paloalto TECHDOCS

Politique de sécurité respectant les meilleures pratiques concernant le centre de données

Version 10.2

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

December 8, 2023

Table of Contents

Liste de vérification des meilleures pratiques de politique de sécurité concernant le centre de données

Les actifs les plus précieux de votre entreprise résident dans votre centre de données, notamment le code source propriétaire, la propriété intellectuelle et les données sensibles de l'entreprise et des clients. Vos clients et vos employés comptent sur vous pour préserver la confidentialité et l'intégrité de leurs données et s'attendent à ce que ces données soient toujours disponibles. Il est donc primordial de mettre en place une politique de sécurité exemplaire pour le centre de données, qui assure la protection de vos données et qui empêche les attaques concluantes. Il ne suffit pas de fortifier le périmètre parce que les attaques peuvent provenir de l'intérieur du réseau, de collaborateurs et sous-traitants dont les identifiants ont été compromis, et parce que, si un pirate informatique réussit à prendre pied dans votre réseau, il peut attaquer depuis l'intérieur du réseau en se déplaçant latéralement de périphérique en périphérique.

Si vous connaissez la plateforme Palo Alto Networks, vous pouvez gagner du temps en utilisant cette liste de contrôle simplifiée pour parcourir la planification préalable au déploiement, les activités de déploiement et la maintenance post-déploiement afin de mettre en œuvre et de maintenir les meilleures pratiques en matière de politique de sécurité du centre de données. Chaque section comprend des liens vers des informations détaillées dans le document Politique de sécurité des meilleures pratiques du centre de données ou dans le Guide de l'administrateur PAN-OS, notamment comment configurer les règles de politique, les profils de sécurité, la prévention des attaques DoS et l'authentification des utilisateurs, comment segmenter votre réseau, et plus.

- Planifiez votre déploiement respectant les meilleures pratiques du centre de données
- Meilleures pratiques relatives au déploiement du centre de données
- Meilleures pratiques concernant le suivi du déploiement du centre de données

Planifiez votre déploiement respectant les meilleures pratiques du centre de données

Préparez-vous à mettre en œuvre les meilleures pratiques dans votre centre de données en développant une stratégie et un plan de déploiement. Utilisez un renforcement positif de la sécurité (créez des règles autorisant le trafic utilisateur et le trafic application que vous voulez autoriser et qui refusent tout le reste), pour atteindre une architecture Zéro Confiance.

STEP 1 | Fixez des objectifs.

- ❑ Définissez l'état futur idéal du réseau de votre centre de données pour vous donner des objectifs concrets à atteindre et sachez identifier quand vous avez atteint ces objectifs.
- ❑ Protégez les flux de trafic de chaque zone d'où proviennent les connexions.
  1. Trafic d'utilisateurs locaux circulant vers le centre de données.
  2. Le trafic circulant depuis Internet vers le centre de données.
  3. Le trafic circulant du centre de données vers Internet.
  4. Trafic circulant entre les serveurs ou les machines virtuelles au sein du centre de données (trafic est-ouest au sein du centre de données).
- ❑ N'autorisez pas de trafic, d'utilisateurs ou d'applications inconnus dans votre centre de données
- ❑ Créez une conception standardisée et évolutive que vous pouvez reproduire et appliquer de manière cohérente dans tous les centres de données.

STEP 2 | Collaborez avec les parties prenantes telles que le département informatique/support informatique/sécurité informatique, ainsi que les groupes nécessitant un accès au centre de données comme l'ingénierie, le juridique, la finance et la DRH, avec comme objectif de développer une stratégie d'accès.

- ❑ Identifiez les utilisateurs ayant des besoins d'accès, ainsi que les ressources auxquelles ils doivent accéder. Comprendre cela vous permet de créer des groupes d'utilisateurs basés sur les besoins en niveaux d'accès afin de concevoir des règles de politique de sécurité efficaces par groupe d'utilisateurs.
- ❑ Identifiez les applications que vous souhaitez autoriser (approuver) dans le centre de données. Afin de réduire la surface d'attaque, approuvez uniquement des applications requises pour des raisons commerciales.

STEP 3 | Évaluez votre centre de données pour comprendre son état actuel afin de pouvoir créer un plan pour transformer la sécurité du centre de données vers l'état futur souhaité.

- ❑ Dressez l'inventaire de l'environnement matériel et virtuel et des ressources, y compris :
  - ❑ Serveurs, routeurs, commutateurs, périphériques de sécurité, équilibreurs de charge et autres infrastructures réseau.
  - ❑ Les applications standard et les applications personnalisées propriétaires ainsi que les comptes de service qu'ils utilisent pour communiquer. Comparez la liste d'applications dans l'inventaire et la liste d'applications que vous voulez approuver.

    Concentrez-vous sur les applications que vous souhaitez autoriser, car vos règles de politique de sécurité relatives à l'autorisation des applications les autorisent et refusent par défaut toutes les autres applications dans le but de réduire la surface d'attaque. Mappez les applications aux besoins de l'entreprise. Si une application n'est pas attribuée à un besoin commercial, demandez-vous si vous devez vraiment l'autoriser.
  - ❑ Évaluez chaque actif pour déterminer lesquels protéger en priorité. Demandez-vous notamment, « Qu'est-ce qui définit et distingue notre entreprise ? », « Quels systèmes doivent être disponibles pour les opérations courantes ? », et « Si je perds telle ressource, quelles seront les conséquences ? »a
- ❑ Collaborez avec des architectes d'applications, des architectes réseau et des architectes d'entreprise, ainsi que des représentants commerciaux, pour qualifier les flux de trafic du centre de données et en savoir plus sur les charges de base du trafic ainsi que ses modèles, pour comprendre ainsi le comportement habituel du réseau. Utilisez les widgets du Centre de Commande de l'Application et les outils d'analyse du trafic pour étudier le trafic de base.

STEP 4 | Créez une stratégie de segmentation du centre de données pour empêcher un programme malveillant ayant réussi à prendre pied dans le centre de données de se déplacer latéralement pour infecter d'autres zones.

- ❑ Utilisez les pare-feu comme des passerelles de segmentation afin d'apporter de la visibilité dans le trafic et les systèmes du centre de données, afin de contrôler de manière minutieuse qui est autorisé à utiliser quelles applications pour accéder à quels périphériques. Segmentez et sécurisez les serveurs non virtualisés avec des pare-feu matériels ainsi que le réseau virtuel avec des pare-feu VM-Series.
- ❑ Utilisez les flexibles outils de segmentation du pare-feu comme les zones, les groupes d'adresses dynamiques, App-ID et User-ID, afin de concevoir une stratégie de segmentation granulaire pour assurer la protection de serveurs et données.
- ❑ Regroupez les actifs qui remplissent des fonctions similaires et nécessitent le même niveau de sécurité dans le même segment.
- ❑ Segmentez les applications du centre de données en segmentant les couches serveurs constituant une couche d'applications (spécifiquement, une chaîne de service composée d'une couche de serveur web, une couche de serveur d'applications, et d'une couche de serveur de base de données) et en utilisant le pare-feu pour contrôler et inspecter le trafic entre les couches.
- ❑ Envisagez l'utilisation d'une solution SDN au cœur du centre de données pour bénéficier d'une infrastructure virtualisée flexible qui optimise l'utilisation des ressources et qui rend les automatisations et les mises à l'échelle plus faciles.

STEP 5 | Prévoyez d'utiliser une méthodologie respectant les meilleurs pratiques pour inspecter l'ensemble du trafic du centre de données afin d'obtenir une visibilité totale, de réduire la surface d'attaque, et empêcher des menaces connues et inconnues.

- ❑ Positionnez les pare-feu matériels et virtuels aux endroits où ils peuvent voir l'ensemble du trafic du réseau du centre de données.
- ❑ Exploitez la puissante boîte à outils du pare-feu pour créer des règles de politique de sécurité basées sur les applications liées à des groupes d'utilisateurs spécifiques et protégées par des profils de sécurité. Transférez les fichiers inconnus vers WildFire et déployez le décryptage pour empêcher les menaces de pénétrer dans le centre de données via le trafic crypté.
- ❑ Utilisez GlobalProtect en mode interne comme une passerelle pour contrôler l'accès au centre de données.
- ❑ Authentifiez les utilisateurs pour empêcher les accès non autorisés et configurez l'authentification multifactorielle pour l'accès aux applications, services et serveurs sensibles, particulièrement pour les sous-traitants, collaborateurs, et autres tierces parties nécessitant un accès à votre centre de données.
- ❑ Gérez les pare-feu de manière centralisée avec Panorama pour appliquer des politiques cohérentes à travers des environnements matériels et virtuels et pour une visibilité centrale.
- ❑ Si vous avez plusieurs centres de données, réutilisez les modèles et les piles de modèles pour appliquer votre politique de sécurité de manière cohérente sur différents emplacements.

STEP 6 | Déployez progressivement vos meilleures pratiques au fil du temps ; commencez par vous concentrer sur les menaces les plus probables pour votre entreprise et votre réseau, et protégez d'abord vos actifs les plus précieux.

Prendre en compte l'ensemble des utilisateurs, des applications, des périphériques et des flux de trafic du centre de données, et créer ensuite une politique de sécurité respectant les meilleures pratiques qui englobe le tout peut sembler une tâche écrasante si vous essayez de tout faire en même temps. Pourtant, en commençant par protéger vos ressources les plus précieuses et en planifiant une mise en place progressive et graduelle, vous pouvez effectuer une transition en douceur, et de manière pratique, d'une politique de sécurité, qui mise sur le hasard, à une politique de sécurité, respectant les meilleures pratiques et autorisant de manière sécurisée applications, utilisateurs et contenu.

Meilleures pratiques relatives au déploiement du centre de données

Mettez en place des pratiques exemplaires dans votre centre de données lorsque vous créez profils de Sécurité, profils de Décryptage, règles de politique de Sécurité, règles de politique d'Authentification et règles de politique de décryptage.

Pour les règles de politique de Sécurité, d'Authentification, et DoS, configurez le transfert de journaux *vers Panorama ou vers un service externe dans le but de centraliser les journaux pour une visualisation et une analyse plus pratiques, avec notifications.*

- Objets, politiques et actions générales du centre de données—Créez des applications propres à l'entreprise pour identifier et contrôler les applications propriétaires avec une politique de sécurité dans le centre de données, configurez des profils de sécurité stricts (antivirus, antispyware, protection contre les vulnérabilités, blocage de fichiers et analyse WildFire), configurez des profils et des politiques de décryptage stricts, bloquez le trafic que vous savez être malveillant ou inutile, et installez l'agent Cortex XDR sur les terminaux pour les protéger.
- Politiques relatives au trafic entre l'utilisateur et le centre de données : configurez des règles de politique de sécurité strictes pour autoriser uniquement l'accès approprié, garantir que les utilisateurs sont authentifiés et déchiffrer le trafic.
- Politiques relatives au trafic d'Internet vers le centre de données : prévenez les risques tels que le téléchargement de logiciels malveillants depuis un serveur externe infecté, l'installation de logiciels malveillants de commande et contrôle sur les terminaux du centre de données, l'autorisation d'accès involontaire et les attaques DoS destinées à perturber la disponibilité du centre de données.
- Politiques relatives au trafic du centre de données vers Internet : prévenez les risques tels que l'exfiltration de données, les logiciels malveillants de commande et contrôle qui tentent d'accéder à Internet et de contacter leur base, ainsi que d'autres logiciels malveillants sur des serveurs compromis qui tentent de télécharger encore plus de logiciels malveillants.
- Politiques relatives au trafic au sein du centre de données : prévenez le mouvement latéral des logiciels malveillants, autorisez uniquement les applications sanctionnées nécessaires à l'entreprise, et décryptez et journalisez le trafic.
- Tri de la base de règles de la politique de sécurité du centre de données : l'ordre des règles dans la base de règles de politique de sécurité est critique, car une fois que le trafic correspond à une règle, le pare-feu exécute l'action de la règle sur le trafic et aucune autre action ne se produira sur le trafic, et en raison de l'effet d'ombredes règles ; suivez les Meilleures pratiques en matière de base de règles de politique de sécurité pour éviter l'effet d'ombre et comprendre comment trier la base de règles.

Objets, politiques et actions générales du centre de données

Assurez-vous que vous pouvez protéger les applications propre à l'entreprise si vous les utilisez. Configurez les profil de sécurité et les profil de décryptage et installez Cortex XDR Agent sur tous les terminaux du centre de données.

- Application propre à l'entreprise
- Profils de sécurité

- Profils de décryptage
- Règles de blocage du trafic
- Installez Cortex XDR Agent sur les terminaux

STEP 1 | Si l'inventaire d'applications de votre centre de données comprend des applications propriétaires personnalisées, procédez alors à la création d'applications personnalisées pour ces applications, afin de les spécifier dans votre politique de Sécurité.

STEP 2 | Configurez des profils de Sécurité stricts respectant les meilleures pratiques pour le centre de données, pour empêcher des menaces de déstabiliser le réseau de votre centre de données.

- ❑ Configurez le profil d'Antivirus respectant les meilleures pratiques en clonant le profil prédéfini et en modifiant les valeurs des décodeurs imap, pop3, en **reset-both (réinitialiser les deux)** dans les colonnes Action et WildFire.
- ❑ Configurez le profil d'Anti-Logiciels Espions respectant les meilleures pratiques en clonant le profil strict prédéfini. Sous l'onglet **Rules (Règles)**, activez l'option single packet capture (capture de paquet unique) sur les menaces de gravité moyenne, élevée et critique pour le trafic que vous journalisez. (Pour le trafic que vous ne journalisez pas, appliquez un profil séparé sans activer la capture de paquet.)

  Dans l'onglet Signatures DNS, modifiez l'**Action** de la requête DNS en **sinkhole** si le pare-feu ne peut pas voir l'initiateur de la requête DNS (ce qui est habituel quand le pare-feu se situe au nord du serveur DNS local), pour vous permettre d'identifier les hôtes infectés. Le sinkhole DNS identifie et localise des hôtes compromis qui tentent d'accéder à des domaines suspects et les empêche d'accéder à ces domaines. Activez l'option extended packet capture (capture étendue de paquet) sur le trafic en entonnoir.

  Autorisez le trafic uniquement vers les serveurs DNS approuvés. Utilisez le service de sécurité DNS *pour empêcher les connexions à des serveurs DNS malveillants.*
- ❑ Configurez le Profil de protection contre les vulnérabilités respectant les meilleures pratiques en clonant le profil strict prédéfini et en modifiant le paramètre de Capture de Paquet pour chaque règle excepté **simple-client-informational** et **simple-server-informational** en **single-packet (paquet unique)**. Si le pare-feu identifie un grand volume de menaces de vulnérabilité et que cela affecte les performances, désactivez la capture de paquet pour les événements de faible gravité.
- ❑ Le Profil de Blocage de Fichiers strict prédéfini est le profil respectant les meilleures pratiques. Si le fait de soutenir des applications critiques vous empêche de bloquer tous les types de fichiers que le profil strict bloque (vous pouvez identifier le type de fichiers utilisés dans le centre de données en filtrant les journaux dans **Monitor** > **Logs** > **Data Filtering**), clonez le profil strict et modifiez-le selon vos besoins. Si les fichiers ne doivent pas circuler dans les deux sens, utilisez le paramètre **Direction** pour restreindre le type de fichier à la seule direction requise.
- ❑ Le Profil d'Analyse WildFire prédéfini est le profil respectant les meilleures pratiques. WildFire fournit la meilleure défense contre les menaces inconnues et les menaces persistantes avancées (ATP).

STEP 3 | Configurez de stricts profils de Décryptage respectant les meilleures pratiques pour le centre de données, pour empêcher un trafic inconnu de pénétrer votre centre de données.

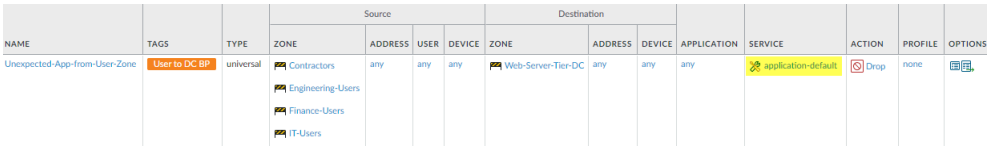
- Pour garantir que les certificats présentés lors du décryptage SSL sont valides, effectuez des vérifications CRL/OCSP.
- Paramètres du protocole SSL : Fixez la **Min Version** sur **TLSv1.2**, la **Max Version** sur **Max**, et décochez l'Algorithme d'Authentification **SHA1**. (Les faibles algorithmes de cryptage 3DES et RC4 sont automatiquement décochés lorsque vous sélectionnez TLSv1.2.) Utilisez TLSV1.3 pour le trafic qui prend en charge TLSV1.3 (de nombreuses applications utilisent des certificats épinglés, qui empêchent le décryptage lorsque TLSV1.3 est utilisé, c'est pourquoi il faut utiliser TLSV1.2 pour ces applications).
- Proxy de transfert SSL Pour **Server Certificate Verification (Vérification du certificat du serveur)**, bloquez les sessions avec des certificats expirés, des émetteurs non approuvés et un état du certificat inconnu, et restreignez les extensions de certificat. Pour les **Contrôles de mode non pris en charge**, bloquez les sessions avec des versions non prises en charge, des suites de cryptage non prises en charges, et une authentification client. Pour les **Contrôles de Défaillance**, bloquer les sessions si les ressources ne sont pas disponibles implique de faire un compromis entre l'expérience utilisateur (le blocage peut affecter l'expérience utilisateur de manière négative) et autoriser des connexions potentiellement dangereuses. Si vous devez envisager ce compromis, envisagez également d'augmenter les ressources disponibles dans le déploiement.
- Inspection SSL entrante : Pour les **Contrôles de mode non pris en charge**, bloquez les sessions avec des versions non prises en charge et des cryptages non pris en charges. Pour les **Contrôles d'échec**, les compromis sont similaires au proxy de transfert SSL.
- Proxy SSH : Pour les **Contrôles de mode non pris en charge**, bloquez les sessions avec des versions et des algorithmes non pris en charge. Pour les **Contrôles d'échec**, les compromis sont similaires au proxy de transfert SSL.
- Appliquez le profil de Non décryptage au trafic que vous avez choisi de ne pas décrypter pour cause de réglementations, règles de conformité, ou pour des raisons professionnelles, sauf au trafic TLSv1.3 (TLSv1.3 crypte les informations de certification afin que le pare-feu ne puisse pas bloquer le trafic basé sur les informations de certificat). Bloquez les sessions aux certificats expirés et provenant de distributeurs non approuvés.

STEP 4 | Configurez les règles de blocage de trafic pour refuser le trafic que vous avez identifié comme malveillant ou sans raison professionnelle.

Journaliser et surveiller les règles de blocage peut révéler des utilisateurs et des applications dont vous ignoriez l'existence sur votre réseau et qui peuvent être légitimes ou signifier une attaque potentielle. Le tri des règles de base de la politique de Sécurité est essentiel pour éviter de *faire de l'ombre* (du trafic correspondant à une règle qui autorise ou qui bloque, avant que ce trafic ne puisse correspondre à une règle que vous voulez qui corresponde avec le trafic). Certaines règles sont pratiquement les mêmes mais activent des rapports séparés pour des ports standard ou non standard, ou pour des applications utilisateurs et des applications provenant d'autres sources. Pour chaque règle, configurez **Journaliser en Fin de Session** dans l'onglet **Actions** et paramétrez le Transfert de Journaux pour suivre et analyser les violations à la règle.

