions)** est activée, vous devez également désactiver l'option visant à **Reject Non-SYN TCP (Rejeter le protocole TCP non-SYN)** (faire passer la sélection de **Global** à **No (Non)**), ou lorsque vous activez ou modifiez une politique d'inspection du contenu du tunnel, le pare-feu abandonne toutes les sessions de tunnel existantes. Créez un profil de protection de zone distinct pour désactiver l'option **Reject Non-SYN TCP (Rejeter le protocole TCP non-SYN)** seulement dans les zones qui disposent de politiques d'inspection du contenu du tunnel et uniquement lorsque vous activez l'option **Rematch Sessions (Revérification des sessions)**.*

- **ICMP Drop (Abandon d'ICMP)** : il n'existe pas de paramètres recommandés standard, parce que l'abandon des paquets ICMP dépend de l'utilisation que vous faites d'ICMP (ou de si vous utilisez ICMP). Par exemple, si vous souhaitez bloquer l'activité ping, vous pouvez bloquer **ICMP Ping ID 0 (ID ping ICMP 0)**.
- **IPv6 Drop (Abandon d'IPv6)** : si la conformité importe, assurez-vous que le pare-feu abandonne les paquets qui comportent des extensions, des en-têtes de routage non conformes, etc.
- **ICMPv6 Drop (Abandon de ICMPv6)** : si la conformité importe, assurez-vous que le pare-feu abandonne certains paquets si les paquets ne correspondent pas à une règle de politique de sécurité.

## Protection du protocole

Dans un profil de protection de zone, la protection du protocole offre une protection contre les attaques basées sur un protocole non IP. Activez la protection de protocole pour bloquer ou autoriser les protocoles non IP entre les zones de sécurité d'un réseau local virtuel de couche 2 ou sur un câble virtuel, ou entre les interfaces d'une même zone sur un réseau local virtuel de couche 2 (Les interfaces et zones de couche 3 abandonnent les protocoles non IP, la protection de protocole non IP ne s'applique donc pas). Configuration de la protection de protocole pour réduire les risques pour la sécurité et faciliter la conformité réglementaire en empêchant les protocoles moins sécurisés d'entrer dans une zone ou une interface dans une zone.

> *Si vous ne configurez pas de profil de protection de zone qui empêche les protocoles non IP de la même zone de passer d'une interface de couche 2 à une autre, le pare-feu autorise le trafic en raison de la règle de politique de sécurité d'autorisation au sein de la zone par défaut. Vous pouvez créer un profil de protection de zone qui bloque les protocoles tels que LLDP au sein d'une zone pour empêcher la découverte de réseaux accessibles via d'autres interfaces de zone.*

Si vous devez savoir quels protocoles non IP s'exécutent sur votre réseau, utilisez des outils de surveillance tels que NetFlow, Wireshark ou d'autres outils tiers pour détecter les protocoles non IP sur votre réseau. Les exemples de protocoles non IP que vous pouvez bloquer ou autoriser comprennent les systèmes LLDP, NetBEUI, spanning Tree, et Supervisory Control and Data Acquisition (SCADA), comme Generic Object Oriented Event (GOOSE).

Créez une **Exclude List (Liste d'exclusion)** ou une **Include Liste (Liste d'inclusion)** pour configurer la protection de protocole pour une zone. La **Exclude List (Liste d'exclusion)** est une liste de blocage - le pare-feu bloque tous les protocoles que vous placez dans la **Exclude List (Liste d'exclusion)** et autorise tous les autres protocoles. La **Include List (Liste d'inclusion)** est une liste d'autorisation - le pare-feu n'autorise que les protocoles spécifiés dans la liste et bloque tous les autres protocoles.

*Utilisez les listes d'inclusion pour la protection de protocole au lieu des listes d'exclusion. Les listes d'inclusion n'autorisent spécifiquement que les protocoles que vous souhaitez autoriser et bloquent les protocoles dont vous n'avez pas besoin sur votre réseau, ou dont vous ignoriez l'existence, ce qui réduit la surface d'attaque et bloque le trafic inconnu.*

Une liste prend en charge un maximum de 64 entrées Ethertype, chacune identifiée par son code IEEE hexadécimal Ethertype. Voici d'autres sources de codes Ethertype : standards.ieee.org/develop/regauth/ethertype/eth.txt et http://www.cavebear.com/archive/cavebear/Ethernet/type.html. Lorsque vous configurez la protection de zone pour les protocoles non-IP sur des zones disposant d'interfaces Ethernet agrégées, vous ne pouvez pas bloquer ou autoriser un protocole non-IP sur une seule interface AE car les interfaces AE sont traitées en tant que groupe.

*La protection du protocole ne vous permet pas de bloquer les trames marquées IPv4 (Ethertype 0x0800), IPv6 (0x86DD), ARP (0x0806) ou VLAN (0x8100). Le pare-feu autorise toujours implicitement ces quatre Ethertypes dans une **Inclure Liste (Liste d'inclusion)** même si vous ne les indiquer pas explicitement dans la liste et ne vous permet pas de les ajouter à une **Exclude List (Liste d'exclusion)**.*

### Protection SGT Ethernet

Dans un réseau Cisco TrustSec, un moteur de services d'identité Cisco (ISE) attribue une étiquette de groupe de sécurité de couche 2 (SGT) de 16 bits à la session d'un utilisateur ou d'un terminal. Vous pouvez créer un profil de protection de zone avec protection SGT Ethernet lorsque votre pare-feu fait partie d'un réseau Cisco TrustSec. Le pare-feu peut inspecter les en-têtes avec 802.1Q (Ethertype 0x8909) pour des valeurs spécifiques d'étiquette de groupe de sécurité (SGT) de couche 2 et supprimer le paquet si la SGT correspond à la liste que vous configurez pour le profil de protection de zone attaché à l'interface. Déterminez à quelles valeurs SGT vous voulez refuser l'accès à une zone.

## Protection de la mémoire tampon des paquets

La protection de la mémoire tampon des paquets protège votre pare-feu et votre réseau contre les attaques par déni de service sur une session unique qui peuvent submerger la mémoire du tampon du pare-feu et occasionner la chute du trafic légitime. Bien que vous ne configuriez pas la protection de la mémoire tampon de paquet dans un profil de protection de zone, ni dans un profil de protection DoS, ni dans une règle de politique, la protection de la mémoire tampon des paquets protège les zones d'entrée. Bien que la protection de zone et DoS s'applique aux nouvelles sessions (connexions) et qu'elle soit granulaire, la protection de la mémoire tampon des paquets s'applique aux sessions existantes et a une portée globale.

Vous Configuration de la protection de la mémoire tampon des paquets globalement pour protéger l'ensemble du pare-feu et vous activez également la protection de la mémoire tampon des paquets sur chaque zone pour protéger les zones :

- **Protection globale de la mémoire tampon des paquets** : le pare-feu surveille les sessions de toutes les zones (que la protection de la mémoire tampon des paquets soit activée ou non) et l'utilisation que font ces sessions de la mémoire tampon des paquets. Vous devez configurer la protection de la mémoire tampon des paquets de manière globale (**Device (Périphérique)** > **Setup (Configuration)** > **Session Settings (Paramètres de session)**) pour protéger le pare-feu et l'activer sur des zones individuelles. Lorsque la consommation de la mémoire tampon des paquets atteint le pourcentage **Activate (Activer)** configuré, le pare-feu utilise Random Early Drop (Abandon anticipé aléatoire ; RED) pour supprimer les paquets des sessions fautives (le pare-feu n'abandonne pas des sessions complètes au niveau global).
- **Protection de la mémoire tampon des paquets par zone** : activer la protection de la mémoire tampon des paquets sur chaque zone (**Network (Réseau)** > **Zones**) pour superposer un deuxième niveau de protection. Lorsque la consommation de la mémoire tampon des paquets dépasse le seuil **Activate (Activer)** et que la protection globale commence à appliquer le RED au trafic de session, le minuteur **Block Hold Time (Délai de maintien du blocage)** démarre alors. Le **Block Hold Time (Délai de maintien du blocage)** correspond à la durée, en secondes, pendant laquelle la session fautive peut se poursuivre avant que le pare-feu ne bloque la session au complet. La session fautive reste bloquée jusqu'à ce que l'expiration du **Block Hold Time (Délai de maintien du blocage)**.

  *Vous devez activer la protection de mémoire tampon des paquets globalement pour qu'elle soit active dans les zones.*

Il existe deux types de protection de mémoire tampon des paquets :

- Protection de la mémoire tampon des paquets basée sur l'utilisation de la mémoire tampon
- Protection de la mémoire tampon des paquets sur la base de la latence

#### Protection de la mémoire tampon des paquets basée sur l'utilisation de la mémoire tampon

La protection de la mémoire tampon des paquets basée sur l'utilisation de la mémoire du tampon est activée par défaut. Prenez des mesures de base de l'utilisation de la mémoire tampon des paquets du pare-feu sur une période donnée (au moins une semaine ouvrable; une période de mesure plus longue fournit cependant une meilleure base de référence) pour comprendre l'utilisation typique.

Pour voir l'utilisation de la mémoire tampon des paquets pendant une période de temps donnée (ou pour voir les cinq premières sessions qui utilisent au moins 2 % de la mémoire tampon des paquets), utilisez la commande CLI opérationnelle :

```
admin1138@thxvm1>show running resource-monitor [day | hour | ingress-
backlogs | minute | second | week]
```

La commande CLI fournit un instantané de l'utilisation de la mémoire tampon pendant la période spécifiée, mais n'est ni automatisée ni continue. Pour automatiser les mesures continues de l'utilisation de la mémoire tampon des paquets afin de pouvoir surveiller les changements de comportement et les événements anormaux, utilisez un script. L'équipe de votre compte Palo Alto Networks peut vous fournir un exemple de script que vous pouvez modifier pour développer votre propre script ; cependant, le script n'est pas officiellement pris en charge et il n'y a pas de support technique disponible pour l'utilisation ou la modification du script.

Si les mesures de base montrent systématiquement une utilisation anormalement élevée de la mémoire tampon des paquets, il se peut que la capacité du pare-feu soit sous-dimensionnée pour les

charges de trafic types. Dans ce cas, envisagez de redimensionner le déploiement du pare-feu. Sinon, vous devez ajuster avec soin les seuils de protection de la mémoire tampon des paquets afin d'éviter tout débordement de la mémoire tampon touchée (et d'éviter l'abandon du trafic légitime). Lorsque le dimensionnement du pare-feu est correct pour le déploiement, seule une attaque devrait entraîner une forte augmentation de l'utilisation de la mémoire tampon.

*Le dépassement de la mémoire tampon des paquets du pare-feu a un impact négatif sur les capacités de transmission des paquets du pare-feu. Lorsque les tampons sont pleins, aucun paquet ne peut pénétrer dans le pare-feu d'aucune interface, pas seulement de l'interface ayant subi l'attaque.*

Les pratiques exemplaires pour l'établissement des seuils sont les suivantes :

- **Alert (Alerte)** et **Activate (Activer)** : démarrez avec les valeurs de seuil par défaut, surveillez l'utilisation de la mémoire tampon des paquets et ajustez les seuils selon les besoins. Le seuil **Alert (Alerte)** est fixé par défaut à 50 % ; lorsque l'utilisation de la mémoire tampon des paquets dépasse le seuil pendant plus de 10 secondes, le pare-feu crée une entrée d'alerte dans le journal du système toutes les minutes. Le seuil **Activate (Activer)**est fixé à 80 % par défaut ; lorsque le seuil est atteint, le pare-feu commence à limiter les sessions les plus abusives. Si le pare-feu est correctement dimensionné, l'utilisation de la mémoire tampon devrait être bien inférieure à 50%.
- **Block Hold Time (Délai de maintien du blocage)** : lorsque l'utilisation de la mémoire tampon des paquets déclenche le seuil **Activate (Activer)**, le **Block Hold Time (Délai de maintien du blocage)** définit la durée pendant laquelle la session fautive peut se poursuivre avant d'être bloquée par le pare-feu. Pendant le **Block Hold Time (Délai de maintien du blocage)**, le pare-feu continue d'appliquer le RED aux paquets des sessions fautives. Commencez par la valeur par défaut du **Block Hold Time (Délai de maintien du blocage)** (60 secondes), surveillez l'utilisation de la mémoire tampon des paquets et ajustez le seuil au besoin. Si le pourcentage d'utilisation de la mémoire tampon des paquets tombe sous le seuil **Activate (Activer)** avant l'expiration du **Block Hold Time (Délai de maintien du blocage)**, le minuteur se réinitialise et ne redémarre que lorsque le seuil **Activate (Activer)** est de nouveau franchi. L'augmentation du **Block Hold Time (Délai de maintien du blocage)** impose une pénalité plus sévère aux sessions fautives et sa réduction impose une pénalité moindre aux sessions fautives.
- **Block Duration (Durée de blocage)** : lors de l'expiration du **Block Hold Time (Délai de maintien du blocage)**, le pare-feu bloque la session fautive pour le délai défini dans la **(Durée de blocage)**. Commencez avec la valeur de seuil par défaut (3 600 secondes), surveillez l'utilisation de la mémoire tampon des paquets et ajustez le seuil aux besoins. Lorsque vous activez la protection de la mémoire tampon des paquets sur une zone, la **Block Duration (Durée de blocage)** affecte chaque session de l'adresse IP même si une seule session d'une adresse IP surutilise la mémoire tampon des paquets. Si vous croyez que le blocage d'adresse IP pendant une heure (3600 secondes) est une pénalité trop sévère, ramenez la **Block Duration (Durée de blocage)** à une valeur acceptable.

En plus de surveiller l'utilisation de la mémoire tampon des sessions individuelles, la protection de la mémoire tampon des paquets peut également bloquer une adresse IP si certains critères sont satisfaits. Lors de la surveillance des tampons des paquets, si le pare-feu détecte qu'une adresse IP source crée rapidement des sessions qui, individuellement, ne seraient pas perçues comme des attaques, il bloque cette adresse IP pendant la **Block Duration (Durée de blocage)** configurée.

*La traduction d'adresses réseau (NAT) (une source externe ayant traduit son trafic Internet en utilisant une NAT source) peut donner l'impression que l'utilisation de la mémoire tampon des paquets a augmenté en raison de l'activité de traduction des adresses IP. Si une telle situation se produit, ajustez les seuils de manière à pénaliser les sessions individuelles mais pas les adresses IP sous-jacentes (les autres sessions de la même adresse IP ne sont donc pas touchées). Pour ce faire, réduisez le **Block Hold Time (Délai de maintien du blocage)** de sorte que le pare-feu bloque les sessions individuelles qui surchargent les tampons plus rapidement, et réduisez la **Block Duration (Durée de blocage)** afin que l'adresse IP sous-jacente ne soit pas indûment pénalisée.*

**Protection de la mémoire tampon des paquets sur la base de la latence**

Comme alternative à la protection de la mémoire tampon des paquets basée sur l'utilisation, vous pouvez déclencher une protection de la mémoire tampon des paquets sur la base de la latence des paquets causée par la mise en mémoire tampon des paquets du plan de données, qui indique l'encombrement du pare-feu. Cette protection de la mémoire tampon des paquets atténue le blocage en tête de ligne en vous alertant de l'encombrement et en effectuant un abandon anticipé aléatoire (RED) sur les paquets. La protection de la mémoire tampon des paquets sur la base de la latence peut déclencher la protection avant que les protocoles ou les applications sensibles à la latence ne soient affectés.

Si votre trafic comprend des protocoles ou des applications qui sont sensibles à la latence, alors une protection de la mémoire tampon des paquets sur la base de la latence sera plus utile qu'une protection du tampon de paquets basée sur l'utilisation de la mémoire tampon.

La protection de la mémoire tampon des paquets sur la base de la latence inclut le réglage d'un seuil **Latency Alert (Alerte de latence)** (en millisecondes), au-dessus duquel le pare-feu commence à générer un événement de journal d'alerte. Le seuil **Latency Activate (Activer la latence)** indique quand le pare-feu active le RED sur les paquets entrants et commence à générer un journal d'activation. Le seuil **Latency Max Tolerate (Tolérance max de latence)** indique quand le pare-feu utilise RED avec une probabilité d'abandon de près de 100 %.

Les paramètres **Block Hold Time (Temps de maintien du blocage)** et **Block Duration (Durée du blocage)** fonctionnent pour la protection de la mémoire tampon des paquets sur la base de la latence de la même manière qu'ils le font pour la protection de la mémoire tampon des paquets basée sur l'utilisation.