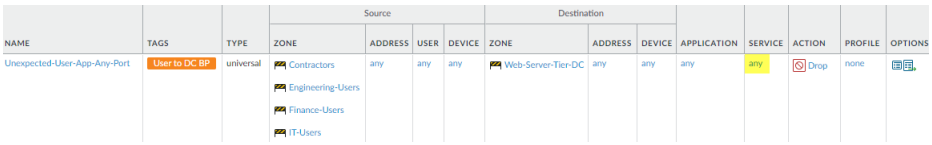
- Bloquez toutes les applications des zones utilisateurs sur le port **application-default (par défaut de l'application)**. Placez cette règle *après* les règles qui autorisent le trafic de l'application légitime en

provenance des zones utilisateur pour identifier les applications utilisateur inconnues ou inattendues sur les ports standard.



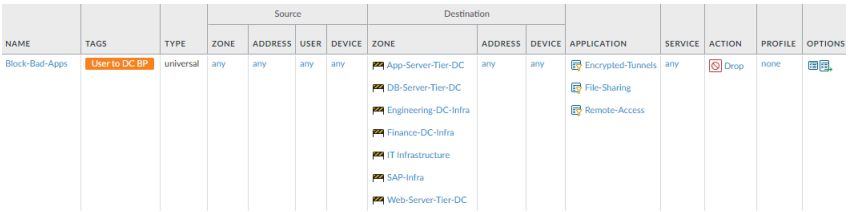
NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-App-from-User-Zone	User to DC BP	universal	Contractors Engineering-Users Finance-Users IT-Users	any	any	any	Web-Server-Tier-DC	any	any	any	application-default	Drop	none	

- Bloquez toutes les applications en provenance des zones utilisateurs sur **tout** port pour saisir le trafic utilisateur tentant d'utiliser des ports non standard. Placez cette règle après la règle de blocage précédente **application-default** pour identifier les applications utilisateurs inattendues ou inconnues sur les ports non standard, qui peuvent se révéler être des applications personnalisées ou des applications utilisant des techniques d'évasion.



NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-User-App-Any-Port	User to DC BP	universal	Contractors Engineering-Users Finance-Users IT-Users	any	any	any	Web-Server-Tier-DC	any	any	any	any	Drop	none	

- Bloquez les applications que vous ne voulez *jamais* dans votre centre de données, comme des applications utilisant des techniques d'évasion communément exploitées, ainsi que des applications sans raison professionnelle. Placez cette règle après les règles d'autorisation pour les applications dans le but, par exemple, d'autoriser des applications de partage de fichiers approuvées avant que le filtre d'application **Filesharing** ne bloque toutes les autres applications de partage de fichiers.

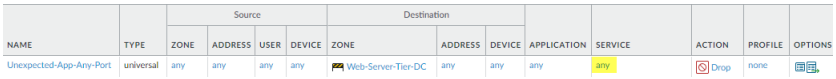


NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Block-Bad-Apps	User to DC BP	universal	any	any	any	any	App-Server-Tier-DC DB-Server-Tier-DC Engineering-DC-Infra Finance-DC-Infra IT Infrastructure SAP-Infra Web-Server-Tier-DC	any	any	Encrypted-Tunnels File-Sharing Remote-Access	any	Drop	none	

- Bloquez toutes les applications de **toute** zone sur le port **application-default (par défaut de l'application)** afin d'identifier les applications inattendues sur ports standard. Des correspondances de règles peuvent signifier des menaces potentielles ou des modifications dans les applications nécessitant de modifier une règle d'autorisation pour les applications. Placez cette règle après les règles d'autorisation pour les applications et la précédente règle de blocage.

NAME	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-App-from-Any-Zone	universal	any	any	any	any	Web-Server-Tier-DC	any	any	any	application-default	Drop	none	

- Bloquez toutes les applications de toute zone sur **tout** port afin d'identifier les applications inattendues sur ports non standard. N'autorisez pas le trafic unknown-tcp, unknown-udp, ou non-syn-tcp. Placez cette règle après les règles d'autorisation pour les applications et la précédente règle de blocage.

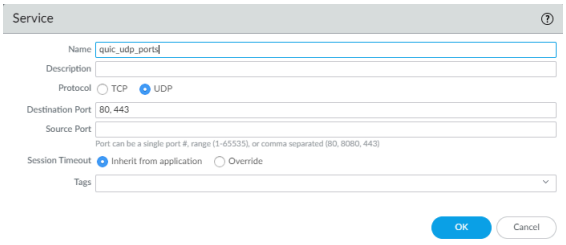


NAME	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-App-Any-Port	universal	any	any	any	any	Web-Server-Tier-DC	any	any	any	any	Drop	none	

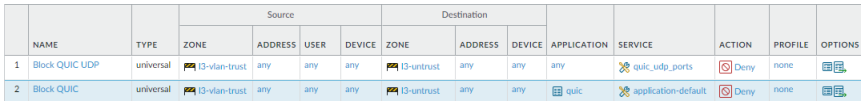
- Bloquez les utilisateurs *inconnus* qui tentent d'exécuter des applications sur tout port afin de révéler des utilisateurs inconnus (lacunes dans la couverture de User-ID, ou pirates informatiques) et identifiez les périphériques compromis (y compris les périphériques embarqués comme les

imprimantes, les lecteurs de cartes ou les appareils photo). Placez cette règle après les règles d'autorisation pour les applications et la précédente règle de blocage.

- En plus de bloquer le trafic potentiellement malveillant, bloquez le protocole Quick UDP Internet Connections (QUIC) à moins que, pour des raisons professionnelles, vous souhaitiez autoriser le trafic crypté du navigateur. Chrome et certains autres navigateurs établissent des sessions au moyen du protocole QUIC au lieu du protocole TLS, mais QUIC utilise un cryptage propriétaire que le pare-feu ne peut déchiffrer ; le trafic potentiellement dangereux peut alors entrer sur le réseau en tant que trafic chiffré. Bloquez les applications QUIC et les ports UDP 80 et 443 pour forcer le navigateur à utiliser TLS. Créez d'abord un service (**Objects** > **Services**) qui comprend 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 afin que les deux premières règles de votre base de règles bloquent QUIC :



STEP 5 | Installez Cortex XDR Agent sur tous les terminaux du centre de données pour vous protéger contre les programmes malveillants et les exploitations au niveau des terminaux.

Cortex XDR Agent protège tous les terminaux de la même manière, afin que le processus de déploiement et la politique de protection contre les programmes malveillants respectant les meilleures pratiques sont les mêmes, aussi bien pour le centre de données que pour tout autre zone du réseau.

Politiques relatives au trafic entre l'utilisateur et le centre de données

Configurez la politique de sécurité, la politique d'authentification et la politique de décryptage pour les utilisateurs qui ont besoin d'accéder au centre de données.

- Règles de politique de sécurité pour les utilisateurs
- Règles de politique d'authentification pour les utilisateurs
- Création d'une règle de politique de décryptage pour les utilisateurs

STEP 1 | Créez des règles de politique de sécurité relatives à la liste d'autorisation pour les applications pour le trafic utilisateur afin d'autoriser l'accès adéquat.

Positionnez les règles d'autorisation pour les accès utilisateurs tout en haut des règles de base, pour éviter de bloquer accidentellement du trafic légitime. Pour chaque règle, configurez **Journaliser en**

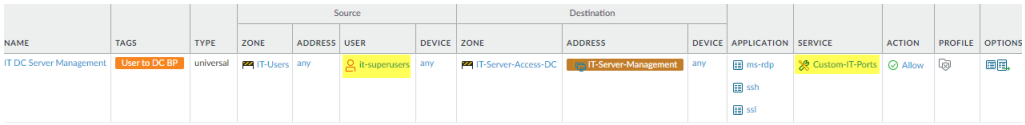
Fin de Session dans l'onglet **Actions** et paramétrez le Transfert de Journaux pour suivre et analyser les violations à la règle.

- Autorisez l'accès des utilisateurs employés aux serveurs DNS d'entreprises internes. Cette règle autorise tout utilisateur, car les utilisateurs accèdent aux services DNS avant de s'identifier. La règle contrôle fermement la zone source, les serveurs de destination et les applications et applique les profils de sécurité au trafic.

  Bloquez l'accès aux serveurs DNS externes au niveau de la passerelle Internet pour empêcher le trafic DNS de sortir vers Internet sur des serveurs publics. Autorisez l'accès uniquement aux serveurs DNS approuvés et utilisez le service DNS Security *pour empêcher les connexions aux serveurs DNS malveillants.*

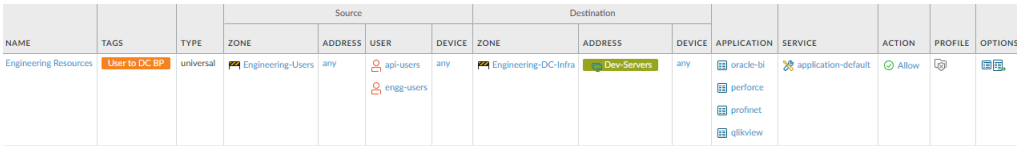
- Autorisez un accès privilégié sécurisé aux interfaces de gestion du centre de données pour le personnel informatique nécessaire. Limitez la règle aux interfaces de gestion (cet exemple utilise un groupe d'adresse pour identifier les périphériques et un service personnalisé pour identifier les ports de gestion) et aux applications nécessaires, dans cet exemple, RDP, SSH et SSL. Utilisez un VLAN dédié pour séparer le trafic de gestion du reste du trafic et placer les interfaces de gestion sur le même sous-réseau.

  Si le même groupe d'utilisateurs du département informatique gère également des commutateurs, des routeurs et d'autres périphériques du centre de données, ajoutez-les à la destination et ajoutez leur port au service personnalisé pour que la règle sécurise le trafic pour les connexions à leurs interfaces de gestion. Si différents groupes du département informatique gèrent différentes ressources du centre de données, créez des règles de politique de sécurité séparées pour chaque groupe ainsi que des règles de politique de décryptage et d'authentification correspondants.

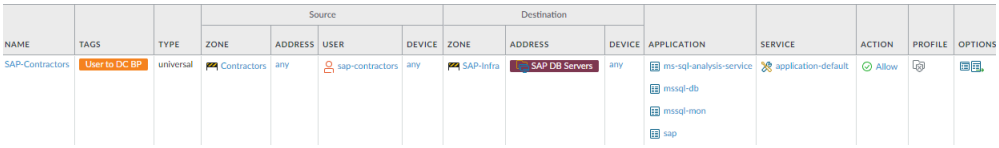


- Autorisez un accès requis pour les groupes d'utilisateurs employés. Ces règles limitent l'accès de chaque groupe d'utilisateurs ou de chaque utilisateur aux applications et serveurs nécessaires.

Cet exemple limite l'accès d'un groupe d'utilisateurs ingénieurs uniquement à ses serveurs de développement et ses applications.



- Autorisez un accès ciblé et limité aux sous-traitants, partenaires, clients et autres tiers. Cet exemple limite l'accès d'un groupe de sous-traitants SAP afin que le groupe ne puisse se connecter qu'aux serveurs de bases de données SAP appropriés, en utilisant uniquement les applications appropriées.

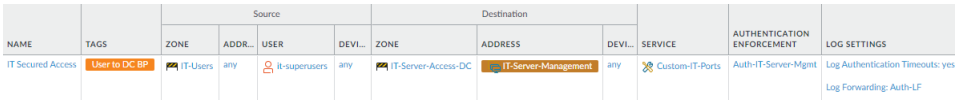


STEP 2 | Créez des règles de politique d'authentification pour le trafic utilisateur pour authentifier l'accès au centre de données.

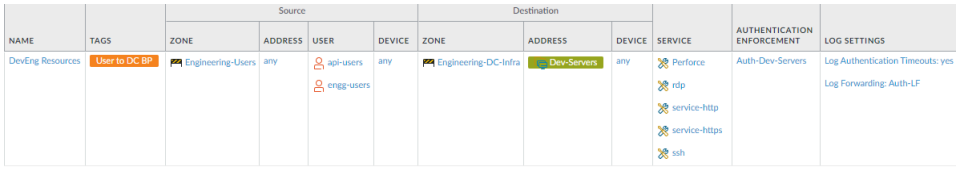
Pour chaque groupe d'utilisateurs ou utilisateur pour lequel vous créez des règles d'autorisation pour les applications, créez une règle d'authentification analogue (hormis la règle d'autorisation pour le DNS, car le DNS survient avant que les utilisateurs ne s'authentifient pour se connecter). Pour chaque règle, configurez **Journaliser en Fin de Session** dans l'onglet **Actions** et paramétrez le Transfert de Journaux pour suivre et analyser les violations à la règle.

- Authentifiez les utilisateurs ayant besoin d'un accès spécialisé. Cet exemple authentifie le personnel du département informatique ayant besoin d'un accès privilégié sécurisé pour gérer les serveurs du centre de données vu dans l'étape précédente de la règle d'autorisation. Puisque compromettre les identifiants d'un utilisateur privilégié revient à remettre les clés du royaume de vos données aux pirates informatiques, exigez une authentification multifactorielle (MFA) pour vous protéger contre les vols d'identifiants.

  Si le même groupe d'utilisateurs du département informatique gère également des commutateurs, des routeurs et d'autres périphériques du centre de données, ajoutez-les à la destination et ajoutez leur port au service personnalisé pour que la règle authentifie le trafic pour les connexions à leurs interfaces de gestion. Si différents groupes du département informatique gèrent différentes ressources du centre de données, créez des règles de politique de sécurité séparées pour chaque groupe ainsi que des règles de politique de décryptage et d'authentification correspondants.

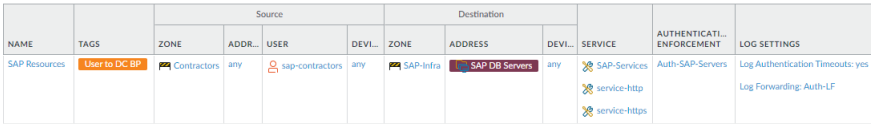


- Authentifiez les employés ayant des raisons commerciales légitimes d'accéder au centre de données. Cet exemple authentifie le groupe d'utilisateurs du département de l'ingénierie informatique vu dans l'étape précédente de la règle d'autorisation.



NAME	TAGS	Source				Destination			SERVICE	AUTHENTICATION ENFORCEMENT	LOG SETTINGS
		ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE			
DevEng Resources	User to DC BP	Engineering-Users	any	api-users engg-users	any	Engineering-DC-Infra	Dev-Servers	any	Perforce rdp service-http service-https ssh	Auth-Dev-Servers	Log Authentication Timeouts: yes Log Forwarding: Auth-LF

- Authentifiez les sous-traitants, les partenaires, les clients et autres groupes de non-employés. Exigez une MFA pour les groupes de non-employés pour vous protéger contre les vols d'identifiants dans une société tierce. Cet exemple authentifie les développeurs SAP vu dans l'étape précédente de la règle d'autorisation.



NAME	TAGS	Source				Destination			SERVICE	AUTHENTICATI... ENFORCEMENT	LOG SETTINGS
		ZONE	ADDR...	USER	DEVI...	ZONE	ADDRESS	DEVI...			
SAP Resources	User to DC BP	Contractors	any	sap-contractors	any	SAP-Infra	SAP DB Servers	any	SAP-Services service-http service-https	Auth-SAP-Servers	Log Authentication Timeouts: yes Log Forwarding: Auth-LF

STEP 3 | Créez des règles de politique de sécurité de décryptage pour le trafic utilisateur pour décrypter le trafic que vous autorisez afin que le pare-feu puisse voir, inspecter et appliquer une politique de sécurité au trafic.

Pour chaque règle de politique de Décryptage, appliquez le profil de Décryptage approprié respectant les meilleures pratiques (Inspection SSL Entrante, Proxy de Transfert SSL, Proxy SSH, ou Sans Décryptage, y compris les paramètres de protocole SSL respectant les meilleures pratiques pour les règles d'inspection SSL entrante et de proxy de transfert SSL) dans le but de bloquer des protocoles et des algorithmes faibles et de vérifier les certificats serveur. Pour chaque règle d'inspection SSL entrante, importez le certificat du serveur du centre de données que vous protégez avec un décryptage.

Excluez le trafic du décryptage *uniquement pour ces deux raisons :*

- *Le trafic interrompt le décryptage pour* des raisons techniques*, comme un certificat épinglé ou une authentification mutuelle. Ajoutez des exclusions techniques à la liste* ***Device*** *>* ***Certificate Management*** *>* ***SSL Decryption Exclusion****.*
- *Le trafic que vous choisissez de ne pas déchiffrer en raison d'activité commerciale, de réglementations ou de règles de conformité ou toute autre comme du trafic lié à la finance, la santé, l'armée ou le gouvernement. Créez* des exclusions de déchiffrement basées sur les politiques *pour le trafic que vous choisissez de ne pas déchiffrer.*

- Décryptez le trafic de la règle de politique de sécurité créée précédemment, autorisant le département informatique à accéder de manière privilégiée aux serveurs de gestion. La règle de politique de décryptage et son profil de décryptage associé diffèrent selon que le groupe

informatique utilise SSL (profil de décryptage du proxy de transfert SSL) ou SSH (profil de décryptage du proxy SSH) pour accéder aux ports de gestion.

Si le même groupe d'utilisateurs du département informatique gère également des commutateurs, des routeurs et d'autres périphériques du centre de données, ajoutez-les à la destination et ajoutez les certificats serveur pour que la règle décrypte le trafic pour les connexions à leurs interfaces de gestion. Si différents groupes du département informatique gèrent différents ensembles de ressources du centre de données, créez des règles de sécurité rigoureuses séparées pour chaque groupe ainsi que des règles de politique de décryptage et d'authentification correspondants.

Pour un accès privilégié SSL :

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
IT DC Management	User to DC BP	IT-Users	it-superusers	IT-Server-Access-DC	IT-Server-Management	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

Pour un accès privilégié SSH :

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
IT DC Mgmt-SSH	User to DC BP	IT-Users	it-superusers	IT-Server-Access-DC	IT-Server-Management	decrypt	ssh-proxy	DC BP Decryption	none	false	true

- Configurez l'inspection SSL entrante pour décrypter le trafic autorisé des groupes d'utilisateurs employés. Cet exemple décrypte le trafic de la règle d'autorisation du groupe utilisateur d'ingénierie informatique.

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Engg to Dev Servers	User to DC BP	Engineering-Users	api-users engg-users	Engineering-DC-Infra	Dev-Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

- Configurez l'inspection SSL Entrante pour qu'elle décrypte le trafic autorisé des sous-traitants, collaborateurs, clients et autres tierces parties. Cet exemple décrypte le trafic de la règle d'autorisation du groupe utilisateur de sous-traitants SAP analogue.

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
SAP Contractors to SAP Servers	User to DC BP	Contractors	sap-contractors	SAP-Infra	SAP DB Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

- Appliquez un profil de non-déchiffrement pour configurer la vérification serveur pour le trafic que vous *choisissez* de ne pas déchiffrer en raison d'activité commerciale, de réglementations ou de règles de conformité ou toute autre comme du trafic lié à la finance, la santé, l'armée ou le gouvernement. Cet exemple montre comment exclure deux groupes d'utilisateurs du département finance du décryptage quand ils accèdent aux serveurs du groupe d'adresses **Fin Servers**.

N'appliquez pas un profil de non-décryptage au trafic TLSV1.3, car les informations du certificat sont cryptées, afin que le pare-feu ne puisse pas bloquer les sessions basées sur les informations de certificat.

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Finance PCI No Decrypt	User to DC BP	Finance-Users	accounting-users finance-users	Finance-DC-Infra	Fin-Servers	no-decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

Politiques relatives au trafic d'Internet vers le centre de données

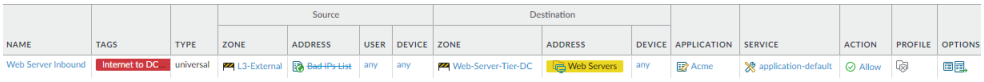
Configurez la politique de sécurité, la politique de décryptage et la politique de protection Denial-of-Service (déni de service - DoS) pour le trafic d'Internet vers le centre de données.

- Politique de sécurité d'Internet au centre de données
- Politique de décryptage d'Internet au centre de données
- Politiques de protection DoS d'Internet au centre de données

STEP 1 | Créez une liste règles de politique de sécurité d'autorisation pour les applications pour le trafic d'Internet vers le centre de données afin de contrôler et sécuriser l'accès de collaborateurs, sous-traitants et clients.

Protégez-vous contre le téléchargement de programmes malveillants depuis un client externe infecté ou contre le placement d'un programme malveillant sur un serveur externe provenant d'un serveur de centre de données infecté. Créez une liste d'autorisation pour les applications requises pour des raisons professionnelles et créez une Liste Dynamique Externe (EDL) pour bloquer les adresses IP malveillantes. Pour chaque règle, configurez **Journaliser en Fin de Session** dans l'onglet **Actions** et paramétrez le Transfert de Journaux pour suivre et analyser les violations à la règle.

Cet exemple restreint les applications et les destinations pour le trafic d'Internet vers le centre de données, et utilise l'option **Negate (Invalider)** pour empêcher la communication avec l'EDL **Bad IPs List**.



Créez des règles similaires pour le trafic d'Internet vers d'autres groupes de serveurs (lorsqu'il est autorisé) et d'autres applications. Rendez chaque règle spécifique pour qu'elle limite l'accès aux seules applications et serveurs nécessaires.

STEP 2 | Création des règles de politique de décryptage du trafic d'Internet vers le centre de données pour décrypter le trafic autorisé.

Configurez l'Inspection SSL Entrante (et importez les certificats du serveur destination dans le pare-feu) afin qu'elle décrypte le trafic des collaborateurs, sous-traitants et clients que les règles de politique de Sécurité autorisent pour le trafic d'Internet vers le centre de données. Cet exemple montre la politique de décryptage pour la précédente règle de politique de Sécurité.

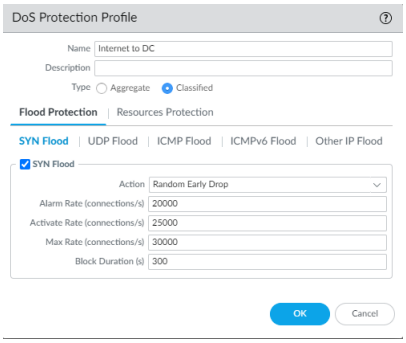
Créez des règles de décryptage correspondant au trafic autorisé par les règles de politique de Sécurité concernant le trafic d'Internet vers le centre de données.

STEP 3 | Créez des règles de politique de Protection DoS pour le trafic d'Internet vers le centre de données pour protéger des serveurs critiques d'attaques par Déni de Service (DoS), en limitant la quantité de connexions par seconde (CPS) autorisées par le pare-feu, afin d'empêcher une attaque SYN flood.

Les pirates informatiques ciblent la couche du serveur web, car s'ils arrivent à la neutraliser, ils peuvent empêcher la plupart des accès légitimes au centre de données. Appliquez une règle de politique de

Protection DoS classée, avec un Profil de Protection DoS limitant les CPS entrants, afin d'empêcher des pics de trafic qui peuvent affecter les performances et la disponibilité du serveur.

- Créez un profil de protection DoS classifié pour protéger la couche du serveur web et empêcher les attaques SYN flood. Les seuils CPS que vous définissez dépendent du taux CPS maximal de base.



- Créez une règle de politique de protection DoS pour spécifier les serveurs web que vous protégez et appliquez-leur le profil de protection DoS classifié.

NAME	TAGS	Source			Destination		SERVICE	ACTION	Protection		LOG FORWARDING
		ZONE/INTERFACE	ADDRESS	USER	ZONE/INTERFACE	ADDRESS			AGGREGATE	CLASSIFIED	
DC Web Server Protection	Internet to DC BP	L3-External	~~Bad IPs List~~	any	Web-Server-Tier-DC	Web Servers	service-http service-https	protect	none	profile: Internet to DC destination-ip-only	DoS-LF

Pour vous protéger d'attaques SYN flood provenant de sources internes, créez une règle de politique de Protection DoS séparée, qui spécifie vos zones internes comme des zones sources au lieu de **L3-External**. Des règles séparées pour des sources d'attaques externes et internes permettent d'obtenir des rapports distincts qui rendent vos enquêtes sur des tentatives d'attaques plus aisées.

- En complément, configurez la Protection du Tampon du Paquet pour chaque zone du centre de données afin de protéger le pare-feu d'attaques DoS sur une session unique pouvant occasionner une chute du trafic légitime.

Politiques relatives au trafic du centre de données vers Internet

Configurez la politique de sécurité et la politique de décryptage pour le trafic du centre de données vers Internet.

- Politique de sécurité du centre de données vers Internet
- Politique de décryptage du centre de données vers Internet

STEP 1 | Créez des règles d'autorisation pour les applications data-center-to-Internet pour protéger les connexions vers des serveurs externes.

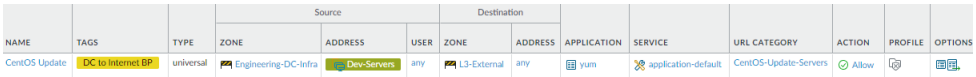
Les serveurs du centre de données peuvent obtenir des mises à jour logicielles ou l'état des certificats à partir de serveurs sur Internet. Le plus grand risque est de se connecter au mauvais serveur. Créez des règles strictes d'autorisation pour les applications pour les mises à jour, afin de limiter les serveurs externes joignables et les applications autorisées (sur leur port par défaut uniquement). Cela empêche les serveurs infectés du centre de données de communiquer à l'extérieur et empêche l'exfiltration de données à l'aide d'applications légitimes comme FTP, HTTP ou DNS sur des ports non standard. En

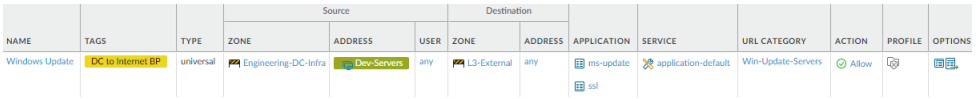
complément, utilisez le contrôle de **Direction** du profil de Blocage de Fichier pour bloquer les fichiers de mise à jour sortants, afin de n'autoriser que le téléchargement des mises à jour logicielles.

Pour chaque règle, appliquez les profils de Sécurité respectant les meilleures pratiques et configurez **Journaliser en Fin de Session** dans l'onglet **Actions**.

Collaborez avec les départements Ingénierie et d'autres groupes ayant recours à des mises à jour logicielles pour journaliser et analyser leurs sessions de navigation Internet, afin de définir les URL où les développeurs se procurent leurs mises à jour.

- Ces exemples permettent aux serveurs du département Ingénierie de communiquer avec les serveurs de mises à jour CentOS (Catégorie d'URL personnalisée **CentOS-Update-Servers**) en utilisant l'application **yum** et avec les serveurs de mises à jour Microsoft (Catégorie d'URL personnalisée **Win-Update-Servers**) en utilisant l'application **ms-update** (vous devez également autoriser **ssl**, car **ms-update** est dépendant de SSL).

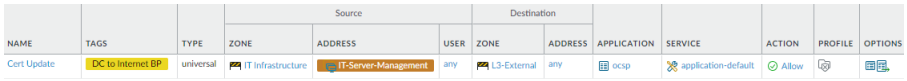




- Autorisez l'accès aux mises à jour DNS et NTP (Catégorie d'URL personnalisée **NTP DNS Update Servers**).

Bloquez l'accès aux serveurs DNS externes au niveau de la passerelle Internet pour empêcher le trafic DNS de sortir vers Internet sur des serveurs publics. Autorisez l'accès uniquement aux serveurs DNS approuvés et utilisez le service DNS Security pour empêcher les connexions aux serveurs DNS malveillants.

- Autorisez les connexions à un Répondeur Online Certificate Status Protocol (OCSP) sur le net pour vérifier l'état de révocation de certificats d'authentification et vous assurer de leur validité. Quand vous configurez un profil de certificat dans le pare-feu, vous pouvez configurer la vérification de l'état CRL comme méthode de secours pour l'OCSP si le répondeur OCSP n'est pas joignable.



STEP 2 | Créez des règles de politique de décryptage du trafic du centre de données vers Internet pour décrypter le trafic autorisé dans la règle de politique de sécurité précédente.

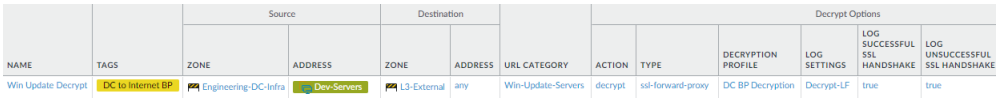
Un serveur de mise à jour compromis pourrait télécharger des logiciels malveillants et les propager à travers le processus de mise à jour logicielle. Il est donc essentiel de décrypter le trafic pour gagner en visibilité. Comme seuls les comptes services sont à l'origine de trafics de mises à jour et que le trafic de

mises à jour ne contient aucune information personnelle ou sensible, cela ne pose pas de problème de respect de la vie privée.

Ne décryptez pas le trafic vers les serveurs OCSP de révocation de certificat, car le trafic utilise habituellement HTTP et il n'est pas crypté. De plus, le décryptage du Proxy de transfert SSL risque d'interrompre le processus de mise à jour, car le pare-feu agit en tant que proxy et remplace le certificat client avec un certificat proxy, que le répondeur OCSP risque de ne pas valider.

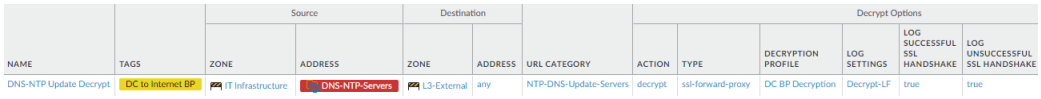
- Décryptez le trafic entre le centre de données et les serveurs de mise à jour. Ces deux exemples décryptent le trafic de mises à jour CentOS et Windows autorisé par les règles de politique de Sécurité vues à l'étape précédente.

NAME	TAGS	Source ZONE	Source ADDRESS	Destination ZONE	Destination ADDRESS	URL CATEGORY	Decrypt Options ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
CentOS Update Decrypt	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	L3-External	any	CentOS-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true



NAME	TAGS	Source ZONE	Source ADDRESS	Destination ZONE	Destination ADDRESS	URL CATEGORY	Decrypt Options ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Win Update Decrypt	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	L3-External	any	Win-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

- Décryptez le trafic entre les serveurs du centre de données et les serveurs de mise à jour NTP et DNS. Cet exemple décrypte le trafic de mises à jour autorisé par la règle de politique de Sécurité vue à l'étape précédente.



NAME	TAGS	Source ZONE	Source ADDRESS	Destination ZONE	Destination ADDRESS	URL CATEGORY	Decrypt Options ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
DNS-NTP Update Decrypt	DC to Internet BP	IT Infrastructure	DNS-NTP-Servers	L3-External	any	NTP-DNS-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

Politiques relatives au trafic au sein du centre de données

Configurez la politique de sécurité et la politique de décryptage pour le trafic entre les serveurs du centre de données et les couches d'applications.

- Politique de sécurité au sein du centre de données
- Politique de décryptage au sein du centre de données

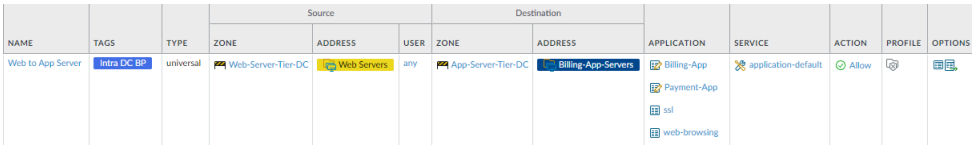
STEP 1 | Créez des règles d'autorisation pour les applications au sein du centre de données pour protéger des serveurs du centre de données d'autres serveurs du centre de données qui seraient compromis.

Une architecture d'applications classique se compose de trois couches de serveurs : les serveurs web, les serveurs d'applications et les serveurs de bases de données. Appliquez des profils de sécurité respectant les meilleures pratiques à la plupart du trafic entre couches de serveurs pour prévenir les menaces. N'appliquez pas de profils de sécurité à des trafics à volume élevé et faible valeur, de type duplication de messagerie et flux de sauvegarde, le pare-feu a déjà inspecté les flux originaux et dépenser des cycles du processeur sur eux n'apporte aucune valeur ajoutée. En revanche, créez des règles d'autorisation pour ces applications afin d'éviter les mauvais usages. Pour chaque règle, configurez **Journaliser en Fin de Session** dans l'onglet **Actions** et paramétrez le Transfert de Journaux pour suivre et analyser les violations à la règle.

Cet exemple configure des règles autorisant le trafic entre couches de serveurs d'applications pour deux applications propriétaires internes au département finance, pour lesquelles nous avons procédé à la

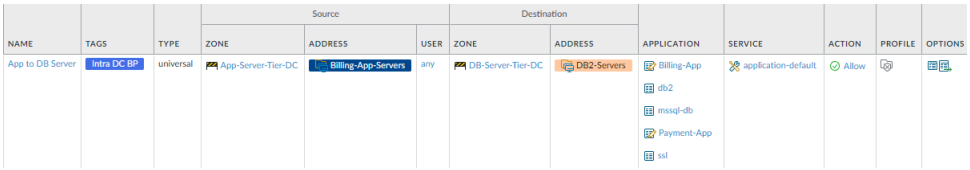
création d’applications personnalisées : **Billing-App (Application de facturation)** et **Payment-App (Application de paiement)**.

- Autorisez le trafic des applications financières entre la couche serveur web et la couche d’applications.



			Source			Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Web to App Server	Intra DC BP	universal	Web-Server-Tier-DC	Web Servers	any	App-Server-Tier-DC	Billing-App-Servers	Billing-App Payment-App ssl web-browsing	application-default	Allow		

- Autorisez le trafic des applications financières entre la couche d’applications et la couche base de données.



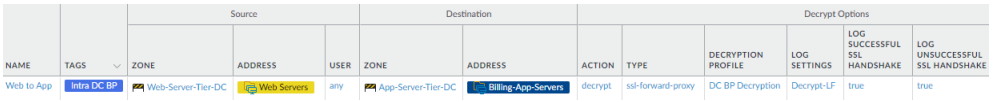
			Source			Destination						
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
App to DB Server	Intra DC BP	universal	App-Server-Tier-DC	Billing-App-Servers	any	DB-Server-Tier-DC	DB2-Servers	Billing-App db2 mssql-db Payment-App ssl	application-default	Allow		

STEP 2 | Créez des règles de politique de décryptage au sein du centre de données pour décrypter le trafic autorisé dans les règles de politique de sécurité précédentes.

Pour les pirates informatiques, le centre de données est l’endroit idéal où se cacher précisément parce que de nombreuses personnes pensent qu’il est sûr et ne cherchent pas les intrus. Néanmoins, le même principe de base qui s’avère exact pour le reste du réseau l’est également pour le centre de données : vous ne pouvez pas vous protéger contre une menace que vous ne voyez pas. Décryptez le trafic au sein du centre de données pour que le pare-feu puisse inspecter le trafic, contrôler l’accès, rendre des menaces visibles, et protéger vos ressources les plus précieuses.

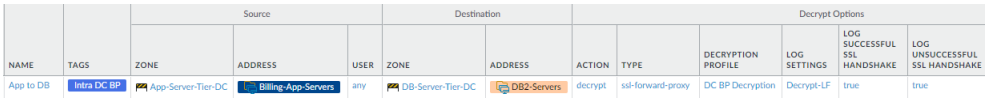
Le trafic du centre de données n’est pas entièrement crypté. Ne dépensez pas vos ressources pour décrypter le trafic non crypté (texte en clair).

- Cette règle décrypte le trafic circulant entre les couches du serveur web et celles du serveur de l’application pour les serveurs de facturation du département des Finances.



		Source			Destination		Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Web to App	Intra DC BP	Web-Server-Tier-DC	Web Servers	any	App-Server-Tier-DC	Billing-App-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

- Cette règle décrypte le trafic circulant entre les couches du serveur web et celles du serveur de la base de données pour les serveurs de facturation du département des Finances.



		Source			Destination		Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
App to DB	Intra DC BP	App-Server-Tier-DC	Billing-App-Servers	any	DB-Server-Tier-DC	DB2-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

Tri de la base de règles de la politique de sécurité du centre de données

Triez correctement les règles dans la base de règles de la politique de sécurité pour garantir que vous n’autorisez que les applications et le trafic que vous avez prévu d’autoriser et qu’aucune règle ne bloque une autre règle.

La section Tri de la base de règles de la politique de sécurité du centre de données montre toute la base des règles des exemples précédents (règles de blocage et règles d'autorisation pour les applications) dans le bon ordre et explique le positionnement de chaque règle. La base de règles de politique de sécurité est une liste ordonnée de vos règles de politique de sécurité.

L'ordre des règles dans la base de règles détermine la manière dont le pare-feu gère le trafic. Lorsque le trafic correspond à une règle dans la base de règles, le pare-feu exécute l'action de la règle sur ce trafic et ne compare pas le trafic à d'autres règles de politique de sécurité. C'est pourquoi l'ordre des règles dans la base de règles de politique de sécurité est essentiel. Si les règles ne sont pas dans le bon ordre, le trafic peut correspondre à une règle à laquelle vous ne vouliez pas qu'il corresponde (c'est ce que l'on appelle l'effet d'ombre).

Le livre Meilleures pratiques en matière de politique de sécurité comprenant les meilleures pratiques en matière de base de règles de politique de sécurité, décrit les meilleures pratiques à suivre lors de la création de votre base de règles de politique de sécurité. Les meilleures pratiques en matière de base de règles de politique de sécurité incluent :

- Garder la base de règles aussi petite que possible pour une gestion plus facile. Dans certains cas, vous pouvez combiner les règles. Il est conseillé de les combiner si cinq des six objets suivants sont identiques dans ces règles : zone source, zone de destination, adresse IP source, adresse IP de destination, port de service et application.
- Utilisez Policy Optimizer pour simplifier la base de règles.
- Utilisez des objets de groupe tels que des groupes d'applications et des groupes d'adresses pour simplifier la base de règles.
- En général, placez les règles plus spécifiques avant les règles plus générales pour éviter l'effet d'ombre.

Meilleures pratiques concernant le suivi du déploiement du centre de données

Après avoir commencé à déployer votre centre de données en respectant les meilleures pratiques, surveillez le réseau pour vous assurer que la sécurité et les accès fonctionnent comme prévu, et maintenez ensuite la base de règles au fur et à mesure que les circonstances évoluent.