## Règles de politique et profils de protection DoS

Les profils de protection DoS et les règles de politique de protection DoS s'allient pour protéger des groupes particuliers de ressources critiques et de ressources critiques individuelles contre la saturation de sessions. Comparativement aux profils de protection de zone, qui protègent des zones complètes contre les attaques par saturation, la protection DoS fournit une défense granulaire pour des systèmes spécifiques, particulièrement des systèmes critiques auxquels les utilisateurs accèdent à partir de l'Internet et qui sont souvent la cible d'attaques, comme les serveurs Web et les serveurs de base de données. Appliquez les deux types de protection, car si vous n'appliquez qu'un profil de protection de zone, une attaque DoS qui cible un système particulier de la zone ne peut alors réussir que si les Connections-Per-Second (connexions par seconde ; CPS) totales n'excèdent pas les taux **Activate (d'activation)** et **Maximum** de la zone.

La protection DoS consomme une grande quantité de ressources, ne l'utilisez donc que pour les systèmes critiques. Tout comme c'est le cas pour les profils de protection de zone, les profil de

protection de zone spécifient les seuils de saturation. Les règles de politique de protection DoS déterminent les périphériques, les utilisateurs, les zones et les services auxquels les profils DoS s'appliquent.

***En plus de configurer la protection DoS et la protection de zone, appliquez le** profil de protection contre les vulnérabilités exemplaire **à chaque règle de politique de sécurité pour vous aider à vous défendre contre les attaques DoS.***

- Protection DoS classée ou regroupée
- Profils de protection DoS
- Règles de la politique de protection DoS

## Protection DoS classée ou regroupée

Vous pouvez configurer une protection ***regroupée*** ou ***classée*** Profils de protection DoS et appliquer un profil ou un profil de chaque type Règles de la politique de protection DoS lorsque vous configurez la protection DoS.

- **Aggregate (Regroupé)** : Établit des seuils qui s'appliquent à l'ensemble du groupe de périphériques indiqué dans la règle de la politique de protection DoS plutôt qu'à chaque périphérique individuel, de sorte qu'un périphérique puisse recevoir la majorité du trafic de connexion autorisé. Par exemple, un **Max Rate (Taux maximum)** de 20 000 CPS indique que le CPS total du groupe est de 20 000, et un périphérique individuel peut recevoir un maximum de 20 000 CPS si d'autres périphériques ne disposent d'aucune connexion. Les politiques de protection DoS regroupées procurent une couche de protection globale (après votre périphérique DDoS dédié au niveau du périmètre Internet et les profils de protection de zone) pour un groupe particulier de périphériques critiques lorsque vous souhaitez appliquer des contraintes supplémentaires sur des sous-réseaux, des utilisateurs ou des services donnés.
- **Classified (Classés)** : Définit les seuils de saturation qui s'appliquent à chaque périphérique spécifié dans une règle de politique de protection DoS. Par exemple, si vous définissez un **Max Rate (Taux max)** de 5 000 CPS, chaque périphérique spécifié dans la règle peut accepter un maximum de 5 000 CPS avant d'abandonner de nouvelles connexions. Si vous appliquez une règle de politique de protection DoS classée à plusieurs périphériques, les périphériques régis par la règle devraient posséder une capacité similaire et vous devrez contrôler leurs taux CPS d'une manière analogue, car les seuils de protection classée s'appliquent à chaque périphérique individuel. Les profils classés protègent les ressources essentielles individuelles.

  Lorsque vous configurez une règle de politique de protection DoS avec un profil de protection DoS (**Option/Protection** > **Classified (Classée)** > **Address (Adresse)**), utilisez le champ **Address (Adresse)** pour spécifier si les connexions entrantes sont comptabilisées dans les seuils du profil selon la correspondance que vous établissez (**source-ip-only (adresse ip source seulement)**, **destination-ip-only (adresse ip de destination seulement)**, ou **scr-dest-ip-both (adresse ip de destination et adresse ip source)** (le pare-feu comptabilise les adresses IP source et de destination vers l'atteinte des seuils). Les compteurs consomment des ressources. La manière dont vous comptez les correspondances d'adresses affectera donc la consommation des ressources du pare-feu Vous pouvez utiliser une protection DoS classée pour :

  - protéger des périphériques essentiels individuels, en particulier les serveurs auxquels les utilisateurs accèdent à partir de l'Internet et qui sont souvent la cible d'attaques, tels que les serveurs Web, les serveurs de base de données et les serveurs DNS; définir des seuils de protection contre la saturation et de protection des ressources dans un profil de protection

DoS. Créez une règle de politique de protection DoS qui applique le profil à chaque adresse IP du serveur en ajoutant les adresses IP en tant que critères de destination de la règle, puis définissez la **Address (Adresse)** sur **destination-ip-only (adresse IP de destination seulement)**.

> *N'utilisez pas la classification **source-IP-only (adresse IP source uniquement)** ou **src-dest-ip-both (adresse IP source et de destination)** pour les zones connectées à Internet dans les règles de politique de protection DoS classées, car le pare-feu n'a pas la capacité de stocker des compteurs pour chaque adresse IP sur Internet. Augmentez le compteur du seuil pour les adresses IP source uniquement pour les règles applicables aux zones internes ou aux mêmes zones. Dans les zones du périmètre, utilisez **destination-ip-only (adresse ip de destination uniquement)**.*

- Surveiller le taux de CPS pour un hôte suspect ou un groupe d'hôtes (la zone qui contient les hôtes ne peut être orientée vers l'Internet). Définissez un seuil d'alarme approprié dans un profil de protection DoS classé pour vous aviser si un hôte initie un large nombre de connexions. Créez une règle de politique de protection DoS qui applique le profil au groupe d'adresses source ou aux adresses sources individuelles, puis définissez la **Address (Adresse)** sur **source-ip-only (adresse ip source uniquement)**. Examinez les hôtes qui initient suffisamment de nouvelles connexions pour déclencher l'alarme.

La manière dont vous configurez la **Address (Adresse)** (**source-ip-only (adresse ip source uniquement)**, **destination-ip-only (adresse ip de destination uniquement)** ou **src-dest-ip-both (adresse IP source et adresse IP de destination)**) pour les profils classés dépend de vos objectifs de protection DoS, de ce que vous protégez et de si les périphériques protégés soient dans des zones Internet.

> *Le pare-feu utilise plus de ressources pour faire le suivi de **src-dest-ip-both (adresse ip source et adresse IP de destination)** en tant que **Address (Adresse)** que pour faire le suivi de **source-IP-only (adresse ip source uniquement)** ou de **destination-ip-only (adresse ip de destination uniquement)**, parce que les compteurs consomment les ressources des adresses IP source et des adresses IP de destination, plutôt que celles de l'un seul des deux.*

Si vous appliquez un profil de protection DoS regroupé et un profil de protection DoS classé à la même règle de politique de protection DoS, le pare-feu applique le profil regroupé d'abord et applique ensuite le profil classé, au besoin. Par exemple, nous protégeons un groupe de cinq serveurs Web avec les deux types de profils dans une règle de politique de protection de DoS. La configuration des profils regroupés abandonne les nouvelles connexions lorsque le total combiné de tout le groupe atteint un **Max Rate (Taux max.)** de 25 000 CPS. La configuration des profils classés abandonne les nouvelles connexions vers un serveur Web individuel du groupe lorsqu'il atteint un **Max Rate (Taux max.)** de 6 000 CPS. Il existe trois scénarios où le trafic des nouvelles connexions traverse les seuils de **Max Rate (Taux max.)** :

- Le nouveau taux CPS dépasse le **Max Rate (Taux max.)** regroupé, mais n'excède pas le **Max Rate (Taux max.)** classé. Dans le présent scénario, le pare-feu applique le profil regroupé et bloque toutes les nouvelles connexions pour la durée du blocage configurée.
- Le nouveau taux CPS n'excède pas le **Max Rate (Taux max.)** regroupé, mais les CPS vers un des serveurs Web dépasse le **Max Rate (Taux max.)** classé. Dans le présent scénario, le pare-feu vérifie le profil regroupé et découvre que le taux du groupe est inférieur à 25 000 CPS. Ainsi, le pare-feu ne bloque pas les nouvelles connexions en fonction de cela. Ensuite, le pare-feu vérifie le profil classé et découvre que le taux d'un serveur particulier dépasse 6 000 CPS. Le pare-feu

applique le profil classé et bloque les nouvelles connexions à ce serveur particulier pour la durée du blocage configurée. Parce que les autres serveurs du groupe se situent dans les limites du **Max Rate (Taux max.)** du profil classé, leur trafic n'est pas affecté.

- Le nouveau taux CPS dépasse le **Max Rate (Taux max.)** regroupé et dépasse également le **Max Rate (Taux max.)** classé pour l'un des serveurs Web. Dans le présent scénario, le pare-feu vérifie le profil regroupé et découvre que le taux du groupe est supérieur à 25 000 CPS. Ainsi, le pare-feu bloque les nouvelles connexions afin de limiter les CPS totales du groupe. Le pare-feu vérifie ensuite le profil classé et découvre que le taux d'un serveur particulier dépasse 6 000 CPS (le profil regroupé applique donc la limite combinée du groupe, ce qui ne suffit toutefois pas à protéger ce serveur en particulier). Le pare-feu applique le profil classé et bloque les nouvelles connexions à ce serveur particulier pour la durée du blocage configurée. Parce que les autres serveurs du groupe se situent dans les limites du **Max Rate (Taux max.)** du profil classé, leur trafic n'est pas affecté.

*Si vous voulez qu'un profil de protection DoS regroupé et classé s'appliquent tous deux au même trafic, vous devez appliquer les deux profils à la même règle de politique de protection DoS. Si vous appliquez le profil regroupé à une règle et le profil classé à une autre règle, même si le même trafic est spécifié, le pare-feu ne peut appliquer qu'un seul profil. En effet, lorsque le trafic met la première règle de politique de protection DoS en correspondance, le pare-feu exécute l'**Action** indiquée dans cette règle et ne compare le trafic à aucune autre règle subséquente. Le trafic n'est donc jamais mis en correspondance avec la seconde règle, et le pare-feu ne peut appliquer son action. (Les règles de la politique de sécurité fonctionnent de la même manière.)*

## Profils de protection DoS

Des profils de protection DoS définissent des seuils de protection contre de nouvelles attaques par saturation basées sur des adresses IP et fournissent une protection des ressources (limites maximales de sessions simultanées pour des points de terminaison et ressources spécifiques). Les profils de protection DoS protègent des appareils spécifiques (profils classés) et des groupes de périphériques (profils regroupés) contre les attaques SYN, UDP, ICMP, ICMPv6 et les autres attaques par saturation IP. La configuration de seuils de protection contre les attaques par saturation dans un profil de protection DoS ressemble à la configuration de la Protection contre la saturation d'un profil de protection de zone, mais les profils de protection de zone protègent des zones d'entrée complètes, tandis que les profils et les règles de politique de protection DoS sont granulaires et ciblés et peuvent même être associés à un seul périphérique (adresse IP). Le pare-feu mesure la quantité agrégée Connections-Per-Second (connexions par seconde ; CPS) à un groupe de périphériques (profil regroupé) ou mesure le CPS aux périphériques individuels (profil classé).

*Mesurez et surveillez la consommation CPU du plan de données du pare-feu afin de vous assurer que chaque pare-feu est correctement dimensionné pour soutenir la protection DoS et la protection de la Zone et d'autres fonctions qui consomment les cycles CPU, telles que le déchiffrement. Si vous utilisez Panorama pour gérer vos pare-feu, la surveillance des pare-feu (**Panorama > Managed Devices (Périphériques gérés) > Health (Santé) > All Devices (Tous les périphériques)**) vous montre la consommation CPU et mémoire de chaque pare-feu géré. Elle peut également vous montrer une ligne de tendance de la consommation CUP moyenne et de l'utilisation maximale sur 90 jours pour vous aider à comprendre la capacité disponible de chaque pare-feu.*

Pour chaque type de saturation, vous définissez trois seuils pour les nouvelles CPS à un groupe de périphériques (regroupé) ou à des périphériques individuels (classé) ainsi qu'une **Block Duration (Durée du blocage)**, et vous pouvez définir une **Action** d'abandon pour les saturations SYN :

- **Alarm Rate (Taux d'alarme)** : lorsque les nouvelles connexions par seconde dépasse ce seuil, le pare-feu génère une alarme DoS. Définissez le taux des profils classés à 15 à 20 % au-delà du taux CPS moyen du périphérique, afin d'éviter que les fluctuations normales causent des alertes. Définissez le taux des profils regroupés à 15 à 20 % au-delà du taux CPS moyen du groupe.
- **Activate Rate (Taux d'activation)** : lorsque les nouvelles connexions par seconde dépasse ce seuil, le pare-feu commence à abandonner de nouvelles connexions pour atténuer la saturation jusqu'à ce que le taux des CPS tombe au-dessous du seuil. Pour les profils classés, le **Max Rate (Taux max.)** devrait correspondre à un taux CPS applicable au ou aux périphériques que vous protégez (le **Max Rate (Taux max.)** ne saturera pas le ou les périphériques critiques). Vous pouvez utiliser le même seuil pour le **Activate Rate (Taux d'activation)** que celui du **Max Rate (Taux max.)**. Ainsi, le pare-feu n'utilisera pas les cookies SYN ou RED avant d'abandonner le trafic avant qu'il n'atteigne le **Max Rate (Taux max.)**. Définissez le **Activate Rate (Taux d'activation)** à une valeur inférieure au **Max Rate (Taux max.)** uniquement si vous voulez abandonner le trafic avant qu'il n'atteigne le **Max Rate (taux max.)**. Pour les profils regroupés, définissez le seuil au-dessus du taux CPS maximal moyen du groupe pour commencer à atténuer les saturations au moyen de RED (ou de cookies SYN pour les attaques par saturation SYN).
- **Max Rate (Taux max.)** : lorsque les nouvelles connexions par seconde dépasse ce seuil, le pare-feu bloque (abandonne) toutes les nouvelles connexions provenant de l'adresse IP indésirable pour la période de **Block Duration (durée du blocage)** précisée. Pour les profils classés, basez le seuil du **Max Rate (Taux max.)** sur la capacité de votre ou vos périphériques que vous protégez pour que le taux CPS ne puisse les saturer. Pour les profils cumulés, fixez la valeur à 80-90 % de la capacité du groupe.
- **Block Duration (Durée du blocage)** : lorsque les nouvelles connexions par seconde dépassent le **Max Rate (Taux max.)**, le pare-feu bloque les nouvelles connexions provenant de l'adresse IP indésirable. La **Block Duration (Durée du blocage)** précise la durée pendant laquelle le pare-feu continue à bloquer les nouvelles connexions provenant de l'adresse IP. Pendant que le pare-feu bloque de nouvelles connexions, il ne compte pas les connexions entrantes et n'augmentent pas les compteurs du seuil. Pour les profils classés et regroupés, utilisez la valeur par défaut (300 secondes) pour bloquer la session qui attaque sans pénaliser les sessions légitimes provenant de la source pendant une période trop longue.

*La protection contre la saturation SYN est la seule pour laquelle vous définirez l'**Action** d'abandon. Commencez par définir l'**Action** sur **SYN Cookies (Cookies SYN)**. Les cookies SYN traitent le trafic légitime équitablement et n'abandonnent que le trafic qui échoue l'établissement de liaison SYN, tandis que l'utilisation du Random Early Drop (Abandon anticipé aléatoire ; RED) permet d'abandonner le trafic de manière aléatoire, ce qui veut dire que RED pourrait affecter le trafic légitime. Cependant, les cookies SYN exigent une consommation plus grande de ressources, parce que le pare-feu fait office de proxy pour le serveur cible et gère l'établissement de la connexion en trois étapes pour le serveur. La solution de compromis consiste à ne pas abandonner le trafic légitime (cookies SYN) pour préserver les ressources du pare-feu (RED). Surveillez le pare-feu, et si les cookies SYN consomment un trop grand nombre de ressources, passez au RED. Si vous ne disposez pas d'un périphérique de prévention DDoS dédié devant le pare-feu, utilisez toujours le RED comme mécanisme d'abandon.*

Les valeurs de seuil par défaut sont élevées pour que les profils de protection DoS n'abandonnent pas soudainement le trafic légitime. Surveillez le trafic de connexion et ajustez les seuils des valeurs d'une façon appropriée pour votre réseau. Commencez par prendre des mesures de référence des CPS moyennes et maximales pour chaque type de saturation pour déterminer les conditions de trafic normales pour les périphériques critiques que vous souhaitez protéger. Puisque le volume de trafic normal peut fluctuer, il vaut mieux ne pas abandonner les connexions trop brusquement. Surveillez et ajustez les seuils de saturation, au besoin, et au fur et à mesure de l'évolution de votre réseau.