STEP 1 | Vérifiez le rapport d'applications prédéfini (**Monitor [Surveillance]** > **Reports [Rapports]** > **Application Reports [Rapports d'applications]** > **Applications**) afin de vérifier que seules les applications comprises dans les règles de politique de sécurité d'autorisation pour les applications s'exécutent.

Si vous trouvez des applications inattendues, passez en revue les règles de politique de Sécurité et affinez-les afin d'éliminer les applications inattendues ou de les adapter aux applications légitimes.

STEP 2 | Journalisez tout le trafic du centre de données.

Palo Alto Networks propose des outils poussés de surveillance et de journalisation, utilisez-les ainsi que les rapports prédéfinis et les rapports personnalisés, pour capturer et surveiller l'activité d'applications, d'utilisateurs, de trafic et de comportements inattendus.

STEP 3 | Créez des rapports personnalisés pour surveiller les règles de blocage, afin de vous permettre de vous protéger contre les attaques potentielles et d'identifier les vides dans les politiques et les comportements inattendus, pour vous permettre d'affiner la base de règles.

STEP 4 | Créez un rapport personnalisé pour journaliser le trafic au sein du centre de données correspondant à la règle d'autorisation de l'intrazone par défaut prédéfinie au bas de la base de règles, qui autorise par défaut l'ensemble du trafic à l'intérieur d'une même zone.

STEP 5 | Activez la journalisation du trafic du centre de données correspondant à la règle d'interzone par défaut prédéfinie au bas de la base de règles, qui refuse par défaut l'ensemble du trafic entre zones, et créez-lui un rapport personnalisé.

STEP 6 | Écoutez et répondez aux commentaires des utilisateurs.

Les plaintes des utilisateurs concernant la perte d'accès à des applications permettent d'identifier les lacunes dans la base de règles ainsi que les applications à risque utilisées avant que la création de règles d'autorisation pour les applications n'empêche leur utilisation.

STEP 7 | Comparez régulièrement la mesure de référence avec sa mesure prise durant l'étape de planification afin d'évaluer le progrès accompli, d'identifier les modifications apportées, et de trouver des aspects à améliorer.

Conjointement, réexaminez vos objectifs concernant l'état futur idéal de votre réseau pour apprécier le progrès effectué. Si vous gérez des pare-feu avec Panorama, surveillez la santé des pare-feu pour comparer les périphériques par rapport à leur rendement de base et comparer leurs rendements entre eux, afin d'identifier les écarts par rapport à leur comportement normal.

STEP 8 | Faites évoluer les règles d'autorisation pour les applications avec le temps, car les applications elles-mêmes évoluent, les besoins des utilisateurs changent et les mises à jour de contenu modifient les App-IDs existantes et introduisent de nouvelles App-IDs.

Maintenez la base de règles du centre de données respectant les meilleures pratiques et examinez les App-IDs nouvelles et modifiées avant d'installer une version avec du nouveau contenu, pour pouvoir modifier la base de règles si les modifications affectent la politique.

STEP 9 | Utilisez les outils d'évaluation et d'examen de Palo Alto pour évaluer vote posture de prévention actuelle et votre façon d'adopter les meilleures pratiques.

STEP 10 | Référez-vous au guide complet Politique de sécurité du centre de données respectant les meilleures pratiques pour plus de détails sur les étapes de planification, de déploiement et de suivi du déploiement, et des avantages que vous pouvez tirer de ces pratiques.

Politique de sécurité respectant les meilleures pratiques concernant le centre de données

Les actifs les plus précieux de votre entreprise résident dans votre centre de données, notamment le code source propriétaire, la propriété intellectuelle et les données sensibles de l'entreprise et des clients. Vos clients et vos employés comptent sur vous pour préserver la confidentialité et l'intégrité de leurs données et s'attendent à ce que vos centres de données soient toujours disponibles, car ils s'attendent à ce que leurs données soient toujours disponibles. Il est important pour l'intégrité et la réussite de votre entreprise de mettre en œuvre une politique de sécurité respectant les meilleures pratiques concernant le centre de données qui protège vos données et empêche les attaques réussies.

Les méthodes et recommandations suivantes fournissent un plan pour la planification, la conception et la mise en œuvre d'une politique de sécurité respectant les meilleures pratiques concernant le centre de données de manière progressive et hiérarchisée. Créer une politique de sécurité exemplaire pour le centre de données peut sembler insurmontable si vous essayez d'instaurer toutes les protections de toutes les zones de votre réseau à un moment donné. Toutefois, si vous évaluez ce qui est le plus important à protéger et commencez à instaurer votre politique de sécurité exemplaire pour le centre de données en commençant par défendre vos ressources les plus précieuses, vous pouvez effectuer la transition graduellement vers une politique de sécurité qui vous permet d'autoriser des applications, des utilisateurs et du contenu de manière sécurisée, sans prendre de risques excessifs.

La liste de vérification des meilleures pratiques de politique de sécurité concernant le centre de données *fournit une vue d'ensemble sur les meilleures pratiques de prédéploiement, déploiement et post-déploiement, ainsi qu'une façon de mettre en place ces meilleures pratiques plus rapidement si vous n'avez pas besoin d'explications détaillées.*

Qu’est-ce qu’une politique de sécurité respectant les meilleures pratiques concernant le centre de données ?

Une politique de centre de données respectant les meilleures pratiques protège les précieuses données de votre propre entreprise, protège la confidentialité de vos clients, collaborateurs et fournisseurs, protège l’intégrité de votre réseau et de vos activités commerciales dans leur ensemble, et permet d’assurer la disponibilité de votre réseau à tout moment. Elle protège contre les attaques provenant de l’extérieur de votre réseau comme de l’intérieur de votre réseau, dans tous les vecteurs.

Une politique du centre de données respectant les meilleures pratiques protège quatre flux de trafic (les régions d’où proviennent les connexions) :

1. Trafic d’utilisateurs locaux circulant vers le centre de données.
2. Le trafic circulant depuis Internet vers le centre de données.
3. Le trafic circulant du centre de données vers Internet.
4. Trafic intra-centre de données circulant entre les serveurs ou les machines virtuelles, également appelé trafic est-ouest.

Une politique du centre de données respectant les meilleures pratiques empêche les pirates informatiques de prendre pied dans votre centre de données et empêche tout pirate informatique réussissant à atteindre le centre de données d’exfiltrer des données ou de se déplacer latéralement à travers le réseau pour compromettre des serveurs critiques. Il empêche aussi bien les menaces connues que celles inconnues, en instaurant des règles de politique de sécurité qui atteignent des niveaux d’exemplarité à la hauteur de vos exigences commerciales. Elle :

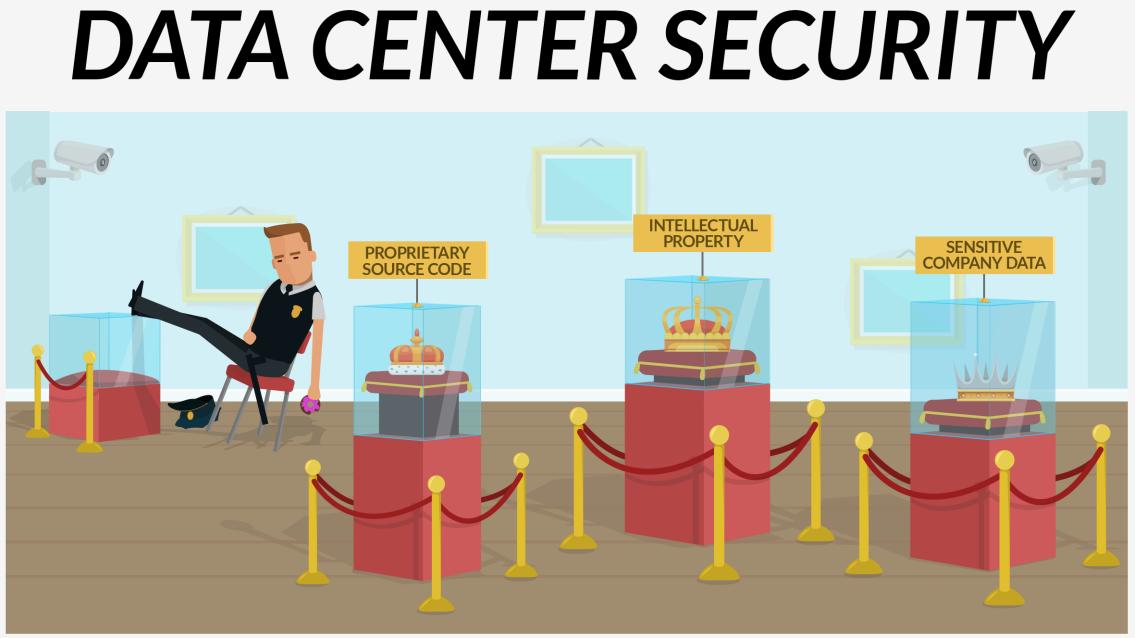
- Identifie les applications quel que soit leur port, le protocole utilisé ou la technique d’évasion utilisée, y compris en décryptant du trafic chiffré.
- Identifie et contrôle les utilisateurs, indépendamment de l’adresse IP, de l’endroit ou de l’appareil
- Protège contre les menaces et vulnérabilités connues et inconnues issues des applications.
- Détecte des comportements anormaux pouvant indiquer qu’une attaque est en cours.

Une politique du centre de données respectant les meilleures pratiques permet également d’attraper les intrus quand ils enfreignent une règle de politique. Lorsqu’une règle est enfreinte, l’attaque est arrêtée, car l’infraction entraîne le pare-feu nouvelle génération à refuser l’accès et la violation est journalisée pour que vous puissiez enquêter sur l’incident et prendre les mesures adéquates.

Pourquoi ai-je besoin d’une politique de sécurité respectant les meilleures pratiques concernant le centre de données ?

Assurer la protection de la disponibilité, de la confidentialité et de l’intégrité de votre réseau pour vous permettre de mener votre activité de manière sécurisée, sans interruption, et en conformité avec les règlementations relatives à la protection des données sensibles, est primordial. L’idée de renforcer l’extérieur du réseau et d’autoriser l’intérieur du réseau à rester plus mou, car l’intérieur serait fiable et dépassé, laisse votre réseau ouvert aux attaques externes, et ne permet pas de prévoir un cas de figure où un pirate informatique décidé, tenace et doté de ressources prendrait pied à l’intérieur du périmètre. Pour cette raison, vous devez protéger le périmètre du centre de données et son intérieur aussi fortement que vous protégez le périmètre du réseau d’entreprise.

Les attaques internes peuvent provenir de sources telles que les employés actuels ou les sous-traitants sur site. Le fil conducteur d’une attaque en interne est la légitimité de la source de l’attaque, qui peut être un utilisateur ou une application légitime. Les attaques externes peuvent provenir de cybercriminels, d’activistes des réseaux et de pirates informatiques financés par des États voyous, ainsi que de voies d’attaques moins évidentes comme un collaborateur ou le système d’un fournisseur compromis, ou encore d’un ancien employé connaissant le réseau. La première étape pour un attaquant extérieur est de prendre pied à l’intérieur du réseau, transformant l’attaque en attaque interne. En substance, toutes les violations sont des attaques internes même si elles proviennent de l’extérieur, car une fois que le pirate informatique réussit à s’introduire dans le réseau, il peut se déplacer librement à travers le réseau.



Si un pirate informatique vole les identifiants d’accès légitimes d’un collaborateur, il peut accéder à votre centre de données en se faisant passer pour un utilisateur légitime. Ensuite, « confortablement installé » à l’intérieur de votre réseau, le pirate informatique peut utiliser vos serveurs internes et vos terminaux pour se déplacer latéralement à travers le réseau et compromettre des systèmes critiques. Une fois qu’un adversaire externe entre par effraction dans votre réseau, vous comptez sur la segmentation du réseau et des utilisateurs ainsi que sur les défenses par couches au sein du réseau pour protéger vos données, comme lorsque l’attaque provient de l’extérieur.

Développer une politique de sécurité respectant les meilleures pratiques permet de protéger votre centre de données contre les attaques, quelle que soit leur origine, par étape, de façon hiérarchisée, en sécurisant vos ressources les plus précieuses en premier et en appliquant de manière graduelle une protection complémentaire. Une transition en douceur d'une politique de sécurité qui mise sur le hasard à une politique de sécurité respectant les meilleures pratiques permet d'assurer la confidentialité de vos données, l'intégrité de votre entreprise et la disponibilité de votre centre de données de manière pratique. Les recommandations suivantes pour la conception et la mise en œuvre d'une politique de sécurité respectant les meilleures pratiques concernant le centre de données vous montrent comment activer en toute sécurité les applications, les utilisateurs et le contenu en classant tout le trafic, tout le temps, avec un minimum d'interruption pour les utilisateurs finaux.

Méthodologie des meilleures pratiques concernant le centre de données

Les meilleures pratiques suivantes garantissent la détection et la prévention à plusieurs étapes du cycle des attaques.

Méthodologie exemplaire	Pourquoi est-ce important ?
Examinez l'ensemble du trafic pour obtenir une visibilité complète	Voir le trafic du réseau vous permet d'identifier la présence de pirates informatiques. Examinez le trafic pour voir les utilisateurs, les applications et le contenu circulant vers l'intérieur, au sein de, et à l'extérieur du centre de données : ❑ Déployez des pare-feu nouvelle génération à des emplacements leur permettant d'inspecter l'ensemble du trafic réseau. N'autorisez pas le trafic à circuler à l'intérieur du centre de données ou entre segments du réseau sans positionner de pare-feu examinant le trafic. ❑ Activez le décryptage SSL sur l'ensemble du trafic entrant ou sortant du centre de données, à moins que la réglementation ou des règles de conformité vous imposent d'exclure certaines catégories comme la santé, les finances, le gouvernement ou l'armée. Vous devez voir les menaces pour pouvoir protéger votre réseau contre elles. Comme plus de 50 % du trafic d'un réseau typique est crypté et que ce pourcentage ne cesse d'augmenter, si vous ne décryptez pas votre trafic, vous ne pouvez pas protéger entièrement votre réseau. ❑ Utilisez App-ID pour identifier les applications et créez des applications propres à l'entreprise pour les applications propriétaires, afin que le pare-feu puisse identifier et catégoriser ces applications de manière appropriée et appliquer la bonne règle de politique de sécurité. Ceci est particulièrement important pour les anciennes applications héritées qui sont autrement catégorisées à tort comme « navigation web » ou « TCP inconnu ». Si vous disposez de stratégies existantes de contrôle prioritaire sur l'application que vous avez créées uniquement pour définir des délais d'expiration de session personnalisés pour un ensemble de ports, convertissez-les en politiques basées sur les applications en configurant des délais d'expiration de session basés sur les services afin de maintenir le délai d'expiration personnalisé pour chaque application, puis migrez la règle vers une règle basée sur les applications. Les politiques de Contrôle Prioritaire pour des Applications sont basées sur le port. Lorsque vous utilisez des politiques de Contrôle Prioritaire pour des Applications pour conserver des délais d'expiration de session personnalisés pour un ensemble de ports, vous perdez de la visibilité sur les applications dans ces flux, et vous ne savez pas quelles applications utilisent les ports et vous ne pouvez pas non plus les contrôler. Les délais d'expiration de session basés sur le service permettent d'avoir des délais d'expiration de session personnalisés tout en maintenant une visibilité sur les applications. ❑ Activez User-ID sur l'ensemble du trafic entrant ou sortant du centre de données pour cartographier le trafic des applications et les menaces qui y seraient associées dans leur contenu, pour les utilisateurs et les services. Comme vous

Méthodologie exemplaire	Pourquoi est-ce important ?
	activez User-ID sur des segments de réseau (zones), vous devez d'abord segmenter le réseau pour activer User-ID. Segmenter le réseau est une meilleure pratique pour gagner en visibilité et réduire la surface d'attaque. ❑ Déployez GlobalProtect en mode interne pour qu'il agisse comme une passerelle pour contrôler l'accès au centre de données. GlobalProtect contrôle les informations sur l'utilisateur pour vérifier les utilisateurs, et les informations sur l'hôte pour vérifier que la sécurité de l'hôte est à jour, en comparant les informations sur l'hôte aux objets HIP et profils que vous définissez. Cela garantit que les hôtes se connectant à votre réseau maintiennent votre niveau de normes de sécurité. ❑ Autorisez **Log At Session End (Se connecter en fin de session)** pour toutes les règles de politique de sécurité. ***Log At Session Start (Se connecter au début de la session)*** *consomme plus de ressources que la connexion uniquement à la fin de la session. Dans la plupart des cas, vous* ***Log At Session End (vous connectez en fin de session)*** *uniquement. Activez à la fois* ***Log At Session Start (Se connecter au début de la session)*** *et* ***Log At Session End (Se connecter en fin de session)*** *uniquement pour le dépannage, pour les sessions de tunnel de longue durée telles que les tunnels GRE (vous ne pouvez pas voir ces sessions dans l'ACC à moins de vous connecter au début de la session) et pour gagner en visibilité sur les sessions OT/ICS (Operational Technology/Industrial Control Systems), qui sont également des sessions de longue durée.* Avoir de la visibilité sur le trafic permet au pare-feu d'utiliser ses technologies natives App-ID, Content-ID, User-ID et Device-ID pour relier les applications, menaces et contenu aux utilisateurs, indépendamment de l'emplacement de l'utilisateur ou du type de périphérique, port, cryptage ou malgré l'utilisation de techniques d'évasion.
Réduire la surface d'attaque	La surface d'attaque consiste en tous les points d'interaction du réseau, aussi bien matériels que logiciels, et comprend les applications, le contenu et les utilisateurs, ainsi que les serveurs, commutateurs, routeurs et autres équipements matériels et virtuels. Réduire la surface d'attaque laisse moins de vulnérabilités à cibler pour les pirates informatiques. Plus vous réduisez la surface d'attaque, plus il est difficile de pénétrer dans le réseau. ❑ Évaluez votre centre de données afin de connaître les applications, le contenu et les utilisateurs du réseau. ❑ Approchez l'application de la sécurité de manière positive en créant des règles de politique de sécurité basées sur les applications qui autorisent uniquement l'utilisation d'applications à des fins professionnelles légitimes sur le réseau, et des règles qui bloquent toutes les applications à risque élevé sans cas d'utilisation légitime.