Une autre méthode de définition des seuils de saturation consiste à utiliser les mesures de référence pour définir les CPS maximales que vous souhaitez autoriser et à partir de ces données pour dériver les taux d'activation et d'alarme permettant d'atténuer la saturation afin de la ramener à un niveau raisonnable.

*Les pare-feux équipés de processeurs à multiples plans de données (DPs) répartissent les connexions à travers les DPs. Habituellement, le pare-feu partage équitablement les réglages de seuils des CPS à travers ses DPs. Par exemple, si un pare-feu possède cinq DP et que vous définissez le* ***Alarm Rate (Taux d'alarme)*** *sur 20 000 CPS, chaque DP a un* ***Alarm Rate (Taux d'alarme)*** *de 4 000 CPS (20 000 / 5 = 4 000). S'il y a plus de 4 000 nouvelles sessions sur un DP, le* ***Alarm Rate (Taux d'alarme)*** *pour ce DP est alors déclenché.*

En plus de définir les seuils de saturation IP, vous pouvez également utiliser les profils de protection DoS pour détecter et prévenir les attaques par épuisement de sessions dans lesquelles un grand nombre d'hôtes (bots) établissent le plus grand nombre de sessions possible pour consommer les ressources de la cible. À l'onglet **Resources Protection (Protection des ressources)** du profil, vous pouvez définir le nombre maximal de sessions simultanées que le ou les périphériques définis dans la règle de politique de protection DoS auxquels vous appliquer le profil peut recevoir. Lorsque le nombre de sessions simultanées atteint sa limite maximale, les nouvelles sessions sont abandonnées.

Le nombre maximal de sessions simultanées à définir dépend du contexte de votre réseau. Comprenez le nombre de session simultanées que les ressources que vous protégez (définies dans la règle de politique de protection DoS à laquelle vous associez le profil) peuvent gérer. Établissez le seuil à environ 80 % de la capacité des ressources, puis surveillez le seuil et ajustez-le au besoin.

Pour les profils regroupés, le seuil de **Resources Protection (Protection des ressources)** s'applique à tous les périphériques définis dans la règle de politique (source et destination). Pour les profils classés, le seuil de **Resources Protection (Protection des ressources)** s'applique au trafic selon que la règle de politique classée s'applique à l'adresse IP source uniquement, à l'adresse IP de destination uniquement ou aux adresses IP source et de destination.

## Règles de la politique de protection DoS

Les règles de la politique de protection DoS contrôlent les systèmes auxquels le pare-feu applique la protection DoS (les seuils de saturation configurés dans les profils de protection DoS que vous associez aux règles de la politique de protection DoS), l'action à prendre lorsque le trafic correspond aux critères définis dans la règle et la manière de journaliser le trafic DoS. Comme la protection DoS consomme les ressources de pare-feu, utilisez-la uniquement pour défendre les ressources critiques spécifiques contre les saturations de session, tout particulièrement les cibles courantes auxquelles les utilisateurs accèdent depuis l'Internet, comme les serveurs Web et les serveurs de base de données. Utilisez les profils de protection de zone pour protéger des zones entières contre les attaques par saturations et les autres types d'attaques. Les règles de la politique de protection DoS procurent des

critères de correspondance granulaires, qui vous procurent la souplesse dont vous avez besoin pour définir exactement les éléments que vous souhaitez protéger :

- zone source, adresse IP (y compris des régions entières) et l'utilisateur;
- zone de destination et adresse IP (y compris des régions entières);
- services (selon le port et le protocole). La protection DoS s'applique uniquement aux services que vous spécifiez. Cependant, le fait de spécifier des services n'autorise pas les services et bloque implicitement tous les autres services. Lorsque vous spécifiez des services, la protection DoS est limitée à ces services. Cependant, les autres services ne sont pas bloqués.

***En plus de protéger les ports de service utilisés sur les serveurs critiques, vous pouvez également assurer la protection contre les attaques par déni de service sur les ports de service non utilisés des serveurs critiques. Pour les systèmes critiques, vous pouvez procéder en créant un profil et une règle de politique de protection DoS pour protéger les ports sur lesquels des services s'exécutent ainsi qu'un autre profil et une autre règle de politique de protection DoS pour protéger les ports sur lesquels aucun service ne s'exécute. Par exemple, vous pouvez protéger les ports de service normaux d'un serveur Web, tels que les ports 80 et 443, avec une seule politique/profil, et protéger l'ensemble des autres ports de service avec l'autre politique/profil. Soyez conscient de la capacité du pare-feu de sorte que le maintien des compteurs DoS n'ait aucune incidence sur la performance.***

Lorsque le trafic est mis en correspondance avec une règle de la politique de protection DoS, le pare-feu effectue l'une des actions suivantes :

- **Refus** : le pare-feu refuse l'accès et n'applique pas de profil de protection DoS. Le trafic qui correspond à la règle est bloqué.
- **Autorisation** : le pare-feu autorise l'accès et n'applique pas de profil de protection DoS. Le trafic qui correspond à la règle est autorisé.
- **Protection** : le pare-feu protège les périphériques définis dans la politique de protection DoS en appliquant les seuils du ou des profils de protection DoS spécifiés au trafic qui correspond à la règle. Une règle peut avoir un profil de protection DoS regroupé et un profil de protection DoS classé. Pour les profils classés, vous pouvez utiliser l'adresse IP source, l'adresse IP de destination, ou les deux pour augmenter les compteurs des seuils de saturation, comme décrit à la section Protection DoS classée ou regroupée. Les paquets entrants peuvent être pris en compte dans les seuils des deux profils de protection DoS s'ils correspondent à la règle.

Le pare-feu n'applique les profils de protection DoS que si l'**Action (Action)** est fixée sur **Protect (Protection)**. Si l'**Action (Action)** indiquée pour la règle de politique de protection DoS est **Protect (Protéger)**, indiquez les profils de protection DoS agrégés ou classés appropriés dans la règle pour que le pare-feu applique les seuils des profils de protection DoS au trafic qui correspond à la règle. La plupart des règles sont des règles de **Protect (Protection)**.

Les actions **Allow (Autoriser)** et **Deny (Refuser)** vous permettent de faire des exceptions au sein de grands groupes, mais n'appliquent pas la protection DoS au trafic. Par exemple, vous pouvez refuser le trafic provenant de plus d'un groupe, tout en autorisant un sous-ensemble de ce trafic. Inversement, vous pouvez autoriser le trafic provenant de plus d'un groupe, tout en refusant un sous-ensemble de ce trafic.

Vous pouvez **Schedule (Planifier)** le moment où une règle de la politique de protection DoS est active (heure de début, heure de fin, période de récurrence). Un cas d'utilisation de la planification

consiste à appliquer différents seuils de saturation à différentes périodes de la journée ou de la semaine. Par exemple, si votre entreprise subit une baisse considérable du trafic pendant la nuit (par rapport à la journée), vous pourriez souhaiter appliquer des seuils de saturation plus élevés pendant la journée, par rapport aux seuils que vous établissez pour la nuit. Une autre utilisation consiste à planifier des seuils spéciaux pour des événements spéciaux, pourvu que le pare-feu prenne en charge les taux de CPS.

Pour faciliter la gestion et l'établissement de rapports granulaires, configurez le **Log Forwarding (Transfert des journaux.)** pour séparer les journaux de protection DoS des autres journaux des menaces. Transférez les événements de non-respect des seuils DoS directement aux administrateurs par courriel en plus d'acheminer les journaux à un serveur, comme un serveur SNMP ou syslog. Si les pare-feu sont bien dimensionnés, le non-respect des seuils ne devrait pas se produire fréquemment et sera un indicateur fort d'une tentative d'attaque.

# Configuration de la protection de zone pour accroître la sécurité du réseau

Les rubriques suivantes fournissent des exemples de configuration de la protection de zone :

- Configuration de la protection contre la reconnaissance
- Configuration de la protection contre les attaques basées sur les paquets
- Configuration de la protection de protocole
- Configuration de la protection de la mémoire tampon des paquets
- Configuration de la protection de la mémoire tampon des paquets sur la base de la latence
- Configuration de la protection SGT Ethernet

## Configuration de la protection contre la reconnaissance

Configurez l'une des actions de Protection contre la reconnaissance suivantes que le pare-feu appliquera en réponse à la tentative de reconnaissance correspondante :

- **Allow (Autoriser)** : le pare-feu autorise la reconnaissance par l'analyse de ports ou le balayage d'hôtes pour poursuivre.
- **Alert (Alerter)** : le pare-feu génère une alerte pour chaque analyse de ports ou balayage d'hôtes correspondant au seuil configuré et dans l'intervalle de temps spécifié. Alert (Alerter) est l'action par défaut.
- **Block (Bloquer)** : le pare-feu supprime tous les paquets suivants entre la source et la destination pendant l'intervalle de temps restant spécifié.
- **Block IP (Blocage IP)** : le pare-feu supprime tous les paquets suivants pour la **Duration (Durée)** indiquée, en secondes (plage comprise entre 1 et 3 600). **Track By (Suivre en fonction de)** détermine si le pare-feu bloque le trafic source ou le trafic source et de destination.

**STEP 1 |** Configurez la protection contre la reconnaissance.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseaux)** > **Zone Protection (Protection de zone)**.
2. Sélectionnez un profil de protection de zone ou **Add (Ajoutez)** un nouveau profil et donnez-lui un **Name (Nom)**.
3. À l'onglet Reconnaissance Protection (Protection de reconnaissance), sélectionnez les types d'analyse contre lesquelles vous souhaitez vous protéger.
4. Sélectionnez une **Action (Action)** pour chaque analyse. Si vous sélectionnez Block IP (Blocage IP), vous devez également configurer l'option **Track By (Suivre en fonction de)** (source ou source et destination) et l'option **Duration (Durée)**.
5. Définissez l'**Interval (Intervalle)** en secondes. Cette option définit l'intervalle de temps pour la détection d'analyses de ports et de balayages d'hôtes.
6. Établissez le **Threshold (Seuil)**. Le seuil définit le nombre d'événements d'analyse de port ou de balayages d'hôtes qui peuvent se produire au cours de l'intervalle configuré ci-dessous avant de déclencher une action.

**STEP 2 |** (Facultatif) Configurez une exclusion d'adresse source.

1. À l'onglet Reconnaissance Protection (Protection de reconnaissance), **Add (Ajoutez)** une exclusion d'adresse source.
   1. Saisissez un **Name (Nom)** descriptif pour l'adresse à exclure.
   2. Définissez le type d'adresse sur **IPv4 (IPv4)** ou sur **IPv6 (IPv6)**, puis sélectionnez un objet d'adresse ou saisissez une adresse IP.
   3. Cliquez sur **OK**.
2. Cliquez sur **OK** pour enregistrer le profil de Protection de Zone.
3. **Commit (Validez)** vos modifications.

## Configuration de la protection contre les attaques basées sur les paquets

Pour accroître la sécurité d'une zone, la Protection contre les attaques basées sur des paquets vous permet d'indiquer si le pare-feu abandonne les paquets IP, IPv6, TCP, ICMP ou ICMPv6 qui possèdent certaines caractéristiques ou retire certaines options des paquets.

Par exemple, vous pouvez abandonner les paquets TCP SYN et SYN-ACK dont la charge utile contient des données lors d'une connexion en trois étapes. Un profil de protection de zone est configuré par défaut pour abandonner les paquets SYN et SYN-ACK contenant des données (vous devez appliquer le profil à la zone).

L'option TCP Fast Open (RFC 7413) préserve la vitesse de connexion en incluant des données dans la charge utile des paquets SYN et SYN-ACK. Un profil de protection de zone traite les connexions qui utilisent l'option TCP Fast Open distinctement des autres paquets SYN et SYN-ACK ; par défaut, le profil autorise les paquets d'établissement de liaison s'ils contiennent un cookie Fast Open valide.

***Si des profils de protection de zone sont déjà établis lorsque vous passez à PAN-OS 8.0, les trois paramètres par défaut s'appliqueront à chaque profil et le pare-feu agira en conséquence.***

À partir de PAN-OS 8.1.2 et des versions ultérieures, vous pouvez utiliser une commande de la CLI (étape 4 de cette tâche) pour permettre au pare-feu de générer un journal des menaces lorsque le pare-feu reçoit et abandonne les types suivants de paquets, pour que vous puissiez plus facilement analyser ces occurrences et également respecter les exigences en matière d'audit et de conformité :

- Attaque Teardrop
- Attaque DoS au moyen du ping de la mort

De plus, la même commande de la CLI permet au pare-feu de générer des journaux de menace pour les types de paquets suivants si vous activez la protection contre les attaques basées sur des paquets correspondante :

- paquets IP fragmentés ;
- adresse IP usurpée ;
- paquets ICMP supérieurs à 1 024 octets ;
- paquets composés de fragments ICMP ;
- paquets ICMP incorporés dans un message d'erreur ;

- premiers paquets d'une session TCP qui ne sont des paquets SYN .

**STEP 1 |** Créez un profil de protection de zone et configurez les paramètres de protection contre les attaques basées sur les paquets.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **Zone Protection(Protection des zones)** et **Add (Ajoutez)** un nouveau profil.
2. Donnez un **Name (Nom)** à la politique et saisissez éventuellement une **Description (Description)**.
3. Sélectionnez **Packet Based Attack Protection (Protection contre les attaques basées sur les paquets)**.
4. À chaque onglet (**IP Drop (Abandon d'IP)**, **TCP Drop (Abandon TCP)**, **ICMP Drop (Abandon de ICMP)**, **IPv6 Drop (Abandon d'IPv6)** et **ICMPv6 Drop (Abandon d'ICMPv6)**), sélectionnez les paramètres de protection contre les attaques basées sur les paquets que vous souhaitez appliquer pour protéger une zone.
5. Cliquez sur **OK**.

**STEP 2 |** Appliquez le profil de protection de zone à une zone de sécurité qui est affectée aux interfaces que vous souhaitez protéger.

1. Sélectionnez **Network (Réseau)** > **Zones (Zones)**, puis choisissez la zone dans laquelle vous souhaitez affecter le profil de protection de zone.
2. **Add (Ajoutez)** les **Interfaces (Interfaces)** qui appartiennent à la zone.
3. Pour **Zone Protection Profile (Profil de protection de zone)**, sélectionnez le profil que vous venez de créer.
4. Cliquez sur **OK**.

**STEP 3 |** **Commit (Validez)** vos modifications.

**STEP 4 |** (PAN-OS 8.1.2 et versions ultérieures) Activez la génération des journaux de menace d'une attaque Teardrop et d'une attaque DoS au moyen du ping de la mort sur le pare-feu. Générez également des journaux de menace pour les types de paquets énumérés ci-dessus si vous activez la protection contre les attaques basées sur les paquets (à l'étape 1). Par exemple, si vous activez la protection contre les attaques basées sur des paquets pour la **Spoofed IP address (Adresse IP usurpée)**, l'utilisation de la commande de la CLI suivante entraîne la génération, par le pare-feu, d'un journal des menaces lorsque le pare-feu reçoit et abandonne un paquet contenant une adresse IP usurpée.

1. Accédez à la CLI.
2. Utilisez la commande de la CLI opérationnelle **`set system setting additional-threat-log on`**. La valeur par défaut est **`off`** (désactivée).

## Configuration de la protection de protocole

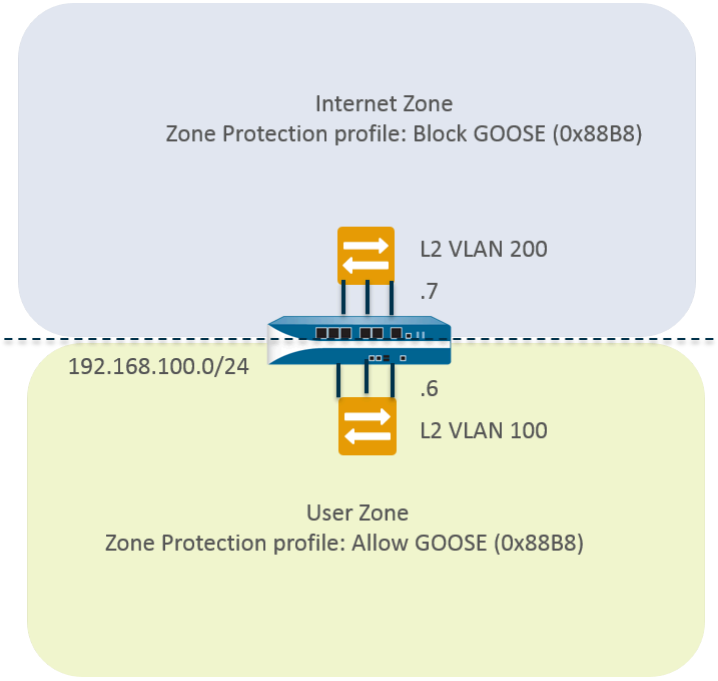
Protégez des zones de sécurité de câble virtuel ou de couche 2 contre les paquets de protocole non IP en utilisant la Protection du protocole.

- Cas d'utilisation : Protection de protocole non IP entre zones de sécurité sur des interfaces de Couche 2

## Cas d'utilisation : Protection de protocole non IP entre zones de sécurité sur des interfaces de Couche 2

Dans ce cas pratique, le pare-feu se trouve dans un VLAN de Couche 2 divisé en deux sous-interfaces. VLAN 100 est 192.168.100.1/24, sous-interface .6. VLAN 200 est 192.168.100.1/24, sous-interface .7. La protection de protocole non IP s'applique aux zones d'entrée. Dans ce cas pratique, si la zone Internet se trouve dans la zone d'entrée, le pare-feu bloque le protocole Generic Object Oriented Substation Event (Événement de sous-station orienté objet générique ; GOOSE). Si la zone utilisateur se trouve dans la zone d'entrée, le pare-feu autorise le protocole GOOSE. Le pare-feu autorise implicitement les trames marquées IPv4, IPv6, ARP et VLAN dans les deux zones.



**STEP 1 |** Configurez les deux sous-interfaces VLAN.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **VLAN (VLAN)** et choisissez **Add (Ajouter)** pour ajouter une interface.
2. **Interface Name (Nom de l'interface)** prend la valeur par défaut vlan. Après le point, saisissez 7.
3. Dans l'onglet **Config (Configuration)**, réglez **Assign Interface To (Affecter interface à)** sur le **VLAN (VLAN)** 200.
4. Cliquez sur **OK**.
5. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **VLAN (VLAN)** et choisissez **Add (Ajouter)** pour ajouter une interface.
6. **Interface Name (Nom de l'interface)** prend la valeur par défaut vlan. Après le point, saisissez 6.
7. Dans l'onglet **Config (Configuration)**, réglez **Assign Interface To (Affecter interface à)** sur le **VLAN (VLAN)** 100.
8. Cliquez sur **OK**.

**STEP 2 |** Configurez la protection de protocole dans un profil de protection de zone pour bloquer les paquets de protocole GOOSE.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **Zone Protection (Protection de zone)**, puis **Add (Ajouter)** un profil.
2. Saisissez le **Name (Nom)** Block GOOSE.
3. Sélectionnez **Protocol Protection (Protection de protocole)**.
4. Choisissez **Rule Type (Type de règle)** pour **Exclude List (Liste d'exclusions)**.
5. Saisissez le **Protocol Name (Nom de protocole)**, GOOSE, pour faciliter l'identification de l'Ethertype sur la liste. Le pare-feu ne vérifie pas si le nom que vous entrez correspond au code Ethertype, il n'utilise le code Ethertype qu'à des fins de filtrage.
6. Saisissez le code 0x88B8 pour **Ethertype**. Ethertype doit être précédé de 0x pour indiquer une valeur hexadécimale. La plage va de 0x0000 à 0xFFFF.
7. Sélectionnez **Enable (Activer)** pour appliquer la protection de protocole. Vous pouvez désactiver un protocole dans la liste, par exemple à des fins de test.
8. Cliquez sur **OK**.

**STEP 3 |** Appliquez le profil de protection de zone à la zone Internet.

1. Sélectionnez **Network (Réseau)** > **Zones (Zones)**, puis **Add (Ajouter)** pour ajouter une zone.
2. Saisissez le **Name (Nom)** de la zone, Internet.
3. Pour **Location (Emplacement)**, sélectionnez le système virtuel auquel la zone s'applique.
4. Pour le **Type (Type)**, sélectionnez **Layer2 (Couche 2)**.
5. **Add (Ajoutez)** l'**Interface (Interface)** qui appartient à la zone, vlan.7.
6. Pour **Zone Protection Profile (Profil de protection de zone)**, sélectionnez le profil Block GOOSE (Bloquer GOOSE).
7. Cliquez sur **OK**.

**STEP 4 |** Configurez la protection de protocole pour autoriser les paquets du protocole GOOSE.

Créez un autre profil de protection de zone nommé Allow GOOSE, et réglez **Rule Type (Type de règle)** sur **Include List (Liste d'inclusion)**.

*Lorsque vous configurez une liste d'inclusion, incluez tous les protocoles non IP requis ; une liste incomplète peut entraîner le blocage de trafic non IP légitime.*

**STEP 5 |** Appliquez le profil de protection de zone à la zone utilisateur.

1. Sélectionnez **Network (Réseau)** > **Zones (Zones)**, puis **Add (Ajouter)** pour ajouter une zone.
2. Saisissez le **Name (Nom)** de la zone, User (Utilisateur).
3. Pour **Location (Emplacement)**, sélectionnez le système virtuel auquel la zone s'applique.
4. Pour le **Type (Type)**, sélectionnez **Layer2 (Couche 2)**.
5. **Add (Ajoutez)** l'**Interface (Interface)** qui appartient à la zone, vlan.6.
6. Pour **Zone Protection Profile (Profil de protection de zone)**, sélectionnez le profil Allow GOOSE (Autoriser GOOSE).
7. Cliquez sur **OK**.

**STEP 6 |** Validez.

Cliquez sur **Commit (Valider)**.

**STEP 7 |** Affichez le nombre de paquets non IP que le pare-feu a perdus selon la protection de protocole.

Accédez à la CLI.

```
> show counter global name pkt_nonip_pkt_drop
> show counter global name pkt_nonip_pkt_drop delta yes
```

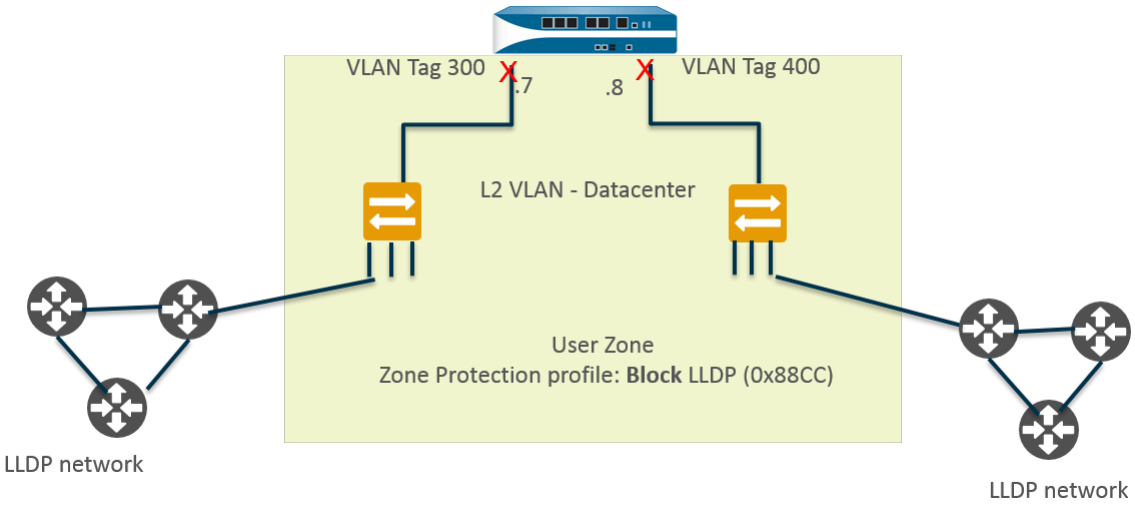
## Cas d'utilisation : Protection de protocole non IP dans une zone de sécurité sur des interfaces de Couche 2

Si vous n'implémentez pas de profil de protection de zone avec une protection de protocole non IP, le pare-feu autorise les protocoles non IP dans une seule zone à aller d'une interface de Couche 2 à une autre. Dans ce cas pratique, le blocage des paquets LLDP garantit que LLDP ne découvre pas un réseau accessible via une autre interface dans la zone.

Dans l'illustration suivante, le VLAN de Couche 2 nommé Datacenter est divisé en deux sous-interfaces : 192.168.1.1/24, sous-interface .7 et 192.168.1.2/24, sous-interface .8. Le VLAN appartient à la zone utilisateur. En appliquant un profil de protection de zone qui bloque LLDP dans la zone utilisateur :

- La sous-interface .7 bloque LLDP de son commutateur au pare-feu sur le X rouge sur la gauche, empêchant le trafic d'atteindre la sous-interface .8.
- La sous-interface .8 bloque LLDP de son commutateur au pare-feu sur le X rouge sur la droite, empêchant le trafic d'atteindre la sous-interface .7.




**STEP 1 |** Créez une sous-interface pour une interface Ethernet.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)** et sélectionnez une interface de Couche 2, dans cet exemple, ethernet1/1.
2. Sélectionnez **Add Subinterfaces (Ajouter sous-interfaces)**.
3. **Interface Name (Nom de l'interface)** prend pour défaut l'interface (ethernet 1/1). Après le point, saisissez 7.
4. Pour **Tag (Étiquette)**, saisissez 300.
5. Pour **Security Zone (Zone de sécurité)**, sélectionnez User (Utilisateur).
6. Cliquez sur **OK**.

**STEP 2 |** Créez une deuxième sous-interface pour l'interface Ethernet.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)** et sélectionnez l'interface de Couche 2, ethernet1/1.
2. Sélectionnez **Add Subinterfaces (Ajouter sous-interfaces)**.
3. **Interface Name (Nom de l'interface)** prend pour défaut l'interface (ethernet 1/1). Après le point, saisissez 8.
4. Pour **Tag (Étiquette)**, saisissez 400.
5. Pour **Security Zone (Zone de sécurité)**, sélectionnez User (Utilisateur).
6. Cliquez sur **OK**.

**STEP 3 |** Créez un VLAN pour l'interface de Couche 2 et deux sous-interfaces.

1. Sélectionnez **Network (Réseau)** > **VLANs (VLAN)**, puis **Add (Ajouter)** pour ajouter un VLAN.
2. Saisissez le **Name (Nom)** du VLAN, pour cet exemple, saisissez Datacenter.
3. Pour **VLAN Interface (Interface VLAN)**, sélectionnez **None (Aucune)**.
4. Pour **Interfaces**, cliquez sur **Add (Ajouter)** et sélectionnez l'interface de Couche 2 : ethernet1/1 et deux sous-interfaces : ethernet1/1.7 et ethernet1/1.8.
5. Cliquez sur **OK**.

**STEP 4 |** Bloquez les paquets des protocoles non IP dans le profil de protection de zone.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **Zone Protection (Protection de zone)**, puis **Add (Ajouter)** un profil.
2. Saisissez le **Name (Nom)**, dans cet exemple, Block LLDP.
3. Saisissez une **Description (Description)** de profil : Bloquez les paquets LLDP d'un réseau LLDP dans les autres interfaces de la zone (intrazone).
4. Sélectionnez **Protocol Protection (Protection de protocole)**.
5. Choisissez **Rule Type (Type de règle)** pour **Exclude List (Liste d'exclusions)**.
6. Saisissez le **Protocol Name (Nom de protocole)** LLDP.
7. Saisissez le code 0x88cc pour **Ethertype**. Ethertype doit être précédé de 0x pour indiquer une valeur hexadécimale.
8. Sélectionnez **Enable (Activer)**.
9. Cliquez sur **OK**.

**STEP 5 |** Appliquez le profil de protection de zone sur la zone de sécurité à laquelle le VLAN de Couche 2 appartient.

1. Sélectionnez **Network (Réseau)** > **Zones**.
2. Sélectionnez **Add (Ajouter)** pour ajouter une zone.
3. Saisissez le **Name (Nom)** de la zone, User (Utilisateur).
4. Pour **Location (Emplacement)**, sélectionnez le système virtuel auquel la zone s'applique.
5. Pour le **Type (Type)**, sélectionnez **Layer2 (Couche 2)**.
6. **Add (Ajoutez)** une **Interface (Interface)** qui appartient à la zone, ethernet1/1.7.
7. **Add (Ajoutez)** une **Interface (Interface)** qui appartient à la zone, ethernet1/1.8.
8. Pour **Zone Protection Profile (Profil de protection de zone)**, sélectionnez le profil Block LLDP (Bloquer LLDP).
9. Cliquez sur **OK**.

**STEP 6 |** Validez.

Cliquez sur **Commit (Valider)**.

**STEP 7 |** Affichez le nombre de paquets non IP que le pare-feu a perdus selon la protection de protocole.

Accédez à la CLI.

```
> show counter global name pkt_nonip_pkt_drop
> show counter global name pkt_nonip_pkt_drop delta yes
```

## Configuration de la protection de la mémoire tampon des paquets

Vous pouvez configurer la Packet Buffer Protection (Protection de la mémoire tampon des paquets) à deux niveaux : au niveau du périphérique (global) et, s'il est activé globalement, vous pouvez également l'activer au niveau de la zone. La protection de la mémoire tampon des paquets (**Device (Périphérique)** > **Setup (Configuration)** > **Session**) consiste à protéger les ressources du pare-feu et à veiller à ce que le trafic malveillant n'entraîne l'inactivité du pare-feu.

La protection de la mémoire tampon des paquets par zone d'entrée (**Network (Réseau)** > **Zones**) offre une deuxième couche de protection qui commence à bloquer l'adresse IP fautive si elle continue de dépasser les seuils de protection de la mémoire tampon des paquets. Le pare-feu peut bloquer tout le trafic de l'adresse IP source fautive. Souvenez-vous que si l'adresse IP source est une adresse IP NAT translatée, de nombreux utilisateurs pourraient utiliser la même adresse IP. Si un utilisateur malveillant déclenche la protection de la mémoire tampon et que la protection de la mémoire tampon est activée sur la zone d'entrée, tout le trafic provenant de l'adresse IP source (même d'utilisateurs non malveillants) peut être bloqué, quand le pare-feu met l'adresse IP dans sa block list.

Le moyen le plus efficace de bloquer les attaques DoS contre un service situé derrière le pare-feu est de configurer la protection de la mémoire tampon globalement et par zone d'entrée

Vous pouvez **activer la protection de la mémoire tampon** pour une zone, mais elle n'est pas active jusqu'à l'activation globale de la protection de la mémoire tampon et que les paramètres soient spécifiés

**STEP 1 |** Activer la protection de la mémoire tampon des paquets

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Session (Session)** et modifiez les Session Settings (Paramètres de session).
2. Sélectionnez la **protection de la mémoire tampon des paquets**.
3. Définir le comportement de la protection de la mémoire tampon
   - **Alert (%) (Alerte (%))** : lorsque l'utilisation de la mémoire tampon des paquets dépasse ce seuil pendant plus de 10 secondes, le pare-feu crée un journal d'événements toutes les minutes. La plage est comprise entre 0 et 99 ; la valeur par défaut est 50. Si la valeur est de 0 %, le pare-feu ne crée pas de journaux d'événements.
   - **Activer (%)** - Quand l'utilisation de la mémoire tampon atteint ce seuil, le pare-feu commence à mitiger les sessions les plus abusives en appliquant le Random Early Drop (RED) La plage est comprise entre 0 et 99 %; la valeur par défaut est 50 %. Si la valeur est de 0 %, le pare-feu n'applique pas la RED. Si l'attaquant arrive d'une zone qui a la protection de la mémoire tampon activée, le pare-feu peut aussi supprimer les sessions abusives ou bloquer l'adresse IP source offensante Commencez par la valeur de seuil par défaut et ajustez-la, au besoin.