Méthodologie exemplaire	Pourquoi est-ce important ?
	❑ Utilisez les informations recueillies en évaluant l'environnement pour créer une stratégie qui segmente le réseau en zones basées sur les exigences métier, les fonctionnalités communes, et les exigences de politique globale, afin que les ressources de chaque zone nécessitent les mêmes niveaux de sécurité. Au sein du centre de données, segmentez en zones les applications tierces comme les bases de données, les serveurs web, les serveurs d'applications, les serveurs de développement et les serveurs de production. La segmentation vous permet de visualiser le trafic entre différents niveaux d'application, car le trafic doit traverser un pare-feu lorsqu'il circule entre les zones. La segmentation granulaire vous permet de créer des règles de politique de sécurité axées sur les exigences métier de chaque zone et de fournir la protection appropriée à chaque segment. La segmentation permet également d'enrayer les mouvements latéraux de logiciels malveillants vers le centre de données et au sein de celui-ci, car la combinaison d'App-ID, Content-ID (prévention des menaces) et User-ID vous permet d'identifier le trafic pouvant bénéficier d'un accès et de refuser le reste. ❑ Déployez GlobalProtect en mode interne pour qu'il agisse comme une passerelle pour contrôler l'accès au centre de données. ❑ Pour réduire encore plus la surface d'attaque, appliquez les profils de blocage de fichiers aux règles de politique de sécurité qui autorisent le trafic de l'application pour bloquer les types de fichiers à risque et malveillants. Préservez-vous des vols d'identifiants en autorisant la politique d'authentification du pare-feu à activer l'authentification multifacteur pour que, même si des pirates informatiques réussissent à voler des identifiants, ils ne puissent pas accéder au réseau du centre de données.
Empêchez les Menaces Connues	Les profils de sécurité associés aux règles d'autorisation des politiques de sécurité balayent le trafic à la recherche de menaces comme des virus, des logiciels espions, des exploits des vulnérabilités dans la couche application, des fichiers malveillants, et plus encore. Le pare-feu applique à ces menaces une action comme autoriser, alerter, abandonner, bloquer l'IP ou il procède à la réinitialisation de la connexion, selon la configuration du profil de sécurité. Suivez les meilleures pratiques de mise à jour de contenu et installez les mises à jour du contenu dès que possible après les avoir téléchargées pour mettre à jour les profils de sécurité et appliquer les dernières protections à votre centre de données. Les profils de sécurité sont des protections fondamentales faciles à appliquer aux règles de politique de sécurité. Les listes dynamiques externes (EDL) protègent également contre les menaces connues. Les EDL importent des listes d'adresses IP, d'URL ou de domaines malveillants et à risque dans le pare-feu pour empêcher les menaces connues. Les EDL proviennent de tierces parties dignes de confiance, d'EDL prédéfinis sur le pare-feu, et d'EDL personnalisés que vous pouvez créer. Les EDL sont mis à jour dynamiquement sur le pare-feu sans nécessiter de validation. La prévention des menaces connues est une autre raison pour laquelle il est important d'activer le décryptage. Si vous ne pouvez pas voir la menace, peu importe

Méthodologie exemplaire	Pourquoi est-ce important ?
	que vous la connaissiez ou non, vous en serez de toute façon victime, car vous ne l'aurez pas vue.
Prévenir les menaces inconnues	Comment détecter une menace que personne n'a jamais vue ? Il suffit de transférer tous les fichiers inconnus vers WildFire à des fins d'analyse. WildFire identifie les logiciels malveillants inconnus ou ciblés. La première fois qu'un pare-feu détecte un fichier inconnu, il transfère le fichier à sa destination interne ainsi qu'au cloud WildFire à des fins d'analyse. WildFire analyse le fichier (ou un lien dans un e-mail) et renvoie un verdict au pare-feu en seulement cinq minutes. WildFire inclut également une signature permettant d'identifier le fichier, changeant son statut de fichier inconnu à connu. Si le fichier contenait une menace, celle-ci est désormais connue. Si le fichier est malveillant, il sera bloqué la prochaine fois qu'il arrivera au pare-feu. Vous pouvez vérifier les verdicts dans les journaux de soumission WildFire (**Monitor [Surveiller]** > **Logs [Journaux]** > **WildFire Submissions [Soumissions WildFire]**). Paramétrez les mises à jour de contenu pour un appareil WildFire pour qu'elles soient téléchargées et installées de manière automatique toutes les minutes, vous assurant ainsi le support le plus actualisé. Par exemple, la prise en charge des fichiers Linux et SMB a été fournie pour la première fois dans les mises à jour du contenu de l'appareil WildFire.

En outre :

- Gérez les pare-feu de manière centralisée avec Panorama pour appliquer de manière cohérente des politiques à travers des environnements matériels et virtuels et pour une visibilité centrale.
- Une application positive de la sécurité permet d'autoriser le trafic que vous souhaitez sur le réseau de votre centre de données et refuser le reste.
- Créez une conception standardisée et évolutive que vous pouvez reproduire et appliquer de manière cohérente dans tous les centres de données.
- Obtenez l'adhésion des cadres dirigeants, des administrateurs du département informatique et du centre de données, d'utilisateurs et d'autres parties concernées.

Appliquez une sécurité nouvelle génération de manière graduelle en vous concentrant sur les menaces les plus probables liées à votre activité professionnelle et à votre réseau, puis déterminez les ressources les plus importantes à protéger afin de les protéger en premier lieu. Posez-vous les questions suivantes pour vous aider à déterminer quels actifs protéger en priorité :

1. *Qu'est-ce qui rend notre entreprise unique ?* Quelles caractéristiques définissent et différencient notre entreprise, et quelles ressources représentent ces caractéristiques ? Les ressources relatives à l'avantage concurrentiel propre à votre entreprise doivent figurer tout en haut de votre échelle de priorité de protection. Par exemple, une société de développement de logiciels donnerait la priorité à son code source, et une société pharmaceutique à ses formules médicamenteuses.
2. *Qu'est-ce qui garantit la pérennité de l'entreprise ?* De quels systèmes et applications avez-vous besoin pour soutenir les opérations quotidiennes de l'entreprise ? Par exemple, votre service Active Directory (AD) permet aux employés d'accéder aux applications et aux postes de travail. En compromettant votre service AD, vous accordez aux pirates informatiques l'accès à tous les comptes de votre entreprise,

leur fournissant un accès complet à votre réseau. D’autres exemples incluent des infrastructures informatiques essentielles comme des outils de gestion et des serveurs d’authentification, ainsi que des serveurs abritant les données les plus essentielles à vos activités commerciales.

3. *Si je perdais cette ressource, qu’arriverait-il ?* Plus les conséquences de la perte d’un actif sont graves, plus la priorité est de protéger cet actif. Par exemple, l’expérience utilisateur peut distinguer une société de service, donc protéger cette expérience est une priorité élevée. Les processus et équipements propriétaires peuvent différencier une entreprise manufacturière, c’est pourquoi la protection de la propriété intellectuelle et des conceptions exclusives est hautement prioritaire. Créez une liste des priorités pour déterminer ce qui doit être protégé en premier.

Définissez l’état futur idéal du réseau de votre centre de données et travaillez par étapes pour atteindre votre but. Revoyez régulièrement votre définition pour tenir compte des changements survenus dans votre entreprise, des nouvelles exigences réglementaires et juridiques ainsi que des nouvelles exigences de sécurité.

Comment puis-je déployer une politique de sécurité du centre de données respectant les meilleures pratiques ?

Le processus de travail pour mettre en place une politique de sécurité du centre de données respectant les meilleures pratiques est de tout connaître sur votre réseau de centre de données et ses ressources, ainsi que sur les capacités de prévention des menaces de votre pare-feu, et de créer ensuite des règles de politique de sécurité initiales basées sur ces informations, en commençant par protéger vos ressources les plus précieuses.

- Comment évaluer votre centre de données : identifiez et hiérarchisez les ressources à protéger, les plus grandes menaces pour ces ressources, ainsi que les applications et utilisateurs autorisés à y accéder.
- Comment décrypter le trafic du centre de données : vous ne pouvez pas protéger votre réseau contre les menaces que vous ne voyez pas. Le trafic crypté est une méthode couramment utilisée par les attaquants pour diffuser des menaces.
- Création d'une stratégie de segmentation du centre de données : segmenter votre centre de donnée empêche un adversaire ayant réussi à prendre pied dans le centre de données de se déplacer latéralement vers d'autres zones.
- Comment créer des profils de sécurité du centre de données respectant les meilleures pratiques : des applications légitimes peuvent distribuer des programmes malveillants de commandement et conduite, des expositions et vulnérabilités répandues (CVE), des téléchargements à la dérobée de contenu malveillant, des attaques par hameçonnage, et des menaces persistantes avancées (APTs). Les profils de sécurité respectant les meilleures pratiques protègent le trafic autorisé contre des menaces connues ou inconnues sur les quatre flux de trafic du centre de données.
- Utilisez Cortex XDR Agent pour protéger les terminaux du centre de données : les pare-feu assurent une protection contre les menaces qui traversent le réseau. Toutefois, les menaces qui s'exécutent sur un terminal ne traversent pas le réseau, donc elles ne passent pas par un pare-feu. Installez Cortex XDR Agents sur chaque terminal pour assurer une protection contre les menaces directement sur les terminaux.
- Création des règles de blocage du trafic pour le centre de données : dans votre centre de données, bloquez les adresses IP que vous avez identifiées comme malveillantes, les applications que les pirates informatiques exploitent fréquemment, les applications conçues pour éviter ou contourner les mesures de sécurité, et les applications sans raison professionnelle.
- Définition de la politique de sécurité initiale pour le trafic de l'utilisateur vers le centre de données : un accès non autorisé fait courir un risque majeur aux informations contenues dans le centre de données. Comme les employés ainsi que les autres utilisateurs du réseau interne d'entreprise sont souvent dignes de confiance, les mesures de sécurité peuvent laisser à désirer. Parfois, le public d'utilisateurs et le centre de données sont même sur un réseau plat. Contrôlez de manière étroite qui peut accéder au centre de données, les ressources auxquelles les différents groupes d'utilisateurs peuvent accéder, et le niveau d'accès aux applications des différents groupes d'utilisateurs.
- Définition de la politique de sécurité initiale du trafic d'Internet vers le centre de données : protégez les serveurs du centre de données de trafic malveillant d'Internet. Exploiter les vulnérabilités latérales du serveur expose le centre de données aux attaques et met vos collaborateurs en péril, car un serveur de centre de données compromis pourrait faire suivre ces exploits aux clients tiers.
- Définition de la politique de sécurité initiale du trafic du centre de données vers Internet : un programme malveillant de commandement et contrôle se cachant dans un serveur Internet-connecté

peut utiliser des applications légitimes pour télécharger encore plus de programmes malveillants. Empêchez les applications d'utiliser les ports non standards, permettez uniquement le transfert de types de fichiers que chaque application utilise de manière légitime, et bloquez les catégories URL telles que les programmes malveillants, le hameçonnage, le proxy anonymiseur, le pair à pair et autres catégories potentiellement malveillantes.

- Définition de la politique de sécurité initiale du trafic au sein du centre de données (trafic dit est-ouest) : les menaces provenant du cœur du centre de données sont souvent négligées, car aucun trafic utilisateur n'y trouve son origine et cet endroit est considéré comme digne de confiance. Cependant, si un attaquant compromet un serveur du centre de données, la communication entre les serveurs et les machines virtuelles peut propager des logiciels malveillants. La politique de sécurité respectant les meilleures pratiques empêche les pirates informatiques de se déplacer latéralement à travers le centre de données et de compromettre plus de systèmes ou d'exfiltrer des données.
- Journalisation et surveillance du trafic du centre de données : journalisez et surveillez le trafic bloqué et autorisé fournit des informations à toutes les étapes de la transition vers une politique de sécurité du centre de données respectant les meilleures pratiques ainsi qu'au niveau de sa maintenance. Cela révèle les applications, les utilisateurs, les tendances de trafic sur votre réseau, y compris ceux dont vous ignoriez l'existence. Ces informations vous aident à enquêter sur de potentiels problèmes de sécurité.
- Maintenez la base de règles du centre de données respectant les meilleures pratiques : surveillez continuellement votre liste d'autorisation pour les applications afin d'adapter vos règles pour supporter des applications nouvellement autorisées et pour déterminer les effets des nouvelles App-IDs ou des App-IDs modifiées sur votre politique.

La section Tri de la base de règles de la politique de sécurité du centre de données récapitule la base de règles de la politique de sécurité.

Comment évaluer votre centre de données ?

Pour réaliser un modèle de sécurité Zero Trust, vous devez connaître et évaluer les actifs de votre centre de données afin de pouvoir protéger en priorité les actifs les plus précieux, déterminer qui doit y avoir accès et comprendre les risques majeurs qu'ils encourent. Comprendre les utilisateurs qui accèdent à ces ressources, les applications autorisées ainsi que le réseau lui-même vous permet d'évaluer quels sont vos besoins et ce en quoi vous pouvez avoir confiance. Ainsi, vous pourrez façonner une politique de sécurité du centre de données respectant les meilleures pratiques, autorisant uniquement les accès utilisateurs et les applications ayant des raisons professionnelles légitimes sur le réseau.

1. **Faites l'inventaire de l'environnement du centre de données** : faites l'inventaire des environnements matériels et virtuels du centre de données, y compris serveurs, routeurs, commutateurs, périphériques de sécurité et autre infrastructure de réseau, et faites l'inventaire des applications du centre de données (y compris les applications propres à l'entreprise développées en interne) ainsi que des comptes de service.

   - Évaluez chaque système basé sur son rôle dans le réseau et sur son importance dans l'activité afin de hiérarchiser les portions de l'infrastructure matérielle et virtuelle à protéger en premier. Par exemple, si votre entreprise implique des transactions par carte de crédit, les serveurs qui gèrent ce type de transactions et le chemin de communication du trafic transportant les informations des cartes de crédit sont des actifs extrêmement précieux qui devraient être protégés en priorité.
   - Examinez les journaux du trafic sur au moins 90 jours pour dresser l'inventaire des applications sur le réseau du centre de données. Créez un rapport personnalisé basé sur la base de données d'applications du centre de données pour vous aider à identifier les applications existantes du centre de données. Utilisez l'inventaire des applications du centre de données pour développer une liste d'autorisation pour les applications que vous voulez approuver ou tolérer dans votre réseau de centre de données, y compris les applications propres à l'entreprise développées en interne.

     Votre inventaire initial d'applications ne doit pas forcément identifier l'ensemble des applications, car en surveillant les règles de blocage que vous configurez pour les règles de base de sécurité du centre de données respectant les meilleures pratiques, vous découvrirez les applications que vous n'avez pas identifiées. Concentrez vos efforts sur l'inventaire des applications et le type d'applications que vous voulez autoriser. Une fois que vous avez fini de dresser la liste d'autorisation pour les applications, toutes les applications que vous n'avez pas explicitement autorisées sont refusées.

   Mappez les applications aux besoins de votre entreprise. Si une application n'est pas attribuée à un besoin commercial, demandez-vous si elle doit être tolérée sur le réseau. Les applications ne répondant à aucun besoin commercial apparent augmentent la surface d'attaque et peuvent faire partie d'un ensemble d'outils d'un pirate informatique. Même si une application non inutile est innocente, la meilleure pratique consiste à la retirer afin qu'il y ait une surface en moins d'exploitable par un pirate informatique. Si plusieurs applications remplissent la même fonction, par

exemple le partage de fichiers ou la messagerie instantanée, envisagez de standardiser une ou deux applications pour réduire la surface d'attaque.

Si des applications internes propres à l'entreprise n'utilisent pas leur port par défaut, notez les ports et les services requis pour les prendre en charge. Envisagez de réécrire les applications internes propres à l'entreprise afin qu'elles utilisent leur port par défaut.

Créez des groupes pour les applications nécessitant un traitement similaire sur le réseau afin d'appliquer efficacement la politique de sécurité aux groupes d'applications plutôt qu'aux applications individuelles. Les groupes d'applications permettent de concevoir et mettre en place des politiques de sécurité plus facilement, car vous pouvez appliquer une politique à l'ensemble des applications d'un groupe à un moment donné, changer la politique de l'ensemble du groupe, ajouter de nouvelles applications au groupe afin d'appliquer la politique du groupe aux nouvelles applications, et réutiliser un groupe d'applications dans de nombreuses règles de politique de sécurité. Par exemple, un groupe d'applications conçu pour des applications de stockage du centre de données peut inclure des applications comme crashplan, ms-ds-smb, et NFS.

- Faites l'inventaire des comptes de service que les applications utilisent pour communiquer entre serveurs et au sein des serveurs du centre de données. La meilleure pratique consiste à utiliser un compte de service pour chaque fonction plutôt qu'un compte de service pour plusieurs fonctions. Cela limite l'accès au compte de service et permet de comprendre plus facilement comment un compte de service a été utilisé si un système est compromis. Une autre meilleure pratique consiste à identifier les comptes de service qui sont codés en dur dans l'application pour pouvoir écrire des signatures de prévention d'intrusion à leur encontre et surveiller leur utilisation.

2. **Qualifiez le trafic du centre de données** : qualifiez et cartographiez le trafic du centre de données pour comprendre comment les données circulent à travers votre réseau et entre utilisateurs et ressources. Constituez une équipe polyvalente comprenant architectes d'applications, architectes réseau, architectes d'entreprise et représentants commerciaux. La caractérisation des flux de trafic vous informe sur les sources et destinations du trafic réseau, les modèles et charges de trafic types, et vous aide à comprendre le trafic sur votre réseau et à protéger en priorité le trafic le plus important. Utilisez les widgets du Centre de Commande de l'Application , les fonctionnalités de surveillance de la santé du pare-feu de Panorama, ainsi que d'autres méthodes pour comprendre la tendance normale du trafic (de base), afin de vous aider à comprendre les tendances d'un trafic anormal, qui pourrait être le signe d'une attaque.
3. **Examinez la segmentation du centre de données** : segmentez les couches de serveurs du centre de données afin que les communications entre les différentes couches du serveur passent par des pare-feu nouvelle génération, et qu'elles soient décryptées, examinées et protégées par une politique de sécurité respectant les meilleures pratiques, et afin que les communications entre le public d'utilisateurs et Internet passent par des pare-feu nouvelle génération. À l'extérieur du centre de données, comprenez quelles zones *peuvent* communiquer avec chaque zone du centre de données et déterminez ensuite quelles zones *devraient* être autorisées à communiquer avec chaque zone du centre de données.
4. **Examinez la segmentation du public utilisateur et déterminez qui devrait avoir accès au centre de données** : attribuez les utilisateurs à des groupes pour segmenter le public utilisateur, afin de contrôler plus facilement l'accès aux systèmes sensibles. Par exemple, les utilisateurs du groupe Gestion de produits ne devraient pas pouvoir accéder aux systèmes des finances ou des ressources humaines. Dans Active Directory (ou tout autre système utilisé), créez des groupes d'utilisateurs granulaires basés sur le niveau d'accès requis par les utilisateurs pour des raisons professionnelles légitimes, afin de contrôler

l'accès aux systèmes et applications. Cela comprend différents groupes d'employés ainsi que différents groupes de sous-traitants, collaborateurs, clients et fournisseurs, regroupés par niveau d'accès requis.

Réduisez la surface d'attaque en créant des groupes d'utilisateurs basés sur les besoins en accès plutôt que sur la seule fonctionnalité, et autorisez uniquement les niveaux d'accès appropriés aux applications pour chaque groupe. Au sein d'une région fonctionnelle comme le Marketing ou les Sous-traitants, créez de multiples groupes d'utilisateurs cartographiés selon les besoins d'accès aux applications.

5. **Surveillance continue du réseau du centre de données** : journalisez et surveillez le trafic du centre de données pour révéler des lacunes dans la politique de sécurité du centre de données respectant les meilleures pratiques, pour révéler des tendances inhabituelles dans le trafic ou des tentatives d'accès inattendues qui pourraient être le signe d'une attaque, et pour diagnostiquer des problèmes d'applications.