     *Le pare-feu consigne les événements d'alertes dans le journal système et les événements relatifs à l'abandon de trafic, au rejet de sessions et au blocage d'adresses IP dans le journal des menaces.*
   - **Block Hold Time (sec) (Délai de maintien du blocage (sec))** : la période pendant laquelle une session atténuée par la RED est autorisée à se poursuivre avant qu'elle ne soit abandonnée par le pare-feu. La plage est comprise entre 0 et 65 535 ; la valeur par défaut est 60. Si la valeur est 0, le pare-feu n'abandonne pas les sessions en fonction de la protection de la mémoire tampon des paquets.
   - **Block Duration (sec) (Période de blocage (sec.))** : ce paramètre définit la durée pendant laquelle une session est rejetée ou une adresse IP est bloquée. La plage est comprise entre 1 et 15 999 999 ; la valeur par défaut est 3 600.
4. Cliquez sur **OK**.
5. **Commit (Validez)** vos modifications.

**STEP 2 |** Activez la protection de la mémoire tampon des paquets sur une zone d'entrée.

1. Sélectionnez **Network (Réseau)** > **Zones**.
2. Choisissez une zone d'entrée et cliquez sur son nom.
3. Cochez la case **Enable Packet Buffer Protection (Activer la protection de la mémoire tampon des paquets)** dans la section Zone Protection (Protection de zone).
4. Cliquez sur **OK**.
5. **Commit (Validez)** vos modifications.

## Configuration de la protection de la mémoire tampon des paquets sur la base de la latence

Configurez la protection de la mémoire tampon des paquets basée sur la latence et appliquez-la à des zones dont le trafic est constitué de protocoles et d'applications sensibles à la latence.

**STEP 1 |** Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Session**.

**STEP 2 |** Modifiez la section Session Settings (Paramètres de session) et activez la **Packet Buffer Protection (Protection de la mémoire tampon des paquets)**.

**STEP 3 |** Activez la **Buffering Latency Based (Mémoire tampon basée sur la latence)**.

**STEP 4 |** Saisissez le seuil **Latency Alert (millisecondes) (Alerte de latence)** au-dessus duquel le pare-feu commence à générer un événement de journal d'alerte toutes les minutes ; la plage est de 1 à 20 000 ; la valeur par défaut est 50.

**STEP 5 |** Saisissez le seuil **Latency Activate (millisecondes) (Activation de latence)** au-dessus de laquelle le pare-feu active l'abandon anticipé aléatoire (RED) sur les paquets entrants et commence à générer un journal d'activation toutes les 10 secondes ; la plage est de 1 à 20 000 ms ; la valeur par défaut est de 200 ms.

**STEP 6 |** Saisissez le seuil **Latency Max Tolerate (millisecondes) (Tolérance max de latence)** au-dessus de laquelle le pare-feu utilise RED avec une probabilité d'abandon proche de 100 % ; la plage est de 1 à 20 000 ms ; la valeur par défaut est de 500 ms.

Si al latence actuelle est une valeur comprise entre le seuil **Latency Activate (Activation de latence)** et le seuil **Latency Max Tolerate (Tolérance max de latence)**, le pare-feu calcule la probabilité d'abandon RED comme suit : (latence actuelle - seuil **Latency Activate (Activation de latence)**) / seuil (**Latency Max Tolerate (Tolérance max de latence)** - seuil **Latency Activate (Activation de latence)**). Par exemple, si la latence actuelle est 300, **Latency Activate (Activation de latence)** est 200, et **Latency Max Tolerate (Tolérance max de latence)** est 500, alors (300-200)/(500-200) = 1/3, ce qui signifie que le pare-feu utilise une probabilité d'abandon RED d'environ 33 %.

**STEP 7 |** Configurez le **Block Hold Time (Temps de maintien de blocage)** et la **Block Duration (Durée de blocage)** comme pour la Packet Buffer Protection (Protection de la mémoire tampon des paquets) en fonction de l'utilisation.

**STEP 8 |** Cliquez sur **OK**.

**STEP 9 |** Activez la deuxième couche de protection pour chaque zone où vous souhaitez une protection du tampon de paquets basée sur la latence.

1. Sélectionnez **Network (Réseau)** > **Zones (Zones)**, puis sélectionnez une zone.
2. Activation de la **Packet Buffer Protection (Protection de la mémoire tampon des paquets)**.

**STEP 10 |** **Commit** (Valider).

## Configuration de la protection SGT Ethernet

Utilisez la tâche suivante pour configurer un profil Protection SGT Ethernet.

**STEP 1 |** Créez un profil de protection de zone pour fournir la protection SGT Ethernet.

1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseaux)** > **Zone Protection (Protection de zone)**.
2. **Add (Ajoutez)** un profil de protection de zone par **Name (Nom)**.
3. Sélectionnez **Ethernet SGT Protection (Protection SGT Ethernet)**.
4. **Add (Ajoutez)** une **Layer 2 SGT Exclude List (Liste d'exclusion SGT de couche 2)** par nom.
5. Saisissez une ou plusieurs valeurs de **Tag (Étiquette)** pour la liste ; la plage est comprise entre 0 et 65535. Vous pouvez saisir des entrées individuelles qui constituent une plage contiguë de valeurs de balises (par exemple, 100-500). Vous pouvez ajouter jusqu'à 100 entrées d'étiquettes (individuelles ou par plage) dans une liste d'exclusion.
6. **Enable (Activez)** la liste d'exclusion SGT de couche 2. Vous pouvez désactiver la liste à tout moment.
7. Cliquez sur **OK**.

**STEP 2 |** Appliquez le profil de protection de zone sur la zone de sécurité à laquelle les inters de couche 2, câble virtuel ou Tap appartiennent.

1. Sélectionnez **Network (Réseau)** > **Zones**.
2. Sélectionnez **Add (Ajouter)** pour ajouter une zone.
3. Saisissez le **Name (Nom)** de la zone.
4. Pour **Location (Emplacement)**, sélectionnez le système virtuel auquel la zone s'applique.
5. Pour **Type**, sélectionnez **Layer2 (Couche 2)**, **Virtual Wire (Câble virtuel)** ou **Tap**.
6. **Add (Ajoutez)** une **Interface** qui appartient à la zone.
7. Pour **Zone Protection Profile (Profil de protection de zone)**, sélectionnez le profil que vous avez créé.
8. Cliquez sur **OK**.

**STEP 3 |** **Commit** (Valider).

**STEP 4 |** Consultez le compteur global de paquets que le pare-feu a abandonné en raison de tous les profils de protection de zone qui utilisent la protection SGT Ethernet.

1. Accédez à la CLI.
2. **`> show counter global name pan_flow_dos_l2_sec_tag_drop`**

# Protection DoS contre la saturation de nouvelles sessions

La protection DoS contre la saturation de nouvelles sessions est bénéfique contre les volumes importants d'attaques sur une session unique ou sur des sessions multiples. Dans une attaque sur une session unique, un pirate se sert d'une seule session pour cibler un périphérique derrière le pare-feu. Si une règle de sécurité autorise le trafic, la session est établie et le pirate lance une attaque en envoyant, à une très grande vitesse, des paquets ayant une adresse IP et un numéro de port source identiques, une adresse IP et un numéro de port de destination identiques et utilisant le même protocole en vue de submerger la cible. Dans une attaque sur des sessions multiples, un pirate se sert de plusieurs sessions (ou connexions par seconde [cps]) d'un seul hôte pour lancer une attaque DoS.

***Cette fonction permettra de vous protéger contre les attaques DoS de nouvelles sessions, c'est-à-dire, du trafic qui n'a pas encore été transféré au matériel. Cette fonction ne protège pas contre une attaque transférée. Cependant, cette rubrique décrit comment vous pouvez créer une règle de politique de sécurité qui permet de réinitialiser le client ; le pirate réinitialise l'attaque avec de nombreuses connexions par seconde et est bloqué par les défenses illustrées à cette rubrique.***

Règles de politique et profils de protection DoS travaillent de concert pour protéger de nombreux paquets SYN, UDP, ICMP et ICMPv6 entrants, et autres types de paquets IP, contre la saturation. Vous déterminez les seuils qui correspondent à une saturation. En général, le profil de protection DoS établit les seuils auxquels le pare-feu génère une alarme DoS, applique des actions comme l'abandon anticipé aléatoire et abandonne d'autres connexions entrantes. Une règle de politique de protection DoS configurée pour protéger (plutôt que pour autoriser ou refuser des paquets) détermine les critères de correspondance des paquets (tels que l'adresse source) afin d'être pris en compte dans les seuils. Cette flexibilité vous permet de bloquer certains trafics, ou d'autoriser certains trafics et de traiter d'autres trafics comme des trafics DoS. Lorsque le taux entrant est supérieur à votre seuil maximal, le pare-feu bloque le trafic en provenance de l'adresse source.

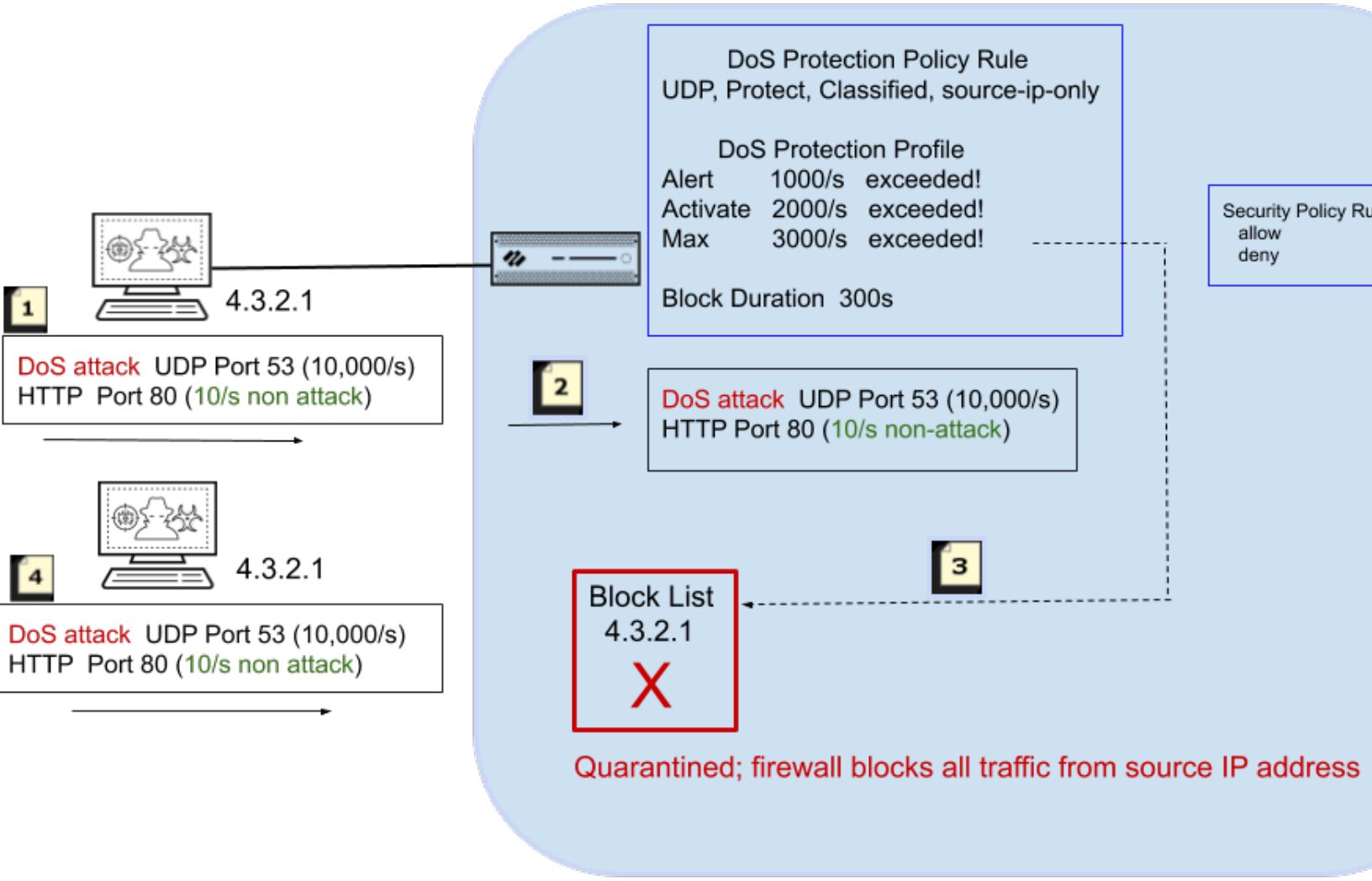
- Attaque DoS sur de multiples sessions
- Attaque DoS sur une session unique
- Configuration de la protection DoS contre la saturation de nouvelles sessions
- Mettre fin à une attaque DoS sur une session unique
- Identifiez les Sessions qui utilisent trop le descripteur de paquet sur puce
- Rejet d'une session sans validation

## Attaque DoS sur de multiples sessions

Configurez la protection DoS contre l'inondation de nouvelles sessions en configurant une règle de politique de protection DoS, qui détermine les critères qui, lorsqu'ils sont associés aux paquets entrants, déclenchent l'action **Protect**. Le profil de protection DoS compte toutes les nouvelles connexions jusqu'à ce qu'il atteigne les seuils du taux d'alerte, du taux d'activation et du taux maximal. Lorsque les nouvelles connexions entrantes par seconde dépassent le taux d'activation, le pare-feu prend l'action spécifiée dans le profil de protection DoS.

La figure et le tableau suivants décrivent dans un exemple l'interaction entre les règles de politique de sécurité, les règles de politique de protection DoS et le profil.



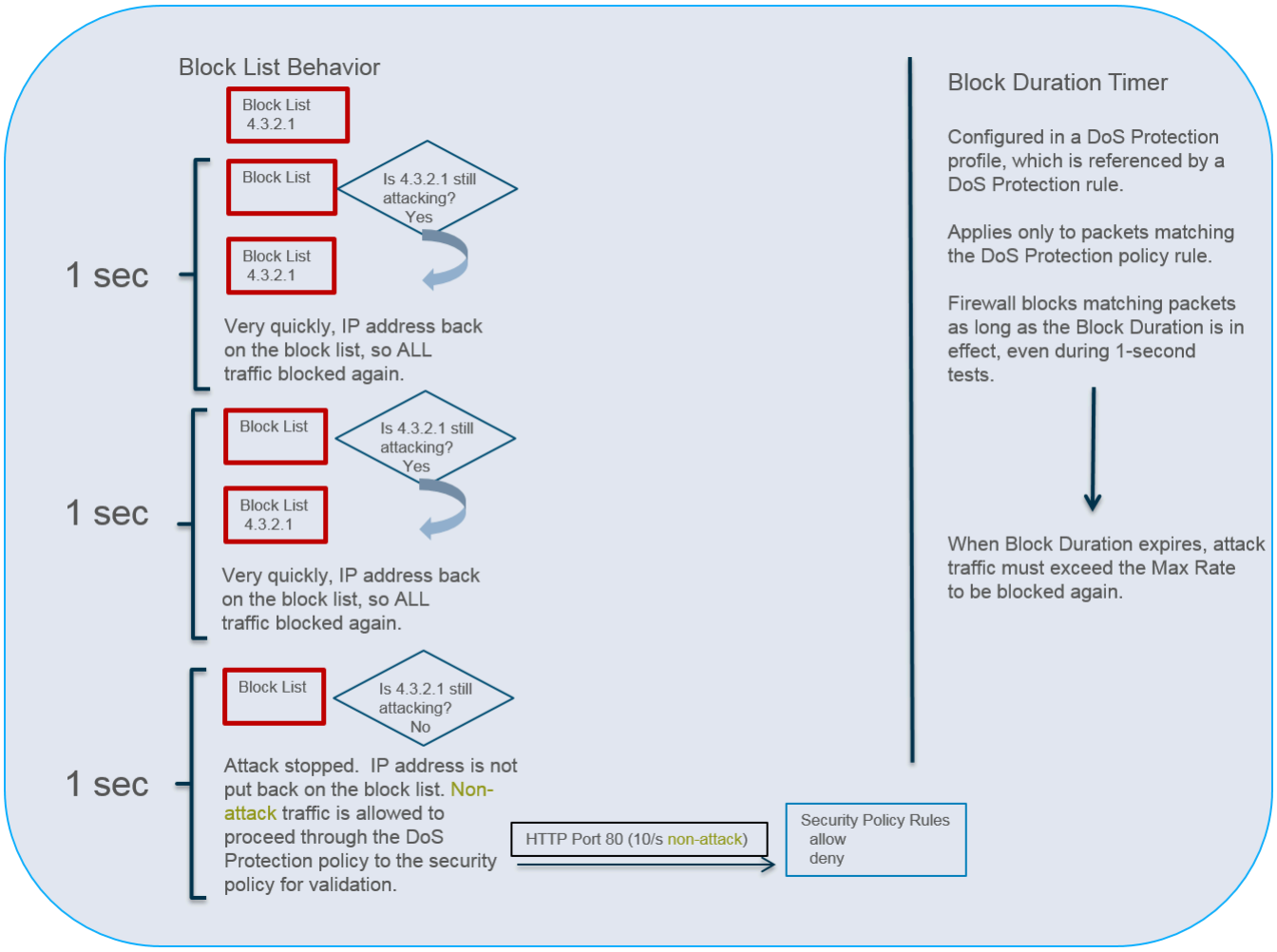

| Séquence d'événements lorsque le pare-feu place une adresse IP en quarantaine | |
|---|---|
| 1 | Dans le présent exemple, un pirate lance une attaque DoS à une vitesse de 10 000 nouvelles connexions par seconde au port UDP 53. Le pirate envoie également dix nouvelles connexions par seconde au port HTTP 80. |
| 2 | Les nouvelles connexions sont mises en correspondance avec des critères de la règle de politique de protection DoS, comme une interface ou une zone source, une adresse IP source, une interface ou une zone de destination, une adresse IP de destination ou un service, parmi d'autres paramètres. Dans cet exemple, la règle de politique précise UDP.<br><br>La règle de stratégie DoS Protection spécifie également l'action **Protect** et **Classified**, deux paramètres qui activent dynamiquement les paramètres du profil DoS Protection. Le profil de protection |