Une méthode utile pour évaluer les actifs consiste à les regrouper. Identifiez vos actifs les plus précieux qui doivent être protégés en priorité, ainsi que les actifs sur lesquels vous pouvez itérer après avoir protégé ces actifs. Hiérarchisez l'ordre dans lequel protéger les ressources dans chaque catégorie. Organisez les ressources de la façon la plus adaptée à votre secteur d'activité. Le tableau suivant vous montre plusieurs possibilités, mais il n'est pas exhaustif. Tenez également compte des exigences de conformité légale pour protéger les données telles que les mots de passe et les informations personnelles et financières lorsque vous décidez des actifs à protéger en priorité.

Table 1: Exemple de catégories d'actifs

Actifs les plus précieux	Autres actifs précieux	Ressources restantes (Itérez)
• Brevets • Code source • Données confidentielles comme conceptions de produit, formules de médicaments, ou données utilisateurs. • Algorithmes propriétaires • Certificats de signature de code et PKI (ce sont les clés de votre royaume chiffré) • Serveur de domaine AD (perdre l'AD donne la possibilité à un pirate informatique de créer des identifiants lui fournissant un accès illimité au réseau) • Autres actifs très prisés qui distinguent votre entreprise des autres entreprises	• Infrastructure informatique critique comme les interfaces de routeurs et de pare-feu • Services d'authentification • Messagerie • VPN, en particulier pour les entreprises hautement décentralisées • Applications de stratégie professionnelle • Serveurs de partage de fichiers • Bases de données	• Équipement de laboratoire réseau • Systèmes de gestion informatique • Autres actifs

Chaque entreprise détermine quels sont ses actifs prioritaires. Pour une société de services, l'expérience utilisateur permet de distinguer la société des autres, ainsi les ressources les plus précieuses peuvent être

celles qui assurent la meilleure expérience utilisateur possible. Pour une entreprise manufacturière, les actifs les plus précieux peuvent être les procédés et les conceptions d'équipements exclusifs. Envisager quelles seraient les conséquences de la perte d'une ressource est une bonne façon de comprendre quelles ressources doivent être protégées en priorité.

Comment décrypter le trafic d'un centre de données ?

Vous ne pouvez pas protéger votre réseau des menaces que vous ne pouvez pas voir ni inspecter. Décrypter le trafic pour révéler les programmes malveillants est essentiel, car la majorité du trafic typique d'un réseau est crypté, et ce volume est en constante augmentation. Un pourcentage de plus en plus important de campagnes de logiciels malveillants qui cachent des intrusions réseau, installent des logiciels malveillants de commande et de contrôle et extraient des données, utilisent également le cryptage.

Pour révéler des applications et des menaces cryptées, placez des pare-feu nouvelle génération matériels ou virtuels à des endroits leur permettant de voir l'ensemble du trafic du centre de données. Décryptez le plus de trafic possible, particulièrement les catégories de trafic à haut risque en destination des serveurs critiques et le trafic stratégique pour l'entreprise. En décryptant le trafic, vous l'identifiez et permettez au pare-feu d'appliquer l'antivirus, les protections contre les vulnérabilités, WildFire et les autres protections appropriées contre les menaces.

Afin d'appliquer le décryptage au trafic, créez des profils de décryptage qui spécifient comment traiter le trafic TSL et SSH et le trafic que vous choisissez de ne pas décrypter ou ne pouvez pas décrypter. Les profils de décryptage définissent les caractéristiques autorisées des protocoles, algorithmes, modes et sessions pour le trafic. Vous appliquez les profils de Décryptage aux règles de politique de décryptage, qui spécifient le trafic auquel le pare-feu applique les profils de Décryptage.

Le pare-feu prend en charge deux types de décryptage SSL/TLS et SSH :

- Proxy de transfert SSL (trafic sortant)
- Inspection SSL entrante (trafic entrant)
- Proxy SSH (habituellement pour sécuriser l'accès des administrateurs qui gèrent les périphériques du réseau)

Au sein du centre de données, décryptez le plus de trafic est-ouest possible. Si des considérations de rendement à cause de la taille inadaptée du pare-feu vous empêchent de décrypter l'ensemble du trafic, privilégiez les serveurs les plus essentiels, les catégories de trafic les plus à risque, et les segments et sous-réseaux IP les moins dignes de confiance, et décryptez autant de trafic que vous pouvez tout en gardant un rendement acceptable. Voici les principales questions que vous devez vous poser : « Que se passe-t-il si le serveur est compromis ? », « Quel risque représente chaque catégorie de trafic ? », et « Quel risque suis-je prêt à prendre par rapport au niveau de rendement que je veux atteindre au cœur du centre de données ? »

Pour le trafic circulant du centre de données vers Internet, décryptez tout excepté le trafic pour lequel vous devez faire des exceptions. La visibilité que fournit le décryptage est particulièrement importante, car les serveurs du centre de données ne doivent pas se connecter à des sites malveillants, transférer des fichiers malveillants, ou être vulnérables au téléchargement de programmes malveillants.

Lorsque vous planifiez votre politique de décryptage, tenez compte des règles et des positions de votre entreprise en matière de conformité de sécurité. Pour le trafic d'utilisateurs vers le centre de données, bien qu'une politique stricte de décryptage puisse causer quelques plaintes au commencement, ces plaintes peuvent attirer votre attention sur des sites non autorisés ou indésirables qui sont bloqués, car ils utilisent des algorithmes faibles ou parce qu'ils ont des problèmes de certificats. Utilisez les plaintes comme des outils pour avoir une meilleure compréhension du trafic sur votre réseau.

De plus, activez la journalisation de décryptage dans les politiques de décryptage et si les ressources le permettent, enregistrez les établissements de liaison retenus et rejetés. Profitez de tous les outils de surveillance et de dépannage du décryptage pour examiner votre déploiement et perfectionner vos politiques et profils.

Le décryptage du trafic consomme les ressources du pare-feu. La quantité de trafic à décrypter varie d'un centre de données à l'autre. Quand vous évaluez la taille du déploiement du pare-feu pour garder un rendement acceptable tout en prenant en charge le décryptage, prenez en compte la quantité de trafic que vous prévoyez de décrypter (certaines applications doivent être décryptées alors que d'autres ne sont pas cryptées et ne nécessitent pas d'être décryptées), le cryptage de décryptage (des cryptages plus forts et plus complexes demandent plus de puissance de traitement pour être décryptés), la taille des clés (des clés de plus grande taille consomment plus de ressources de décryptage), le type d'échange de clé (par exemple, des échanges de clés RSA consomment plus de ressources de traitement que des clés PFS), et la capacité des pare-feu. Travaillez de concert avec votre équipe commerciale et vos représentants Palo Alto Networks pour dimensionner le déploiement du pare-feu de manière appropriée à votre réseau afin de pouvoir déchiffrer le trafic et exposer les menaces.

Les entreprises ayant des activités financières, par exemple, qui requièrent un système de sécurité extrêmement fort pour leurs clés privées, peuvent faire appel à des Modules Matériels de Sécurité (HSM) tiers pour sécuriser et gérer les clés privées de l'entreprise, au lieu de les conserver dans le pare-feu.

- Création des profils de décryptage respectant les meilleures pratiques concernant le centre de données
- Exclusion de tout trafic inadapté au décryptage du centre de données

Création des profils de décryptage respectant les meilleures pratiques concernant le centre de données

Les profils de décryptage spécifient la manière dont le pare-feu vérifie le trafic déchiffré ainsi que le trafic que vous ne pouvez pas ou choisissez de ne pas déchiffrer. Le pare-feu vérifie les protocoles, les certificats serveur, les caractéristiques de la session et les cryptages (algorithmes d'échange de clés, algorithmes d'encodage, algorithmes d'authentification). Vous appliquez les profils de décryptage (**Objects** > **Decryption Profile**) aux règles de politique de décryptage (**Policies** > **Decryption**). Les règles de politique de décryptage définissent le trafic à vérifier en utilisant la source, la destination, la catégorie de service ainsi que la catégorie URL comme des critères de correspondance afin d'avoir un contrôle granulaire sur le trafic auquel vous appliquez un profil de Décryptage. Vous configurez la journalisation du décryptage et le transfert des journaux dans la règle de politique.

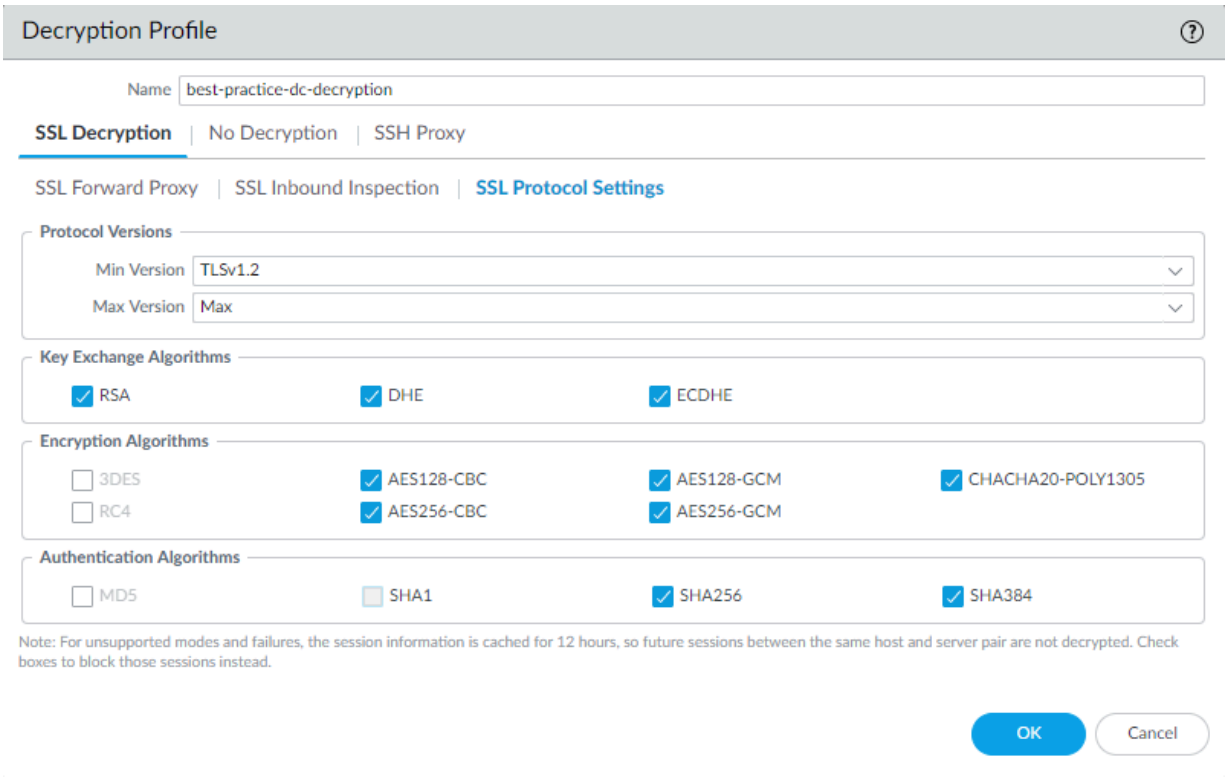
Pour décrypter du trafic sortant, le pare-feu agit comme un proxy de transfert entre le client interne et le serveur externe. Afin d'examiner du trafic entrant, le pare-feu effectue une copie du trafic de la session entrante et décrypte et examine la copie.

STEP 1 | Configurez le pare-feu pour qu'il effectue des vérifications CRL/OCSP, afin de vous assurer que les certificats présentés au cours du décryptage sont valides.

STEP 2 | Configurez le **SSL Decryption (Décryptage SSL)** > **SSL Protocol Settings (Paramètres du protocole SSL)** pour bloquer les versions SSL/TLS vulnérables telles que TLSv1.0, TLSv1.1 et

SSLv3 et pour éviter les algorithmes de cryptage faibles tels que RC4 et 3DES et les algorithmes d'authentification faibles tels que MD5 et SHA1.

Les paramètres du protocole SSL s'appliquent à tout trafic décrypté.



Définissez la **Min Version** (Version min.) du protocole sur **TLSv1.2** et la **Max Version** (Version max.) sur **Max** pour bloquer les protocoles faibles. Utilisez le protocole TLS le plus fort qui est disponible. Créez des politiques et des profils de décryptage distincts pour optimiser la sécurité. Par exemple, si d'anciens sites dont vous avez besoin à des fins professionnelles ne prennent en charge que des protocoles plus faibles, créez un profil de décryptage distinct pour autoriser le protocole plus faible et appliquez-le dans une politique de décryptage uniquement aux sites qui ne prennent pas en charge au moins le protocole TLSv1.2. Cela s'applique également aux sites professionnels essentiels qui ne prennent pas en charge les algorithmes puissants pour des catégories d'URL différentes pour mettre au point la sécurité par rapport à la performance.

Si le site n'héberge pas d'application professionnelle légitime, n'affaiblissez pas votre posture de sécurité en renforçant ce site : des protocoles ainsi que des cryptogrammes 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 professionnelles, utilisez la fonction de Filtrage des URL pour bloquer l'accès à l'ensemble de la catégorie. Ne renforcez pas de faibles

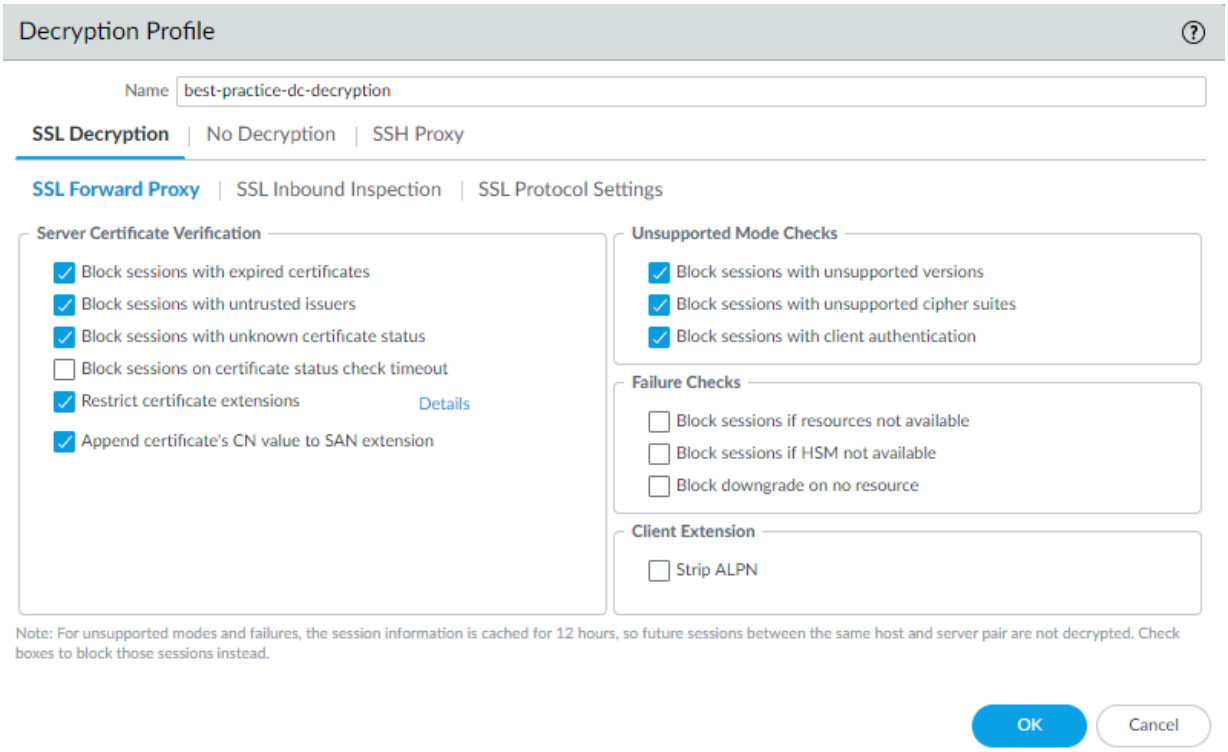
protocoles ou de faibles algorithmes de cryptage ou d'authentification sauf si vous y êtes obligé afin de renforcer des sites importants reposant sur d'anciens systèmes.

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.

De nombreuses applications mobiles utilisent des certificats épinglés. Comme TLSv1.3 crypte les informations de certification, le pare-feu ne peut pas ajouter ces applications mobiles automatiquement à la liste d'exclusion de décryptage SSL. Pour ces applications, assurez-vous que la ***Max Version*** *(Version maximale) du profil de décryptage est configurée sur TLSv1.2 ou appliquez une politique de non-décryptage pour le trafic.*

STEP 3 | Configurez les paramètres **SSL Decryption (Décryptage SSL)** > **SSL Forward Proxy (Proxy de transfert SSL)** du trafic sortant pour bloquer les exceptions lors de la négociation TSL et pour bloquer les sessions qui ne peuvent être déchiffrées.

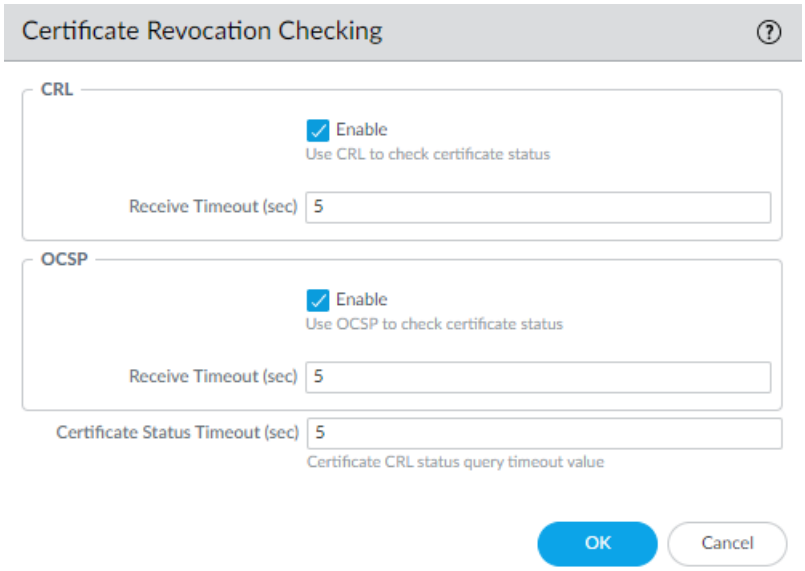
Dans certains cas, les paramètres respectant les meilleures pratiques dépendent des règles de conformité de votre entreprise. Appliquez le profil de décryptage Proxy de transfert SSL aux règles de politique de sécurité qui contrôlent le trafic sortant.



Bloquez les exceptions au cours des négociations TSL et bloquez les sessions ne pouvant être décryptées.

- **Vérification du Certificat Serveur** : le fait de cocher ou non **Blocage des sessions à expiration du délai de vérification du certificat** dépend de la position de votre entreprise concernant les règles de conformité, car cela implique un compromis entre une sécurité plus stricte 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 sur le délai d'expiration de vérification de l'état du certificat** et que le serveur de révocation est lent à répondre, vous pouvez utiliser **Device (Périphérique)** > **Setup (Configuration)** > **Session** > **Decryption Settings**

(Paramètres de décryptage) et cliquer sur **Certificate Revocation Checking (Vérification de la révocation du certificat)** pour modifier la valeur du délai d'expiration par défaut de cinq secondes en une autre valeur.



Activez la vérification de la révocation des certificats CRL et OCSP, car les certificats du serveur peuvent contenir l'URL CRL dans l'extension CDP (CRL Distribution Point) ou l'URL OCSP dans l'extension du certificat AIA (Authority Information Access).

Bien que la meilleure pratique consiste à utiliser un certificat approprié, certains certificats laissent le champ SAN (Subject Alternate Name) vide, ce qui peut amener les pare-feu à rejeter ces certificats. Cochez **Ajouter la valeur du CN du certificat à l'extension SAN** pour copier automatiquement le numéro du certificat dans le champ SAN si le champ SAN est vide. Ainsi, si vous menez des activités avec des sites qui ne remplissent pas les champs SAN de leur certificat, vous pouvez toujours accepter leurs certificats. Sinon, les sites doivent régénérer leurs certificats pour se conformer aux meilleures pratiques et remplir le champ SAN.

Bloquez toutes les autres exceptions de vérification du certificat du serveur.

- **Contrôles de mode non pris en charge** : si vous ne bloquez pas les sessions avec des versions non prises en charge et des suites de cryptage non prises en charge, les utilisateurs reçoivent un message d'avertissement qu'ils n'ont qu'à cliquer pour atteindre le site Internet à risque. Si vous configurez des paramètres de protocole SSL très stricts, c'est précisément pour bloquer et vous protéger de serveurs qui utilisent ces faibles (à risque) versions de protocoles et d'algorithmes. De plus, bloquer des sessions avec des contrôles de modes non pris en charge vous protège de portes dérobées malveillantes et autres menaces utilisant un cryptage personnalisé et non standard pour dissimuler leurs activités.

  Le blocage de sessions nécessitant une authentification client vous permet de choisir d'autoriser ou de bloquer les sessions utilisant une authentification client. Bien que l'authentification serveur puisse être l'unique authentification utilisée pour établir une session, certains sites font appel à une authentification mutuelle, où aussi le serveur comme le client s'authentifient pour établir une session. L'authentification client utilisant un certificat numérique X.509 est semblable à une authentification serveur dans la mesure où les deux méthodes utilisent un certificat numérique émis par une autorité de certification pour authentifier la session. Le certificat client agit comme un identifiant numérique pour le client, demeure sur l'équipement du client, et ne peut être déplacé

sur d'autres équipements. Toutefois, l'authentification client empêche le pare-feu de décrypter la session, car le pare-feu nécessite aussi bien le certificat client que le certificat serveur pour réaliser un décryptage bidirectionnel, alors que le pare-feu ne connaît que le certificat serveur. Cela met un terme au décryptage de sessions avec authentification client.

Si vous n'activez pas l'option **Blocage des 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. Les entrées demeurent 12 heures dans le cache et finissent par expirer. Si un même utilisateur ou un utilisateur différent tente d'accéder au serveur pendant les 12 heures en utilisant l'authentification client, le pare-feu fait correspondre la session à l'entrée dans le cache de décryptages exclus, ne tente pas de décrypter le trafic, et autorise la session cryptée.

Si le cache d'exclusions se remplit, le pare-feu purge les entrées les plus anciennes à mesure que de nouvelles entrées se présentent. Si vous changez la politique ou le profil de Décryptage, le pare-feu évacue le cache d'exclusion, car la politique ou le profil peut changer le résultat de classification de la session.

Si vous activez l'option**Blocage de sessions nécessitant une authentification client**, le pare-feu bloque les sessions utilisant une authentification client, à l'exception des sessions de sites demeurant sur la liste d'exclusion du décryptage SSL (**Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **SSL Decryption Exclusion (Exclusion du décryptage SSL)**).

Vous aurez peut-être besoin d'autoriser sur votre réseau le trafic en provenance d'autres sites utilisant une authentification client en plus des sites prédéfinis présents sur la liste d'exclusion du Décryptage SSL. Créez un profil de décryptage autorisant des sessions avec authentification client. Ajoutez-le à la règle de politique de décryptage s'appliquant uniquement aux serveurs abritant l'application. Pour renforcer encore plus la sécurité, vous pouvez exiger une Authentification Multifactorielle pour compléter le processus de connexion de l'utilisateur.

Pour tout autre trafic, appliquez le profil de décryptage qui bloque les sessions avec authentification client.

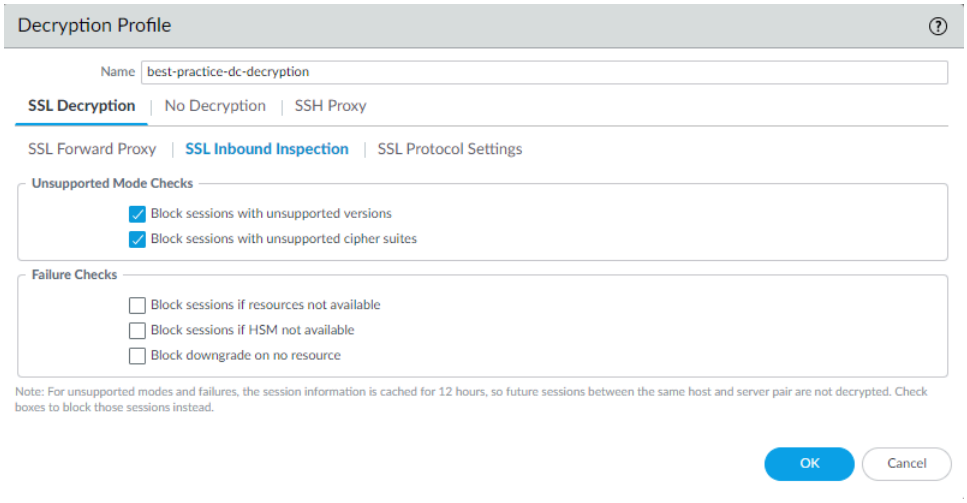
- **Contrôles de Défaillance** : si vous n'activez pas le **Blocage de sessions si les ressources ne sont pas disponibles**, le manque de ressources de traitement risque d'autoriser des connexions potentiellement dangereuses. Si vous bloquez des sessions pour lesquelles les ressources ne sont pas disponibles, cela peut affecter l'expérience utilisateur. 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.

  Si vous utilisez un Hardware Security Module (module de sécurité matériel - HSM) pour stocker vos clés privées, que vous cochiez ou non **Block sessions (Bloquer les sessions) si le HSM n'est pas disponible** dépend de vos règles de conformité concernant la provenance des clés privées et de votre façon de traiter le trafic crypté 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 (HA) (PAN-OS 8.0 prend en charge deux membres d'une paire HA HSM).

- **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.

STEP 4 | Configurez les paramètres **SSL Decryption (Décryptage SSL)** > **SSL Inbound Inspection (Inspection SSL entrante)** pour inspecter le trafic entrant dans vos serveurs internes depuis un client externe et pour bloquer les sessions douteuses.

Appliquez le profil d’Inspection SSL Entrante aux règles de politique de sécurité contrôlant le trafic entrant.



- **Contrôles de mode non pris en charge** : le pare-feu ne peut pas décrypter les versions de session et les cryptages non pris en charge par le pare-feu. Pour empêcher les pirates informatiques d’utiliser des versions et des cryptages non pris en charge de se faufiler dans votre réseau, bloquez les versions de session et les suites de cryptages non pris en charge par votre pare-feu. De plus, le blocage de sessions avec des vérifications de mode non prises en charge vous protège des portes dérobées malveillantes et autres menaces qui utilisent un cryptage personnalisé et non standard pour masquer leurs activités.

  Sur le serveur, activez uniquement les chiffrements que vous prenez en charge sur le pare-feu. Assurer cette compatibilité rend la négociation entre le client et le serveur plus fluide.
- **Contrôles de Défaillance** : si vous n’activez pas le **Blocage de sessions si les ressources ne sont pas disponibles**, le manque de ressources de traitement risque d’autoriser des connexions potentiellement dangereuses. Si vous bloquez des sessions pour lesquelles les ressources ne sont pas disponibles, cela peut affecter l’expérience utilisateur. La mise en œuvre ou non de contrôles

de défaillance dépend de la position de votre entreprise en matière de conformité à la sécurité et de l'importance qu'elle accorde à l'expérience utilisateur, comparée à une sécurité plus stricte.

Si vous utilisez un Hardware Security Module (module de sécurité matériel - HSM) pour stocker vos clés privées, que vous cochiez ou non **Block sessions (Bloquer les sessions) si le HSM n'est pas disponible** dépend de vos règles de conformité concernant la provenance des clés privées et de votre façon de traiter le trafic crypté 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 (HA) (PAN-OS 8.0 prend en charge deux membres d'une paire HA HSM).

- **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.

STEP 5 | Pour le trafic SSH, configurez les paramètres du profil de décryptage Proxy SSH.

Le décryptage SSH autorise le trafic SSH correctement routé et rejette le trafic utilisant un tunnel SSH (redirection de port SSH), sans toutefois effectuer d'inspection de menace ou de contenu sur le trafic SSH. Des sessions utilisant des SSH peuvent tunneliser 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 :

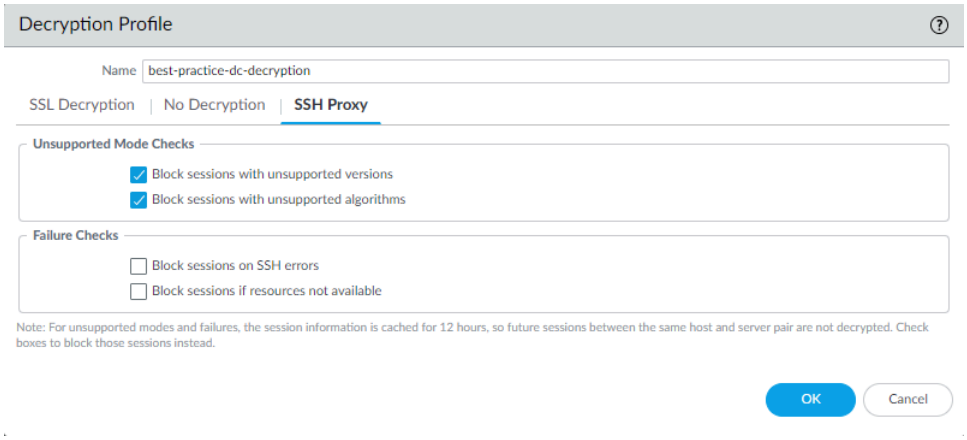
- session
- X11
- forwarded-tcpip
- direct-tcpip

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.

Pour la plupart des groupes utilisateurs, vous n'avez probablement pas de raison d'autoriser le trafic SSH dans le centre de données. Le protocole SSH est habituellement utilisé pour des accès distants aux serveurs, une possibilité qu'il vaut mieux éviter pour la plupart des utilisateurs, car cela expose votre centre de données à un risque accru, à l'accès à des serveurs Linux et à du transfert de fichiers. Vous n'avez pas la possibilité de décrypter du trafic SSH, donc toute personne utilisant le protocole

SSH pour accéder aux ressources d'un centre de données doit être fiable, et même dans ce cas, tous les profils de menaces doivent être appliqués à toute règle autorisant un accès SSH, afin de détecter la présence de logiciel malveillant, de virus, de logiciel espion, etc.

Par exemple, un cas d'utilisation est le personnel du département informatique dont la tâche est de gérer et maintenir les serveurs du centre de données, et qui utilise donc le protocole SSH pour des accès distants.



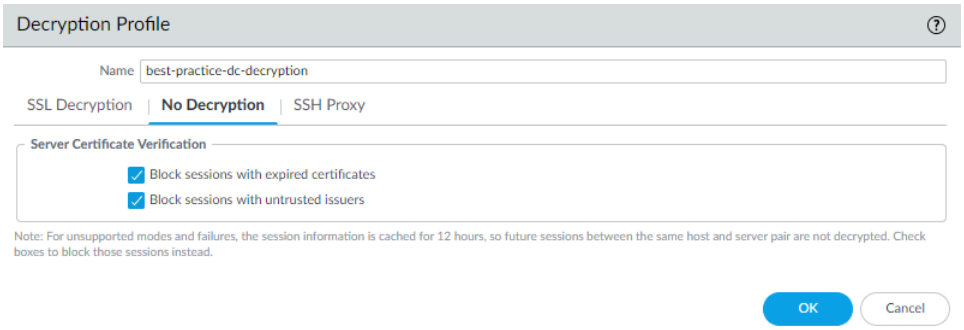
- **Contrôles de mode non pris en charge** : le pare-feu ne peut pas décrypter les versions de session et les cryptages non pris en charge par le pare-feu, et les cryptages peuvent s'avérer vulnérables. Pour empêcher les pirates informatiques d'utiliser des versions et des cryptages non pris en charge de se faufiler dans votre réseau, bloquez les versions de session et les suites de cryptages non pris en charge par votre pare-feu. Par ailleurs, bloquer des sessions avec des contrôles de modes non pris en charge vous protège de portes dérobées malveillantes et autres menaces utilisant un cryptage personnalisé et non standard pour dissimuler leurs activités.
- **Contrôles de Défaillance** : si vous n'activez pas le **Blocage de sessions si les ressources ne sont pas disponibles**, le manque de ressources de traitement risque d'autoriser des connexions potentiellement dangereuses. Si vous bloquez des sessions pour lesquelles les ressources ne sont pas disponibles, cela peut affecter l'expérience utilisateur. 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.

STEP 6 | Pour le trafic que vous choisissez de ne pas décrypter, configurez les paramètres **Aucun décryptage** pour bloquer les sessions cryptées destinées aux sites dont les certificats ont expiré ou aux émetteurs non approuvés.

Appliquez le profil « Aucun décryptage » uniquement au trafic que vous choisissez de ne pas décrypter pour suivre les législations ou les règles de conformité, et non au trafic que vous ne pouvez pas décrypter pour des raisons techniques, comme un certificat épinglé (ajoutez ce trafic à la liste

d'exclusion du décryptage SSL). La meilleure pratique consiste à décrypter autant de trafic du centre de données que possible.

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.



Exclusion de tout trafic inadapté au décryptage du centre de données

Deux types de trafic ne se prêtent pas au décryptage :

- Le trafic qui interrompt le décryptage pour des raisons techniques, comme faire appel à l'authentification par certificat client, un certificat épinglé ou une chaîne de certificat incomplète.
- Le trafic que vous choisissez de ne pas décrypter.

Le pare-feu fournit une liste prédéfinie d'exclusions de décryptage SSL (**Device [Périphérique] > Certificate Management [Gestion de Certificat] > SSL Decryption Exclusion [Exclusion de Décryptage SSL]**) pour des sites couramment utilisés qui interrompent le décryptage pour des raisons techniques. Vous pouvez supprimer des sites prédéfinis de la liste en cochant la case en regard du nom d'hôte du site, puis en cliquant sur **Disable (Désactiver)**. Vous pouvez aussi ajouter des sites à la liste. Utilisez la liste d'exclusions de décryptage uniquement pour les sites qui interrompent le décryptage pour des raisons techniques, ne l'utilisez pas pour des sites que vous choisissez de ne pas décrypter. Si le décryptage interrompt une application importante, ajoutez-la à la liste d'exclusions de décryptage pour créer une exception à l'adresse IP, au domaine ou au nom commun précis qui se trouvent dans le certificat associé à l'application. Certaines applications internes propres à l'entreprise peuvent cesser de fonctionner si vous les décryptez.

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 cryptage 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** > **Certificate Management** > **SSL Decryption Exclusion** > **Show Local Exclusion Cache**).

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.

Si la raison technique d'exclusion un site du décryptage est une chaîne de certificat incomplète, vous pouvez utiliser les informations dans le journal de décryptage pour réparer la chaîne de certificat incomplète *afin que vous puissiez autoriser, décrypter et inspecter the trafic.*

Vous pouvez choisir de ne pas décrypter le trafic pour des raisons telles que la réglementation et la conformité à la loi. Par exemple, le Règlement général sur la protection des données (RGPD) de l'Union Européenne (UE) introduit une forte protection de toutes les données personnelles pour tous les individus. 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.

Concernant le trafic que vous choisissez de ne pas décrypter, assurez-vous que c'est réellement du trafic que vous ne voulez pas décrypter, puis créez une exclusion basée sur une politique qui spécifie l'application, le groupe d'utilisateurs, la source et la destination, l'URL, la catégorie et/ou le service, afin de limiter chaque exclusion le plus possible. Plus l'exclusion de décryptage sera spécifique, mieux c'est, afin de ne pas exclure du décryptage plus de trafic que nécessaire par inadvertance.

Création d’une stratégie de segmentation du centre de données

Un réseau plat et non segmenté est difficile à défendre, car une fois qu’un attaquant a réussi à accéder au réseau, il peut se déplacer latéralement et compromettre des systèmes essentiels. Cela est particulièrement vrai au sein du centre de données, où les entreprises gardent leurs ressources les plus précieuses. Les anciennes méthodes de segmentation, telles que VLAN et ACL, ne s’adaptent pas facilement, sont difficiles à automatiser et ne prennent en considération ni les comptes utilisateurs, ni les contenus, ni les applications. Elles ne fournissent ainsi que peu de prise et peu de visibilité sur le trafic.

Créez une stratégie de segmentation qui vous fournit un contrôle d’accès plus granulaire aux ressources de votre centre de données, pour une meilleure visibilité sur le trafic. Plus votre stratégie de segmentation est granulaire, plus vous gagnerez en visibilité sur le trafic, car ce dernier doit traverser un pare-feu (une passerelle de segmentation) lorsqu’il circule entre les segments. La segmentation facilite également la conformité et les audits de conformité, car vous pouvez contrôler l’accès aux données sensibles, personnelles et critiques à un niveau très granulaire et autoriser uniquement l’accès nécessaire à ces données. Cela protège les données et réduit la portée des audits.

Votre stratégie de segmentation du centre de données dépend de votre architecture et de vos objectifs commerciaux, il n’y a donc pas de mise en œuvre de type « taille unique ». Toutefois, prendre connaissance de ces principes généraux vous aidera à concevoir et à instaurer une stratégie de segmentation capable de protéger le réseau de votre centre de données et ses précieuses informations.

- Comment segmenter le centre de données ?
- Comment segmenter les applications du centre de données ?

Comment segmenter le centre de données ?

Votre façon de segmenter votre centre de données dépend de vos besoins commerciaux et de l’architecture réseau de votre centre de données, ainsi que de votre solution SDN, qui peut dicter la méthode de segmentation. Par exemple, les interfaces vwire contrôlent la connectivité du pare-feu sur un hôte NSX. Comme les interfaces vwire ne routent ou ne commutent pas le trafic sur un hôte NSX, elles doivent appartenir à la même zone, afin que les ressources d’un occupant en particulier (département, client, ou couche d’applications) fassent partie d’une zone et que le pare-feu utilise des groupes d’adresses dynamiques pour segmenter le trafic des applications au sein de cette zone. Chaque locataire dispose d’une zone distincte avec ses propres interfaces vwire. Pour d’autres solutions SDN, des occurrences de pare-feu virtuels séparés peuvent segmenter le trafic.