| Séquence d'événements lorsque le pare-feu place une adresse IP en quarantaine | |
|---|---|
| | DoS précise qu'un taux maximal de 3000 paquets par seconde est autorisé. Lorsque les paquets entrants correspondent à la règle de stratégie DoS Protection, les nouvelles connexions par seconde sont comptées pour les seuils **Alert (Alerte)**, **Activate (Activer)** et **Max Rate (Taux maximum)**.<br><br>*Vous pouvez également utiliser une règle de politique de sécurité pour bloquer tout le trafic provenant de l'adresse IP source si vous jugez qu'elle est malveillante en tout temps.* |
| 3 | Les 10 000 nouvelles connexions par seconde dépassent le seuil du **taux maximal**. Lorsque toutes les situations suivantes se produisent :<br>• le seuil est dépassé,<br>• une **Block Duration (durée de blocage)** est précisée, et<br>• **Classified (Classifié)** est défini de sorte à inclure l'adresse IP source,<br>le pare-feu place l'adresse IP source offensante sur la liste de blocage. |
| 4 | Une adresse IP figurant sur la liste de blocage est en quarantaine, ce qui signifie que tout le trafic provenant de cette adresse IP est bloqué. Le pare-feu bloque l'adresse IP source offensante avant que des paquets d'attaques supplémentaires n'atteignent la politique de sécurité. |

La figure suivante décrit de façon plus détaillée ce qui se produit après qu'une adresse IP qui correspond à la règle de politique de protection DoS est ajoutée à la liste de blocage. Elle décrit également le minuteur de la Durée de blocage.




Chaque seconde, le pare-feu autorise l'adresse IP à être retirée de la liste de blocage afin qu'il puisse tester les schémas de trafic et détermine si l'attaque se poursuit. Le pare-feu prend l'action suivante :

- Au cours de cette période d'essai d'une seconde, le pare-feu autorise les paquets qui ne correspondent pas au critère de la politique de protection DoS (le trafic HTTP dans le présent exemple) via les règles de politique de protection DoS de la politique de sécurité à des fins de validation. Très peu de paquets, voire aucun, ont le temps de passer, puisque le premier paquet d'attaques que le pare-feu reçoit après que l'adresse IP a été retirée de la liste de blocage sera mis en correspondance avec les critères de la politique de protection DoS, ce qui se traduira rapidement par le retour de l'adresse IP sur la liste de blocage pendant une autre seconde. Le pare-feu répète cet essai chaque second, jusqu'à ce que l'attaque cesse.
- Le pare-feu empêche tout le trafic d'attaque de passer les règles de politique de protection DoS (l'adresse reste sur la liste d'interdiction) jusqu'à l'expiration de la durée de blocage.

*Les vérifications aux secondes illustrées dans la figure précédente se produisent sur les modèles du pare-feu qui disposent de plusieurs processeurs de plan de données et un processus réseau matériel. Tous les systèmes de plan de données simples ou les systèmes sans processeur de réseau matériel effectuent cette atténuation dans le logiciel et utilisent un intervalle de cinq secondes.*

Lorsque l'attaque cesse, le pare-feu ne remet pas l'adresse IP sur la liste de blocage. Le pare-feu autorise le trafic qui ne constitue pas une attaque à passer les règles de politique de protection DoS pour se rendre aux règles de politique de sécurité à des fins d'évaluation. Vous devez configurer une règle de politique de sécurité, car, sans une telle règle, une règle de refus implicite bloque tout le trafic.

La liste de blocage se fonde sur une combinaison de zones sources et d'adresses sources. Ce comportement autorise l'existence d'adresses IP doubles, tant qu'elles se trouvent dans des zones différentes appartenant à des routeurs virtuels distincts.

Le paramètre Durée de blocage d'un profil de protection DoS précise la durée pendant laquelle le pare-feu bloque les paquets [offensants] qui correspondent à une règle de politique de protection DoS. Le trafic d'attaque demeure bloqué jusqu'à l'expiration de la durée de blocage, après quoi le trafic d'attaque doit de nouveau surpasser le seuil du taux maximal avant d'être bloqué à nouveau.

***Si le pirate utilise des sessions ou des robots multiples pour lancer des sessions d'attaque multiples, les sessions comptent dans le calcul des seuils établis pour le profil de protection DoS sans qu'une règle de refus de la politique de sécurité soit en place. Ainsi, une attaque sur une seule session exige l'existence d'une règle de refus de la politique de sécurité pour que chaque paquet compte dans le calcul des seuils ; ce n'est toutefois pas le cas d'une attaque sur des sessions multiples.***

Par conséquent, la protection DoS contre la saturation de nouvelles sessions autorise le pare-feu à défendre efficacement une adresse IP source tant que le trafic d'attaque se déroule et à permettre le trafic autre à traverser dès que l'attaque cesse. En plaçant l'adresse IP offensante sur la liste de blocage, vous permettez à la fonctionnalité de protection DoS de tirer profit de la liste de blocage, qui a été conçue pour mettre toutes les activités en quarantaine à partir de cette adresse IP source, tels que des paquets avec une application différente. La mise en quarantaine de l'adresse IP de toutes les activités procure une protection contre un pirate moderne qui tente une attaque d'applications rotative, dans le cadre de laquelle le pirate ne fait que passer aux applications pour initier une nouvelle attaque ou utilise une combinaison d'attaques diverses dans une attaque DoS hybride. Vous pouvez surveiller les adresses IP bloquées pour afficher la liste des blocs, en supprimer les entrées et obtenir des informations supplémentaires sur une adresse IP dans la liste des blocs.

***Depuis la version 7.0.2 de PAN-OS, le comportement du pare-feu a été modifié ; en effet, il place l'adresse IP source utilisée pour lancer l'attaque sur la liste de blocage. Lorsque l'attaque cesse, le trafic autre que d'attaque a l'autorisation de passer l'application des règles de politique de sécurité. Le trafic d'attaque qui a été mis en correspondance avec le profil de protection DoS et les règles de politique de protection DoS demeure bloqué jusqu'à l'expiration de la durée de blocage.***

## Attaque DoS sur une session unique

Une attaque DoS sur une session unique ne déclenchera généralement pas de profils de protection de zone ou DoS, puisqu'il s'agit d'attaques qui sont formées après que la session a été créée. Ces attaques sont autorisées par la politique de sécurité, parce qu'une session est autorisée à être créée, et, une fois la session créée, l'attaque fait grimper le nombre de paquets et rend le périphérique cible inactif.

Configuration de la protection DoS contre la saturation de nouvelles sessions pour assurer une protection contre la saturation de nouvelles sessions (saturation d'une session unique et de sessions

multiples). Dans l'éventualité où une attaque sur une session unique a cours, vous pouvez également faire l'Mettre fin à une attaque DoS sur une session unique.

## Configuration de la protection DoS contre la saturation de nouvelles sessions

**STEP 1 |** Configurez les règles de politique de sécurité de sorte à refuser le trafic provenant de l'adresse IP du pirate et à autoriser d'autre trafic, selon les besoins de votre réseau. Vous pouvez préciser n'importe quel critère de correspondance d'une règle de politique de sécurité, comme l'adresse IP source. (Obligatoire pour l'atténuation des attaques sur une session unique ou des attaques qui n'ont pas déclenché le seuil de la politique de protection DoS ; facultatif pour l'atténuation des attaques sur des sessions multiples).

*Il s'agit de l'une des étapes qu'il faut généralement effectuer pour mettre fin à une attaque qui a cours. Reportez-vous à la section* Mettre fin à une attaque DoS sur une session unique*.*

- Création d'une règle de politique de sécurité

**STEP 2 |** Configurez un profil de protection DoS afin d'assurer une protection contre la saturation.

*Étant donné que les attaques par saturation peuvent se produire sur de multiples protocoles, il est recommandé d'activer la protection pour tous les types de saturation dans le profil de protection DoS.*

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **DoS Protection (Protection DoS)** et **Add (Ajoutez)** un **Name (Nom)** de profil.
2. Comme **Type (Type)**, sélectionnez **Classified (Classé)**.
3. Pour procurer une **Flood Protection (Protection contre la saturation)**, sélectionnez tous les types de protection contre la saturation :
   - **saturation SYN**
   - **saturation UDP**
   - **Saturation ICMP**
   - **Saturation ICMPv6**
   - **Autre attaque par saturation IP**
4. Lorsque vous activer **SYN Flood (Saturation SYN)**, sélectionnez l'**Action (Action)** qui se produit lorsque les Connections Per Second (connexions par seconde ; cps) dépassent le seuil du **Activate Rate (Taux d'activation)** :
   1. **Random Early Drop (Abandon anticipé aléatoire)** : Le pare-feu se sert d'un algorithme pour progressivement abandonner ce type de paquet. Si l'attaque persiste, plus le taux cps entrant est élevé (supérieur au **Activate Rate (Taux d'activation)**), plus le nombre de paquets abandonnés par le pare-feu est élevé. Le pare-feu abandonne des paquets jusqu'à ce que le taux cps entrant atteigne le **Max Rate (Taux Max.)**. Lorsque cela se produit, le pare-feu abandonne toutes les connexions entrantes. **Random Early Drop** (Abandon anticipé aléatoire ; RED) est l'action par défaut de la **SYN Flood**

**(Saturation Syn)**, et la seule action de la **UDP Flood (Saturation UDP)**, de la **ICMP Flood (Saturation ICMP)**, de la **ICMPv6 Flood (Saturation ICMPv6)** et de la **Other IP Flood (Saturation des autres IP)**. Le RED est plus efficace que les cookies SYN et peut faire face à des attaques de plus grande importance ; il ne fait toutefois aucune distinction entre bon et mauvais trafic.

2. **SYN Cookies (Cookies SYN)** : plutôt que d'immédiatement envoyer le SYN au serveur, le pare-feu génère un cookie (pour le serveur) à envoyer au client dans le paquet SYN-ACK. Le client répond avec son ACK et le cookie ; après cette validation, le pare-feu envoie le SYN au serveur. L'action **SYN Cookies (Cookies SYN)** fait appel à un plus grand nombre de ressources du pare-feu que l'action **Random Early Drop (Abandon anticipé aléatoire)** ; il est plus exigeant, car il affecte le mauvais trafic.

5. (Facultatif) Sur chacun des onglets relatifs à la saturation, modifiez les seuils suivants afin de les adapter à votre environnement :

   - **Alarm Rate (connections/s) (Taux d'alarme (connexions/sec))** : précise le taux de seuil (cps) auquel une alarme DoS est générée. (Plage de 0 à 2 000 000 ; valeur par défaut : 10 000).
   - **Activate Rate (connections/s) (Taux d'activation (connexions/sec))** : précise le taux de seuil (cps) auquel une réponse DoS est activée. Lorsque le seul du **Activate Rate (Taux d'activation)** est atteint, le **Random Early Drop (Abandon anticipé aléatoire)** se produit. Plage de 0 à 2 000 000 ; valeur par défaut : 10 000. (Dans le cas de la saturation SYN, vous pouvez sélectionner les actions qui se produisent).
   - **Max Rate (connections/s) (Taux maximal (connexions/sec))** : précise le taux de seuil de connexions entrantes par seconde que le pare-feu autorise. Lorsque le seuil est dépassé, les nouvelles connexions qui arrivent sont abandonnées. La plage est comprise entre 2 et 2 000 ; la valeur par défaut est 40,000.

   *Les valeurs de seul définies par défaut à cette étape ne sont que des points de départ et pourraient ne pas convenir à votre réseau. Vous devez analyser le comportement de votre réseau afin de bien définir des valeurs de seuil initiales.*

6. Sur chacun des onglets relatifs à la saturation, indiquez la **Block Duration (Durée de blocage)** (en secondes). Il s'agit de la durée de temps pendant laquelle le pare-feu bloque les paquets qui correspondent à la règle de politique de protection DoS qui référence ce profil. Indiquez une valeur supérieure à zéro. (Plage de 1 à 21 600 ; valeur par défaut : 300).

   *Définissez une valeur de **Block Duration (Durée de blocage)** faible si vous craignez que des paquets que vous avez incorrectement identifiés en tant que trafic d'attaque puissent être bloqués inutilement.*

   Définissez une valeur de **Block Duration (Durée de blocage)** élevée si vous vous préoccupez davantage de bloquer des attaques importantes que de bloquer incorrectement des paquets qui ne font pas partie d'une attaque.

7. Cliquez sur **OK**.

**STEP 3 |** Configurez une règle de politique de protection DoS qui précise les critères de mise en correspondance du trafic entrant.

*Les ressources du pare-feu sont limitées. Il est donc préférable de ne pas effectuer de classement selon l'adresse source pour les zones ayant accès à Internet, car il peut y avoir un très grand nombre d'adresses IP uniques qui correspondent à la règle de la politique de protection DoS. De nombreux compteurs seraient alors nécessaires, et le pare-feu manquerait de ressources pour effectuer le suivi. Vous devez plutôt définir une règle de politique de protection DoS qui effectue un classement selon l'adresse de destination (du serveur que vous protégez).*

1. Sélectionnez **Policies (Politiques)** > **DoS Protection (Protection DoS)** et **Add (Ajoutez)** un **Name (Nom)** à l'onglet **General (Général)**. Celui-ci est sensible à la casse et peut comporter 31 caractères maximum, y compris des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement.
2. À l'onglet **Source (Source)**, choisissez **Zone (Zone)** ou **Interface (Interface)** pour définir le **Type (Type)**, puis **Add (Ajoutez)** la ou les zones ou interfaces. Sélectionnez la zone ou l'interface, selon votre déploiement et ce que vous voulez protéger. Par exemple, si vous n'avez qu'une interface arrivant sur le pare-feu, sélectionnez Interface (Interface).
3. (Facultatif) Pour la **Source Address (Adresse source)**, sélectionnez **Any (Indifférent)** pour que toute adresse IP entrante corresponde à la règle ou **Add (Ajoutez)** un objet d'adresse, comme une région géographique.
4. (Facultatif) Pour **Source User (Utilisateur source)**, sélectionnez **any (indifférent)** ou précisez un utilisateur.
5. (Facultatif) Sélectionnez **Negate (Ignorer)** pour faire correspondre n'importe quelles sources, sauf celles que vous précisez.
6. (Facultatif) À l'onglet **Destination (Destination)**, choisissez **Zone (Zone)** ou **Interface (Interface)** pour définir le **Type (Type)**, puis **Add (Ajoutez)** la ou les zones ou interfaces de destination. Par exemple, entrez la zone de sécurité que vous souhaitez protéger.
7. (Facultatif) Pour la **Destination Address (Adresse de destination)**, sélectionnez **Any (Indifférent)** ou entrez l'adresse IP du périphérique que vous souhaitez protéger.
8. (Facultatif) À l'onglet **Option/Protection (Option/Protection)**, **Add (Ajoutez)** un **Service (Service)**. Sélectionnez un service ou cliquez sur **Service (Service)** et saisissez un **Name (Nom)**. Sélectionnez **TCP (TCP)** ou **UDP (UDP)**. Saisissez un **Destination Port (Port de destination)**. En ne précisant pas de service particulier, vous permettez que la règle soit mise en correspondance avec une saturation de tout type de protocole sans égard au port d'une application.
9. À l'onglet **Option/Protection (Option/Protection)**, sous **Action (Action)**, sélectionnez **Protect (Protéger)**.
10. Sélectionnez **Classified (Classé)**.
11. Pour le **Profile (Profil)**, sélectionnez le nom du profil de **DoS Protection (Protection DoS)** que vous avez créé.
12. Pour l'**Address (Adresse)**, sélectionnez **source-ip-only (ip-source-uniquement)** ou **src-dest-ip-both (adresses-IP-source-et-de-destination-à-la-fois)**, afin de déterminer le type

d'adresses IP auxquelles la règle s'applique. Choisissez le paramètre selon la façon dont vous souhaitez que le pare-feu identifie le trafic offensant :

- Indiquez **source-ip-only (ip-source-uniquement)** si vous souhaitez que le pare-feu n'effectue le classement qu'en fonction de l'adresse IP source. Étant donné que les pirates testent souvent le réseau entier pour y trouver des hôtes à attaquer, le paramètre **source-ip-only (ip-source-uniquement)** est le paramètre type pour effectuer un examen général.
- Indiquez **src-dest-ip-both (adresses-IP-source-et-de-destination-à-la-fois)** si vous voulez procurer une protection contre les attaques DoS sur le serveur qui possèdent une adresse de destination particulière et que vous voulez également vous assurer que chaque adresse IP source ne dépassera pas un seuil de connexions par seconde défini pour ce serveur.

13. Cliquez sur **OK**.

**STEP 4 |** Validez.

Cliquez sur **Commit (Valider)**.

## Mettre fin à une attaque DoS sur une session unique

Pour atténuer une attaque DoS sur une session unique, vous devez tout de même procéder à la Configuration de la protection DoS contre la saturation de nouvelles sessions à l'avance. Après la configuration de cette fonction, une session pourrait être établie avant que vous vous rendiez compte qu'une attaque DoS (à partir de l'adresse IP de cette session) est en cours. Lorsque vous constatez qu'une attaque DoS sur une session unique a cours, exécutez la tâche suivante pour mettre fin à la session, afin que les prochaines tentatives de connexion à partir de cette adresse IP déclenchent la protection DoS contre la saturation des nouvelles sessions.

**STEP 1 |** Identifiez l'adresse IP source qui est à l'origine de l'attaque.

Par exemple, utilisez la fonctionnalité de capture de paquets du pare-feu avec un filtre de destination pour recueillir un échantillon du trafic qui se rend à l'adresse IP de destination. Vous pouvez également utiliser l'ACC pour filtrer sur l'adresse de destination afin de visualiser l'activité qui touche l'hôte cible faisant l'objet de l'attaque.

**STEP 2 |** Créez une règle de politique de protection DoS qui bloquera l'adresse IP du pirate après que les seuils d'attaques ont été dépassés.

**STEP 3 |** Créez une règle de politique de sécurité pour refuser l'adresse IP source et son trafic d'attaque.

**STEP 4 |** Mettez fin aux attaques provenant de l'adresse IP source qui en est à l'origine en exécutant la commande opérationnelle **clear session all filter source *<adresse-ip>***.

Si vous connaissez l'ID de session, vous pouvez également exécuter la commande **clear session id *<valeur>*** pour mettre fin à cette session uniquement.

*Si vous utilisez la commande **clear session all filter source *<adresse-ip>***, toutes les sessions correspondant à l'adresse IP source sont rejetées ; il peut s'agit de bonnes et de mauvaises sessions.*

Une fois que vous avez mis fin à la session d'attaque, les tentatives subséquentes visant à former une session d'attaque sont bloquées par la politique de sécurité. La politique de protection DoS compte toutes les tentatives de connexion dans le calcul des seuils. Lorsque le seuil du taux maximal est dépassé, l'adresse IP source est bloquée pendant la durée de blocage, tel que décrit à la section Attaque DoS sur des sessions multiples.

## Identifiez les Sessions qui utilisent trop le descripteur de paquet sur puce

Lorsqu'un pare-feu laisse présager que les ressources diminuent, il se peut que celui-ci soit victime d'une attaque qui envoie un nombre très élevé de paquets. Dans une telle situation, le pare-feu se met à mettre en tampon les paquets entrants. Vous pouvez rapidement identifier les sessions qui utilisent un pourcentage excessif du descripteur de paquet sur puce et atténuer leur effet en les ignorant.

Effectuez la tâche suivante sur n'importe quel modèle de pare-feu matériel (pas un pare-feu VM-Series) pour identifier, pour chaque emplacement et plan de données, le pourcentage du descripteur de paquet sur puce utilisé, les cinq principales sessions qui utilisent plus de deux pour cent du descripteur de paquet sur puce et les adresses IP sources associées à ces sessions. Une fois que vous disposez de ces informations, vous êtes plus à même de prendre la mesure qui s'impose.

**STEP 1 |** Affichez l'utilisation des ressources, les premières sessions et les détails des sessions du pare-feu. Exécutez la commande opérationnelle suivante dans la CLI (un exemple de résultat de la commande suit) :

```
admin@PA-7050> show running resource-monitor ingress-backlogs
-- SLOT:s1, DP:dp1 -- USAGE - ATOMIC: 92%  TOTAL: 93%
TOP SESSIONS:SESS-ID      PCT   GRP-ID   COUNT
6            92%   1        156                   7        1732
SESSION DETAILS SESS-
ID PROTO SZONESRC       SPORT  DST       DPORT  IGR-IF    EGR-
IF       APP
```

```
6    6     trust 192.168.2.35 55653  10.1.8.89 80  ethernet1/21
 ethernet1/22 undecided
```

La commande affiche, au plus, les cinq premières sessions qui utilisent, individuellement, 2 % ou plus du descripteur de paquet sur puce.

L'exemple de résultat présenté ci-dessus indique que la session 6 utilise 92 % du descripteur de paquet sur puce avec des paquets TCP (protocole 6) provenant de l'adresse IP source 192.168.2.35.

- **SESS-ID** : indique l'ID de session global qui est utilisé dans toutes les autres commandes **`show session`**. L'ID de session global est unique au sein du pare-feu.
- **GRP-ID** : indique une étape interne du traitement des paquets.
- **NOMBRE** : indique le nombre de paquets qui se trouvent dans ce GRP-ID pour cette session.
- **APP** : indique l'App-ID extrait des informations de session, ce qui peut vous aider à déterminer si le trafic est légitime. Par exemple, si les paquets utilisent un port TCP ou UDP commun, mais que le résultat de la CLI indique que l'APP est **`undecided`**, les paquets pourraient en fait être du trafic d'attaque. L'APP est **`undecided`** lorsque les décodeurs IP de l'application ne peuvent obtenir suffisamment d'information pour déterminer l'application. Si l'APP est **`unknown (inconnue)`**, cela indique que les décodeurs IP de l'application ne peuvent reconnaître l'application ; une session d'une APP **`unknown (inconnue)`** qui utilise un pourcentage élevé du descripteur de paquet sur puce est également suspecte.

Pour restreindre les résultats affichés :

Sur un modèle PA-7000 Series uniquement, vous pouvez restreindre les résultats à un emplacement, à un plan de données ou aux deux. Par exemple :

```
admin@PA-7050> show running resource-monitor ingress-backlogs slot
 s1
admin@PA-7050> show running resource-monitor ingress-backlogs slot
 s1 dp dp1
```

Sur les modèles PA-5200 Series et PA-7000, vous pouvez restreindre les résultats à un plan de données. Par exemple :

```
admin@PA-5260> show running resource-monitor ingress-backlogs dp
 dp1
```

**STEP 2 |** Servez-vous des résultats de la commande pour déterminer si l'adresse IP source utilisant un pourcentage élevé du descripteur de paquet sur puce envoie du trafic légitime ou d'attaque.

Dans l'exemple de résultat ci-dessus, une attaque sur une session unique est probablement en train de se produire. Une seule session (ID de session 6) utilise 92 % du descripteur de

paquet sur puce pour l'emplacement 1, le plan de données 1, et, à ce stade-ci, l'application est **undecided (non définie)**.

- Si vous déterminez qu'un seul utilisateur envoie une attaque et que le trafic n'est pas transféré, vous pouvez mettre fin à une attaque DoS sur une session unique. Vous pouvez au moins procéder à la configuration de la protection DoS contre la saturation de nouvelles sessions.
- Sur un modèle matériel qui possède un field-programmable gate array (réseau logique programmable ; FPGA), le pare-feu transfère le trafic au FPGA lorsque possible afin d'augmenter la performance. Si le trafic est transféré au matériel, la suppression de la session n'aide en rien, puisque, dans ce cas-là, c'est le logiciel qui doit gérer le barrage des paquets. Vous devriez plutôt passer au Rejet d'une session sans validation.

Pour voir si une session est transférée ou non, utilisez la commande opérationnelle **show session id *<id de session>*** dans la CLI, comme illustré à l'exemple suivant. La valeur

`layer7processing (traitement 7 couches)` indique `completed (terminé)` pour les sessions transférées ou `enabled (activé)` pour les sessions qui n'ont pas été transférées.

```
admin@PA-5060> show session id 68088184

Session        68088184

        c2s flow:
                source:      1.1.42.15 [trust]
                dst:         1.2.27.99
                proto:       6
                sport:       55993           dport:      6881
                state:       ACTIVE          type:       FLOW
                src user:    unknown
                dst user:    unknown
                offload:     Yes

        s2c flow:
                source:      1.2.27.99 [untrust]
                dst:         1.1.42.15
                proto:       6
                sport:       6881            dport:      55993
                state:       ACTIVE          type:       FLOW
                src user:    unknown
                dst user:    unknown
                offload:     Yes

        DP                                   : 2
        index(local):                        : 979320
        start time                           : Tue Oct 27 14:20:09 2015
        timeout                              : 1200 sec
        time to live                         : 1167 sec
        total byte count(c2s)                : 270
        total byte count(s2c)                : 270
        layer7 packet count(c2s)             : 3
        layer7 packet count(s2c)             : 3
        vsys                                 : vsys1
        application                          : bittorrent
        rule                                 : rule1
        session to be logged at end          : True
        session in session ager              : True
        session updated by HA peer           : False
        layer7 processing                    : completed
        URL filtering enabled                : False
        session via syn-cookies              : False
        session terminated on host           : False
        session traverses tunnel             : False
        captive portal session               : False
        ingress interface                    : ethernet1/21
        egress interface                     : ethernet1/22
        session QoS rule                     : N/A (class 4)
        tracker stage l7proc                 : ctd decoder bypass
        end-reason                           : unknown
```

Si la commande **show session id (afficher id de session)<*session-id*>** affiche des informations similaires aux suivantes, la sortie implique que la session n'a pas encore été installée sur le pare-feu PAN-OS. L'une des raisons pour lesquelles cela peut se produire est que le trafic est refusé en raison d'une règle de politique de sécurité configurée.

**> show session id (afficher id de session)*xxxxxxxxxx***

Session *xxxxxxxxxx*

Mauvaise clé: c2s: 'c2s' (Mauvaise clé)

Bad Key: s2c: ‘s2c’ (Mauvaise clé)

index(local): : *yyyyyyy*

# Rejet d'une session sans validation

Effectuez cette tâche pour rejeter de façon permanente une session, notamment une session qui overloading the packet buffer or on-chip packet descriptor surcharge le tampon de paquet ou le descripteur de paquet sur puce). Aucune validation n'est requise ; la session est rejetée immédiatement après que vous avez exécuté la commande. Les commandes s'appliquent aux sessions transférées et non transférées.

**STEP 1 |** Dans la CLI, exécutez la commande opérationnelle suivante sur n'importe quel modèle matériel :

```
admin@PA-7050> request session-discard [timeout <seconds>] [reason
 <reason-string>] id <session-id>
```

La délai par défaut est 3 600 secondes.

**STEP 2 |** Vérifiez que les sessions ont été rejetées.

```
admin@PA-7050> show session all filter state discard
```

# Certifications

Les rubriques suivantes décrivent comment configurer les pare-feu et les appareils Palo Alto Networks® pour prendre en charge les Critères Communs et les normes FIPS 140-2 (Federal Information Processing Standards 140-2), qui sont des certifications de sécurité assurant un ensemble standard de fonctionnalités et de garanties de sécurité. Ces certifications sont souvent requises par les organismes gouvernementaux américains civils et les entrepreneurs du gouvernement.

Pour obtenir des précisions, sur les certifications de produits et les validations de tiers, reportez-vous à la page consacrée aux certifications.

# Activation de la prise en charge des normes FIPS (Federal Information Processing Standard) et des Critères Communs

Les procédures suivantes vous permettent d'activer le mode FIPS-CC sur une version logicielle prenant en charge les Critères Communs et les normes FIPS 140-2 (Federal Information Processing Standard 140-2). Si vous activez le mode FIPS-CC, toutes les fonctionnalités FIPS et CC sont comprises.

Le mode FIPS-CC est pris en charge sur tous les appareils et pare-feu Palo Alto Networks de dernière génération, y compris les pare-feu VM-Series. Pour activer le mode FIPS-CC, vous devez d'abord démarrer le pare-feu dans le Maintenance Recovery Tool (Outil de récupération après maintenance ; MRT), puis faites passer le mode opérationnel du mode normal au mode FIPS-CC. La procédure à suivre pour changer le mode opérationnel est le même pour tous les pare-feu et les appareils, mais celle à suivre pour accéder au MRT diffère.

***Si vous activez le mode FIPS-CC, les paramètres d'usine par défaut du pare-feu seront rétablis et toute configuration sera alors supprimée.***

- Accès au Maintenance Recovery Tool (Outil de récupération après maintenance ; MRT)
- Passer en mode opérationnel FIPS-CC

## Accès au Maintenance Recovery Tool (Outil de récupération après maintenance ; MRT)

Le Maintenance Recovery Tool (Outil de récupération après maintenance ; MRT) vous permet d'effectuer plusieurs tâches sur les appareils et pare-feu Palo Alto Networks. Par exemple, vous pouvez rétablir les paramètres d'usine du pare-feu ou de l'appareil, revenir à une version antérieure de PAN-OS ou à une mise à jour de contenu antérieure, exécuter des diagnostics sur le système de fichiers, recueillir des renseignements sur le système et extraire des journaux. De plus, vous pouvez utiliser le MRT pour passer en mode opérationnel FIPS-CC ou pour passer du mode FIPS-CC au mode normal.

Les procédures suivantes décrivent la manière d'accéder au Maintenance Recovery Tool (Outil de récupération après maintenance ; MRT) sur divers produits Palo Alto Networks.

- Accédez au MRT sur les appareils et pare-feu matériels (comme les pare-feu PA-220 et PA-7000 Series ou les appareils M-Series).
  1. Établissez une session de console série vers le pare-feu ou l'appareil.
     1. Fixez un câble série à partir du port série de votre ordinateur au port console sur l'appareil ou le pare-feu.

        *Si votre ordinateur ne dispose d'aucun port série 9 broches, mais qu'il dispose d'un port USB, utilisez un convertisseur USB vers Série pour établir la connexion. Si le pare-feu possède un port console micro-USB, reliez-le au port à l'aide d'un câble USB-A à micro-USB standard.*
     2. Ouvrez le logiciel d'émulation de terminal de votre ordinateur et définissez les paramètres sur 9600-8-N-1, puis connectez-vous au port COM approprié.

        *Sur un système Windows, vous pouvez vous rendre dans le Panneau de configuration pour consulter les paramètres du port COM inscrits sous Périphériques et imprimantes en vue de déterminer le port COM qui est affecté à la console.*
     3. Connectez-vous au moyen d'un compte administrateur. (Le nom d'utilisateur et le mot de passe par défaut est admin/admin.)
  2. Saisissez la commande de la CLI suivante et appuyez sur **y** pour confirmer :

     ```
     debug system maintenance-mode
     ```
  3. Une fois que le pare-feu ou l'appareil ouvre l'écran d'accueil du MRT (délai d'environ deux ou trois minutes), appuyez sur la touche Entrée sur l'option **Continue** pour accéder au menu principal du MRT.

     *Vous pouvez également accéder au MRT en redémarrant le pare-feu ou l'appareil et en saisissant **maint** à l'invite du mode maintenance. Une connexion de port série directe à la console est nécessaire.*

     Une fois que le pare-feu ou l'appareil redémarre sous le MRT, vous pouvez accéder au MRT à distance en établissant une connexion SSH à l'adresse IP de l'interface de gestion (MGT). Lorsque l'invite de connexion apparaît, saisissez **maint** comme nom d'utilisateur et le numéro de série du pare-feu ou de l'appareil comme mot de passe.

- Accédez au MRT sur les pare-feu VM-Series déployés dans un cloud privé (comme VMware ESXi ou l'hyperviseur KVM).
  1. Établissez une session SSH vers l'adresse IP de gestion du pare-feu et connectez-vous à l'aide d'un compte utilisateur.
  2. Saisissez la commande de la CLI suivante et appuyez sur **y** pour confirmer :

     ```
     debug system maintenance-mode
     ```

     *Comptez environ 2 ou 3 minutes pour que le pare-feu redémarre dans le MRT. Pendant ce temps, votre session SSH se déconnectera.*
  3. Lorsque le pare-feu affiche l'écran d'accueil du MRT, connectez-vous selon le mode opérationnel :
     - **Mode normal** : établissez une session SSH vers l'adresse IP de gestion du pare-feu et connectez-vous en utilisant **maint** comme nom d'utilisateur et le numéro de série du pare-feu ou de l'appareil comme mot de passe.
     - **Mode FIPS-CC** : accédez à l'outil de gestion de la machine virtuelle (comme le client vSphere) et connectez-vous à la console de la machine virtuelle.
  4. Dans l'écran d'accueil du MRT, appuyez sur Entrée sur l'option **Continue** pour accéder au menu principal du MRT.

- Accédez au MRT sur les pare-feu VM-Series déployés dans le cloud public (comme AWS ou Azure).
  1. Établissez une session SSH vers l'adresse IP de gestion du pare-feu et connectez-vous à l'aide d'un compte utilisateur.
  2. Saisissez la commande de la CLI suivante et appuyez sur **y** pour confirmer :

     ```
     debug system maintenance-mode
     ```

     *Comptez environ 2 ou 3 minutes pour que le pare-feu redémarre dans le MRT. Pendant ce temps, votre session SSH se déconnectera.*
  3. Lorsque le pare-feu affiche l'écran d'accueil du MRT, connectez-vous selon le type de machine virtuelle :
     - **AWS** : connectez-vous en tant que **ec2-user** et sélectionnez la clé publique SSH qui a été affectée à la machine virtuelle lors de son déploiement.
     - **Azure** : entrez les informations d'identification que vous avez créées lors du déploiement du pare-feu VM-Series.
     - **GCP** : connectez-vous en tant que **gcp-user** et sélectionnez la clé publique SSH qui a été affectée à la machine virtuelle lors de son déploiement.
  4. Dans l'écran d'accueil du MRT, appuyez sur Entrée sur l'option **Continue** pour accéder au menu principal du MRT.

# Passer en mode opérationnel FIPS-CC

La procédure suivante décrit comment faire passer un produit Palo Alto Networks du mode opérationnel normal au mode FIPS-CC.

*Lorsque l'appareil est en mode FIPS-CC, vous ne pourrez configurer aucun paramètre via la console, y compris les paramètres de l'interface de gestion. Avant d'activer le mode FIPS-CC, assurez-vous que votre réseau est configuré pour autoriser l'accès à l'interface de gestion via SSH ou l'interface Web. L'interface de gestion utilisera par défaut une adresse statique de 192.168.1.1 si vous utilisez un pare-feu PA-Series ou une adresse récupérée via DHCP s'il s'agit d'un pare-feu VM-Series. Les appareils WildFire, Virtual Panorama et M-series Panorama auront par défaut une adresse statique de 192.168.1.1.*

*Une fois le mode FIPS-CC activé, toutes les configurations et tous les paramètres sont effacés. Si un administrateur a des configurations ou des paramètres qu'il souhaite réutiliser après l'activation du mode FIPS-CC, l'administrateur peut enregistrer et exporter la configuration avant de passer en mode FIPS-CC. La configuration peut ensuite être importée une fois le changement de mode de fonctionnement terminé. La configuration importée doit être modifiée conformément à* Fonctions de sécurité FIPS-CC *sinon le processus d'importation échouera.*

*Les clés, mots de passe et autres paramètres de sécurité critiques ne peuvent pas être partagés entre les modes.*

*Si vous modifiez le mode opérationnel d'un pare-feu ou d'un Collecteur de journaux dédié géré par un serveur de gestion Panorama en mode FIPS-CC, vous devez également modifier le mode opérationnel de Panorama en mode FIPS-CC. Ceci est nécessaire pour sécuriser les hachages de mot de passe pour les mots de passe d'administrateur local transmis depuis Panorama.*

**STEP 1 |** (Public Cloud VM-Series firewalls or Public Cloud Panorama Virtual Appliances only (Pare-feu Public Cloud VM-Series ou Appareils virtuels Public Cloud Panorama uniquement)) Créez une clé SSH et connectez-vous au pare-feu ou à Panorama.

Sur certaines plateformes de cloud public, telles que Microsoft Azure, vous devez disposer d'une clé SSH pour éviter un échec d'authentification après le passage en mode FIPS-CC. Vérifiez que vous avez déployé le pare-feu pour vous authentifier à l'aide de la clé SSH. Bien que vous puissiez déployer le pare-feu VM-Series ou Panorama sur Azure et vous connecter en utilisant un nom d'utilisateur et un mot de passe, vous ne pourrez pas vous authentifier en utilisant le nom d'utilisateur et le mot de passe après avoir modifié le mode opérationnel en FIPS-CC. Après être repassé en mode FIPS-CC, vous devez utiliser la clé SSH pour vous connecter et pouvoir ensuite configurer un nom d'utilisateur et un mot de passe que vous pourrez utiliser pour une connexion ultérieure à l'interface Web du pare-feu.

**STEP 2 |** Connectez-vous au pare-feu ou à l'appareil et Accès au Maintenance Recovery Tool (Outil de récupération après maintenance ; MRT).

**STEP 3 |** Dans le menu, sélectionnez **`Set FIPS-CC Mode`** (Définir le mode FIPS-CC).

**STEP 4 |** Sélectionnez **`Enable FIPS-CC Mode (Activer le mode FIPS-CC)`**. L'opération de changement de mode commence une réinitialisation complète des paramètres d'usine et

un indicateur d'état indique la progression. Une fois le changement de mode terminé, l'état `Success` s'affiche.

*Toutes les configurations et tous les paramètres sont effacés et ne peuvent pas être récupérés une fois le changement de mode terminé.*

**STEP 5 |** Lorsque vous y êtes invité, sélectionnez **`Redémarrer`**.

*Si vous modifiez le mode opérationnel d'un pare-feu VM-Series déployé dans le cloud public et que vous perdez votre connexion SSH au MRT avant de le **`redémarrer`**, vous devez attendre de 10 à 15 minutes pour que la modification de mode ait lieu ; connectez-vous de nouveau au MRT, puis redémarrez le pare-feu pour terminer l'opération. Après la réinitialisation en mode FIPS-CC, sur certains facteurs de forme virtuels (Panorama ou VM-Series), vous ne pouvez vous connecter qu'en utilisant la clé SSH, et si vous n'avez pas configuré l'authentification à l'aide d'une clé SSH, vous ne pouvez plus vous connecter au pare-feu au redémarrage.*

Une fois que vous êtes passé en mode FIPS-CC, l'état suivant s'affiche : `FIPS-CC mode enabled successfully`.

De plus, les modifications suivantes sont en vigueur :

- FIPS-CC s'affiche en permanence dans la barre d'état située en bas de l'interface Web.
- Les informations d'identification de connexion administrateur par défaut sont désormais admin/paloalto.

Consultez la section Fonctions de sécurité FIPS-CC pour obtenir des précisions sur les fonctions de sécurité qui s'appliquent en mode FIPS-CC.

# Fonctions de sécurité FIPS-CC

Lorsque le mode FIPS-CC est activé, les fonctions de sécurité suivantes sont appliquées sur tous les pare-feu et appareils :

- Pour vous connecter, le navigateur doit être compatible avec le protocole TLS 1.1 (ou toute version ultérieure) ; sur un appareil WF-500, l'appareil est géré uniquement via la CLI et vous devez vous connecter au moyen d'une application client compatible avec SSHv2.
- Tous les mots de passe doivent comporter huit caractères minimum.
- Dans les paramètres d'authentification, vous devez vous assurer que le **Failed Attempts (Nombre d'échecs de tentatives)** et le **Lockout Time (min) (Délai de verrouillage (en minutes))** sont supérieurs à 0. Si un administrateur atteint le seuil **Failed Attempts (Nombre d'échecs de tentatives)**, l'administrateur est verrouillé pour la durée définie dans le champ **Lockout Time (min) (Délai de verrouillage (en minutes))**.
- Dans les paramètres d'authentification, vous devez vous assurer que le **Idle Timeout (Délai d'inactivité)** est supérieur à 0. Si une session de connexion est inactive pendant une durée supérieure à la valeur indiquée, l'administrateur est automatiquement déconnecté.
- Vous pouvez configurer la **Absolute Session Length (Longueur absolue de session)** pour fixer la durée maximale en minutes pendant laquelle un utilisateur peut être connecté. La durée minimale qui peut être fixée est de 60 minutes. Vous recevrez un avertissement de fin de session 5 minutes avant l'expiration du délai. Cette fonction ne peut pas être désactivée en mode FIPS-CC et est activée par défaut lors d'une session de 30 jours.
- Vous pouvez configurer le **Max No. of Sessions (Nombre maximal de sessions)** pour déterminer combien d'utilisateurs peuvent être connectés simultanément au même compte d'administrateur.
- Le pare-feu ou l'appareil détermine automatiquement le niveau d'auto-test approprié et applique la force appropriée aux algorithmes cryptographiques et aux suites de cryptage.
- Les algorithmes non approuvés FIPS/CC ne sont pas décryptés et sont donc ignorés lors du décryptage.
- MS-CHAPv2 n'est pas compatible avec le mode FIPS-CC. Il est recommandé d'utiliser RADIUS avec TLS.
- Lors de la configuration d'un VPN IPSec, l'administrateur est invité à sélectionner une option Suite de cryptage.
- (Pour Panorama et WildFire uniquement) IPSec peut être activé sur l'interface de gestion pour protéger des protocoles tels que NTP, RADIUS, TACACS et DNS.
- Les certificats auto-générés et importés doivent contenir des clés publiques avec un cryptage RSA 2 048 bits (ou supérieur) ou ECDSA 256 bits (ou supérieur) ; vous devez également utiliser un résumé de l'algorithme SHA256 ou supérieur.

  *Vous ne pouvez pas utiliser un Module de sécurité matériel (HSM) pour stocker les clés ECDSA privées utilisées pour le décryptage du Proxy de transfert SSL ou l'Inspection SSL entrante.*
- Les connexions de gestion Telnet, TFTP et HTTP ne sont pas disponibles.
- Vous devez activer le chiffrement de la liaison de contrôle HA1. Vous devez définir les paramètres de resaisie automatique ; vous devez définir le paramètres de données sur une valeur qui ne

dépasse pas 1000 Mo (vous ne pouvez laisser la valeur par défaut) et vous devez définir un intervalle de temps (vous ne pouvez laisser l'intervalle désactivé).

- En mode FIPS-CC, le port de console série fonctionne comme port de sortie d'état uniquement ; l'accès à la CLI n'est pas disponible.
- Sur les pare-feu VM-Series matériels ou sur cloud privé qui ont été redémarrés dans le MRT, le port de console série offre un accès interactif au MRT.
- L'accès console interactif n'est pas pris en charge par les pare-feu VM-Series sur cloud privé hyperviseurs qui ont été redémarrés dans le MRT ; vous ne pouvez accéder au MRT qu'en utilisant SSH.
- Vous devez configurer manuellement une nouvelle master key (clé principale) avant l'expiration de l'ancienne clé principale ; la **Auto Renew Master Key (clé principale de renouvellement automatique)** n'est pas prise en charge en mode FIPS-CC.

  Si la clé principale expire, le pare-feu ou Panorama redémarre automatiquement en mode Maintenance. Vous devez alors effectuer le rétablissement des paramètres d'usine du pare-feu.
- Le mode Zero Touch Provisioning (ZTP) est désactivé sur le pare-feu PA-5450 et les pare-feux de la série PA-400 si le mode FIPS-CC est activé.
- (Panorama managed firewalls (Pare-feu gérés par Panorama)) Un pare-feu en mode FIPS-CC doit être géré par un serveur d'administration Panorama™ en mode FIPS-CC.

  La gestion d'un pare-feu en mode FIPS-CC n'est pas prise en charge pour un Panorama qui n'est pas en mode FIPS-CC.

# Nettoyage de la mémoire d'échange sur le pare-feu ou les appareils en mode FIPS-CC

Vous devez vous assurer que l'information sensible est supprimée de la mémoire d'échange avant de désaffecter un pare-feu ou un appareil (en mode FIPS-CC) ou avant de l'envoyer en réparation. Utilisez cette procédure pour supprimer tous les cryptographic security parameter (paramètres de sécurité cryptographiques ; CSP) de l'information à partir des partitions d'échange.

*Si vous envoyez un pare-feu qui est géré par Panorama à des fins de réparation, reportez-vous à la section* Avant de commencer le remplacement du pare-feu RMA.

**STEP 1 |** Ouvrez une session de gestion SSH sur le pare-feu ou l'appareil.

**STEP 2 |** Exécutez la commande opérationnelle suivante :

```
request [restart | shutdown] system with-swap-scrub [dod | nnsa]
```

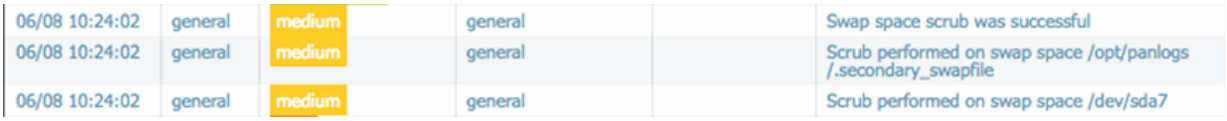
Par exemple, pour éteindre le pare-feu ou l'appareil et effectuer un nettoyage du Département de la Défense (DoD), exécutez la commande suivante :

```
request shutdown system with-swap-scrub dod
```

**STEP 3 |** Appuyez sur **Y** lorsque vous êtes invité à démarrer le nettoyage.

**STEP 4 |** Vérifiez que le nettoyage s'est terminé avec succès Affichez le journal **System (Système)**, puis filtrez sur le mot `swap`. Le journal **System (Système)** indique l'état du nettoyage pour chaque partition d'échange (soit une ou deux partitions selon le modèle) et affiche également une entrée de journal qui indique l'état global du nettoyage. Si le nettoyage s'est terminé avec succès sur toutes les partitions d'échange , le journal **System (Système)** affiche `Swap space scrub was successful`.

Si le nettoyage a échoué sur une ou plusieurs partitions d'échange, le journal **System (Système)** affiche `Swap space scrub was unsuccessful`. L'écran suivant présente les résultats du journal pour un pare-feu qui contient deux partitions.



| | | | | | |
|---|---|---|---|---|---|
| 06/08 10:24:02 | general | medium | general | | Swap space scrub was successful |
| 06/08 10:24:02 | general | medium | general | | Scrub performed on swap space /opt/panlogs /.secondary_swapfile |
| 06/08 10:24:02 | general | medium | general | | Scrub performed on swap space /dev/sda7 |

*Pour afficher les journaux de nettoyage au moyen de la CLI, exécutez la commande* ***`show log system | match swap`***.

*Si vous lancez le nettoyage au moyen de la commande d'arrêt, le pare-feu ou l'appareil s'éteindra une fois le nettoyage terminé. Avant de pouvoir allumer le pare-feu ou l'appareil, vous devez d'abord déconnecter et reconnecter la source d'alimentation.*