Les pare-feu Palo Alto Networks nouvelle génération fournissent des outils flexibles pour segmenter le trafic :

- **Zones** : le trafic franchissant des zones passe à travers le pare-feu pour être inspecté. Toute communication autorisée dans le centre de donnée doit passer à travers un pare-feu pour être soumise à une inspection complète de menaces (antivirus, anti-logiciels espion, protection contre les vulnérabilités, blocage de fichiers, analyse WildFire, et filtrage des URL concernant le trafic du centre de données quittant l’entreprise et pour les applications abritées par des occupants clients). Par défaut, le pare-feu refuse tout trafic entre zones (trafic intra-zone). Vous devez écrire des règles de politique de sécurité spécifiques pour autoriser le trafic à passer entre les zones, afin que seul le trafic explicitement autorisé puisse se déplacer d’une zone à une autre. Votre façon d’utiliser les zones pour

segmenter votre centre de données dépend des ressources dont vous avez besoin pour les séparer des autres ressources. Par exemple, une architecture commune comprend des zones distinctes pour les serveurs de développement et les serveurs de production. Vous pouvez utiliser les zones pour segmenter les serveurs abritant des informations hautement sensibles comme les informations sur les paiements par carte (PCI) ou des renseignements personnels (PII), pour segmenter différents départements internes de l'entreprise comme le Marketing, l'Ingénierie et la DRH, et pour segmenter les ressources clients et les applications hébergées chez le client.

Envisagez d'utiliser des profils de protection de zone pour protéger les zones contre les saturations, les activités de reconnaissance (analyses de ports et balayages d'hôtes), les attaques basées sur les paquets de couche 3 et les attaques basées sur les paquets non-IP (couche 2).

- **Groupes d'adresses dynamiques** : à cette fin, les groupes d'adresses dynamiques sont des listes d'adresses IP importées par le pare-feu et utilisées dans une politique de sécurité, permettant de définir les groupes serveurs de manière dynamique plutôt que statique. Ajouter ou retirer des adresses IP d'un groupe d'adresses dynamiques met à jour automatiquement la politique de sécurité, sans besoin d'action valider de la part du pare-feu. Au sein d'une zone, le fait d'utiliser des groupes d'adresses dynamiques dans des règles de politique de sécurité d'autorisation pour les applications de confiance autorise les interactions serveur à serveur pour des applications et services spécifiques. Par exemple, dans NSX, utilisez des groupes d'adresses dynamiques pour segmenter les couches serveurs au sein d'une couche d'applications.
- **User-ID** : activez User-ID pour créer des règles d'autorisation pour les applications basées sur des groupes d'utilisateurs pour segmenter les utilisateurs des groupes d'applications et des groupes serveurs.

Quand vous concevez votre plan de segmentation du centre de données, gardez à l'esprit les directives générales suivantes :

- Comment évaluer votre centre de données afin de pouvoir le segmenter par étapes et protéger en priorité les actifs les plus précieux et les plus sensibles.
- Utilisez une solution SDN (telle que NSX, ACI, OpenStack) au sein du centre de données pour fournir une infrastructure virtualisée évolutive et agile. SDN est la meilleure façon de centraliser la gestion du réseau du centre de données, d'optimiser l'exploitation des ressources de calcul, d'adapter et d'automatiser le réseau, ainsi que de contrôler et sécuriser le trafic sur un réseau virtualisé. Même si vous pouvez créer une architecture non-SDN répliquant de manière générale une architecture SDN, c'est une opération difficile, qui prend du temps, qui est source d'erreurs pouvant engendrer des pannes, et qui ne respecte pas les meilleures pratiques. Les solutions SDN optimisent l'utilisation des ressources fondamentales de calcul du centre de données, sans sacrifier à la sécurité.
- Utilisez des pare-feu matériels nouvelle génération pour segmenter et sécuriser les anciens serveurs non virtualisés et utilisez des pare-feu VM-Series pour segmenter et sécuriser le réseau du centre de données virtuel.
- Regroupez les actifs qui remplissent des fonctions similaires et nécessitent le même niveau de sécurité dans le même segment du centre de données. Par exemple, positionnez les serveurs se connectant à Internet dans le même segment.

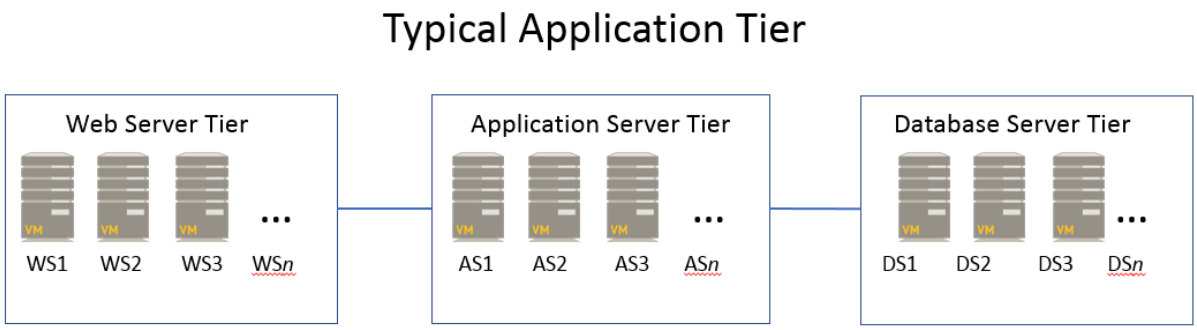
Basez votre plan de segmentation sur plusieurs critères afin de développer le plan adéquat pour sécuriser votre entreprise.

Comment segmenter les applications du centre de données ?

Segmentez les applications du centre de données pour empêcher les logiciels malveillants de se déplacer entre les applications et pour activer ces applications en toute sécurité pour les utilisateurs. *Les couches d'applications* fournissent les ressources et fonctions nécessaires aux applications du centre de données. Une couche d'applications consiste en plusieurs *couches serveurs* travaillant ensemble pour répondre aux requêtes et aux commandes relatives à une application spécifique. Généralement, une couche d'applications est composée de trois couches serveurs :

- *La couche de serveur web* : l'interface application pour les utilisateurs.
- *La couche de serveur d'applications* : accepte les requêtes de la couche de serveur web pour traiter et générer les fonctionnalités de l'application.
- *La couche de serveur de base de données* : contient les données requises par l'application pour fonctionner.

Chaque couche serveur contient des serveurs similaires fonctionnels travaillant ensemble pour qu'une couche d'applications puisse présenter une application à un utilisateur.



Les couches serveurs au sein de chaque couche d'applications créent une *chaîne de service* de VMs. Les chaînes de service guident le trafic à travers les appareils du centre de données virtuel pour fournir des services d'applications. Au sein d'une couche d'applications, un serveur web peut communiquer avec un serveur d'applications qui abrite le code de l'application, et ce serveur d'applications peut communiquer avec un serveur de base de données qui abrite du contenu. La communication entre les trois serveurs, qui demeurent sur différentes couches serveurs au sein d'une couche d'applications, est la chaîne de service.

Les centres de données contiennent plusieurs couches d'applications, et elles peuvent être dédiées à des départements, clients, sous-traitants, et autres sous-groupes spécifiques. Segmentez l'infrastructure des applications du centre de données pour empêcher des communications non autorisées et inutiles entre ressources d'applications et pour inspecter le trafic des applications.

Segmentation d'Applications	Comment segmenter les applications
Couche d'Applications	Segmentez la couche serveur au sein de chaque couche d'applications en configurant un pare-feu différent par zone et pour chaque couche serveur, afin de vous permettre de contrôler l'accès à chaque ensemble de serveurs et d'examiner le trafic circulant entre chaque couche serveur lorsqu'il traverse le pare-feu. Par exemple, positionnez les serveurs web, les serveurs d'applications et les serveurs de base de données dans des zones distinctes afin que le trafic entre couches serveurs

Segmentation d'Applications	Comment segmenter les applications
	passe tout le temps à travers un pare-feu nouvelle génération pour une inspection complète. Selon vos besoins commerciaux, il vous faudra peut-être créer plus d'une zone pour chaque couche d'applications afin de séparer les occupants, pour équilibrer les charges, pour utiliser les couches d'applications à d'autres fins, pour fournir plusieurs niveaux de sécurité ou pour connecter différents ensembles de serveurs. Segmentez le centre de données pour réduire la surface d'attaque de chaque couche d'applications en groupant dans une même zone uniquement les serveurs nécessitant les mêmes niveaux de confiance et nécessitant de communiquer avec des couches d'applications similaires.
Couche du serveur web	Le trafic pénètre habituellement dans le centre de données par des serveurs web, même s'il existe des cas spéciaux comme des accès sécurisés au centre de données configurés par le département informatique pour des besoins de gestion. Comme pour les autres couches du serveur, créez une zone distincte pour la couche du serveur web afin de pouvoir lui appliquer une politique de sécurité granulaire. Étant donné que la couche du serveur web communique avec des périphériques situés en dehors du centre de données, elle représente une cible de choix pour les attaquants. Placez la couche du serveur web sur un réseau distinct, par exemple à l'aide d'un VLAN. L'ensemble du trafic entrant et sortant du VLAN, l'ensemble du trafic entrant et sortant du centre de données, doit passer par un pare-feu nouvelle génération. Vous pouvez le faire en configurant le pare-feu nouvelle génération comme passerelle par défaut ou en utilisant une solution SDN telle que NSX pour diriger le trafic. Segmentez les serveurs au sein de la couche du serveur web pour les empêcher de communiquer entre eux, par exemple en utilisant une règle traditionnelle telle que *NSX Distributed Firewall (DFW)* pour ouvrir un port ou bloquer le trafic au sein de la couche.
Serveurs d'applications pour service d'infrastructure	Segmentez les serveurs fournissant des services d'infrastructure essentiels comme DNS, DHCP, et NTP, et autorisez l'accès uniquement à leurs adresses IP spécifiques, en utilisant uniquement les applications appropriées. *Autorisez le trafic uniquement vers les serveurs DNS approuvés. Utilisez le service de sécurité DNS pour empêcher les connexions à des serveurs DNS malveillants.*
Applications	Utilisez App-ID pour créer des règles de politique de sécurité d'autorisation pour les applications, qui segmentent les applications en contrôlant qui peut accéder à quelles applications et sur quel ensemble de serveurs (à l'aide des groupes d'adresses dynamiques). App-ID vous permet d'appliquer des règles de politique de sécurité granulaires aux applications qui peuvent se trouver sur la même ressource de calcul mais nécessitant de différents niveaux de sécurité et de contrôle d'accès. Créez des applications propres à l'entreprise pour identifier de façon unique les applications propriétaires et segmenter l'accès. Si vous avez déjà des politiques

Segmentation d’Applications	Comment segmenter les applications
	de Contrôle Prioritaire pour des Applications, créées uniquement pour définir des délais d’expiration de session personnalisés pour un ensemble de ports, convertissez ces politiques de Contrôle Prioritaire pour des Applications existantes en politiques basées sur des applications, en configurant des délais d’expiration de session basés sur le service, afin de conserver un délai d’expiration personnalisé pour chaque application et de migrer ensuite la règle vers une règle basée sur des applications. Les politiques de Contrôle Prioritaire pour des Applications sont basées sur le port. Lorsque vous utilisez des politiques de Contrôle Prioritaire pour des Applications pour conserver des délais d’expiration de session personnalisés pour un ensemble de ports, vous perdez de la visibilité sur les applications dans ces flux, et vous ne savez pas quelles applications utilisent les ports et vous ne pouvez pas non plus les contrôler. Les délais d’expiration de session basés sur le service permettent d’avoir des délais d’expiration de session personnalisés tout en conservant une visibilité sur les applications. Pour migrer d’une politique de sécurité basée sur les ports avec des délais d’expiration d’applications propres à l’entreprise à une politique basée sur les applications, n’utilisez pas de règles de contrôle prioritaire sur l’application pour maintenir les délais d’expiration personnalisés, car vous perdez de la visibilité sur les applications. À la place, définissez un délai d’expiration de session basé sur le service pour chaque application, et migrez ensuite la règle vers une règle basée sur les applications.

N’utilisez pas de pare-feu nouvelles génération pour segmenter les serveurs au sein d’une couche serveur spécifique. Lorsque vous avez besoin d’empêcher l’intercommunication des serveurs au sein d’une couche serveur, utilisez une règle classique de type NSX DFW pour ouvrir un port ou bloquer du trafic au sein de la couche. Toutefois, les serveurs au sein d’une couche serveur ont souvent besoin de communiquer. Par exemple, une couche de serveur de base de données peut être un cluster de serveurs nécessitant une intercommunication libre.

Comment créer des profils de sécurité respectant les meilleures pratiques concernant le centre de données ?

Les profils de sécurité offrent des protections fondamentales en recherchant les menaces dans le trafic que vous autorisez sur le réseau. Les profils de sécurité fournissent une suite complète d'outils coordonnées de prévention des menaces, qui bloquent le trafic d'applications pair à pair de commandement et conduite (C2), les types de fichiers à risque, les tentatives d'exploit de vulnérabilités et signatures antivirus, et ils identifient également les programmes malveillants, aussi bien nouveaux qu'inconnus.

Cela requiert relativement peu d'effort d'appliquer des profils de sécurité, car Palo Alto Networks fournit des profils prédéfinis que vous pouvez simplement ajouter aux règles d'autorisation des politiques de sécurité. Personnaliser des profils de sécurité s'avère tout aussi facile, car vous pouvez cloner un profil prédéfini et le modifier. Bien entendu, vous pouvez également créer un profil de sécurité de toutes pièces sur le pare-feu ou sur Panorama.

Pour détecter les menaces connues et inconnues dans votre trafic, associez des profils de sécurité à toutes les règles de politique de sécurité autorisant du trafic sur le réseau, pour permettre au pare-feu d'inspecter tout le trafic autorisé. Le pare-feu applique les profils de sécurité au trafic correspondant à la règle d'autorisation de la politique de sécurité, balaye le trafic conformément aux paramètres du profil de sécurité, et enfin prend les mesures appropriées pour protéger le réseau. Les recommandations pour les profils de sécurité respectant les meilleures pratiques s'appliquent à l'ensemble des quatre flux de trafic du centre de données sauf dans les cas mentionnés.

Téléchargez automatiquement les mises à jour du contenu *et installez-les dès que possible afin de disposer des signatures et du contenu de prévention des menaces les plus récents (antivirus, antispyware, vulnérabilités, logiciels malveillants, etc.) sur le pare-feu et de bloquer les dernières menaces.*

- Création du profil d'antivirus respectant les meilleures pratiques pour le centre de données
- Création du profil d'anti-logiciels espions respectant les meilleures pratiques pour le centre de données
- Création du profil de protection contre les vulnérabilités du centre de données respectant les meilleures pratiques
- Création du profil de blocage de fichiers respectant les meilleures pratiques pour le centre de données
- Création du profil d'analyse WildFire pour le centre de données respectant les meilleures pratiques

Créez un ou plusieurs groupes de profil de sécurité *afin que vous puissiez appliquer tous les profils à une règle de politique de sécurité en même temps plutôt que de les préciser individuellement.*

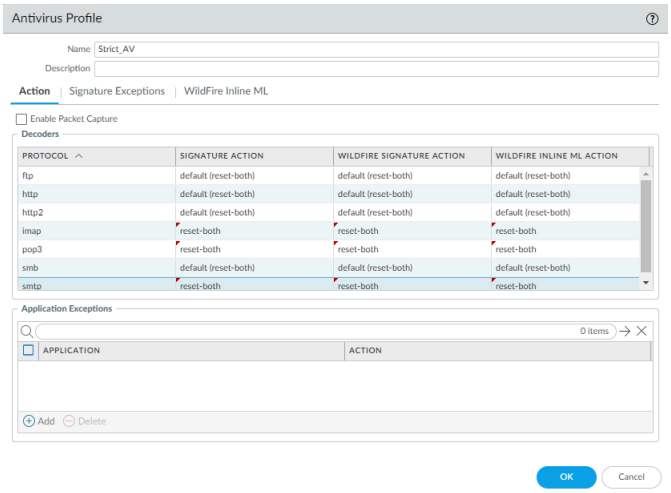
Vous n'avez pas besoin d'abonnement au Filtrage des URL en ce qui concerne les pare-feu du centre de données s'il n'y a pas de connexion sortante directe vers Internet. Les pare-feu qui ne se connectent pas directement à Internet ne nécessitent pas de solution PAN-DB de filtrage URL, car cette solution identifie les URL Internet et non les URL privées de centres de données, donc vérifier les URL en regard de la base de données PAN-DB après l'avoir importée ne s'applique pas au trafic du centre de données. Si vous ne savez pas si un pare-feu possède ou non du trafic URL, demandez un abonnement d'essai à une solution de filtrage d'URL et paramétrez le profil pour qu'il alerte sur toutes les catégories URL, afin d'identifier tout trafic URL. Par ailleurs, le filtrage des URL doit prendre place sur des pare-feu, au périmètre du réseau,

où l'utilisateur entre et quitte le réseau, et non au périmètre du centre de données. Envisagez de créer des catégories d'URL personnalisées (**Objects [Objets]** > **Custom Objects [Objets personnalisés]** > **URL Category [Catégorie URL]**) pour identifier et contrôler l'accès aux services web internes du centre de données.

Création du profil d'antivirus respectant les meilleures pratiques pour le centre de données

Clonez le Profil antivirus par défaut et modifiez-le. Pour garantir la disponibilité des applications critiques pour votre entreprise, prenez des mesures de transition sûres lorsque vous passez de votre état actuel au profil des meilleures pratiques. Pour mettre en place les meilleures pratiques, modifiez le profil par défaut comme indiqué ici et joignez-le à toutes les règles de politique de sécurité autorisant du trafic. Le profil d'antivirus possède des décodeurs de protocole lui permettant de détecter des virus et des logiciels espions et de les empêcher d'être transférés à travers sept protocoles : FTP, HTTP, HTTP2, IMAP, POP3, SMB et SMTP. Vous pouvez mettre en œuvre des actions WildFire pour l'ensemble des sept protocoles, car le profil d'antivirus exécute des actions en se basant sur les signatures WildFire et sur le machine-learning conforme.

Configurez le profil d'antivirus cloné respectant les meilleures pratiques dans le but de réinitialiser le client et le serveur pour l'ensemble des sept décodeurs de protocoles et les actions WildFire, puis appliquez ce profil aux règles d'autorisation pour l'ensemble des quatre flux de trafic du centre de données.



Des triangles rouges dans le coin supérieur gauche d'une cellule indiquent que l'action est modifiée (changée par rapport à l'action par défaut) et le nom du profil modifié est **Strict_AV**.

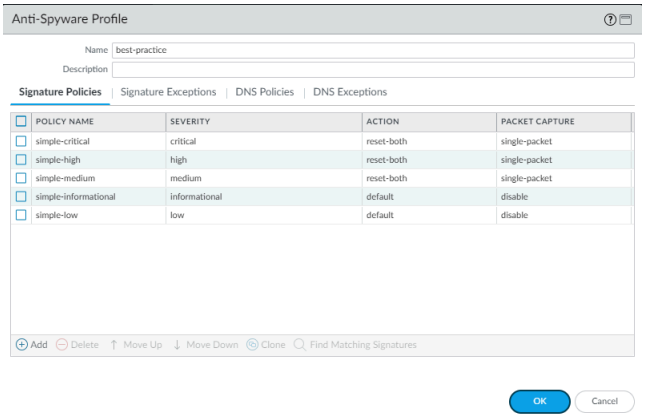
Joignez le profil d'antivirus respectant les meilleures pratiques à toutes les règles de politique de sécurité autorisant du trafic pour bloquer des fichiers malveillants connus (logiciels malveillants, DNT et virus) lorsqu'ils tentent de pénétrer le réseau. Par exemple :

- Le trafic au sein du centre de données : le profil d'Antivirus, parallèlement au profil de Protection contre les Vulnérabilités, permet d'empêcher les pirates informatiques d'utiliser des exploits pour mettre à profit des vulnérabilités et propager des logiciels malveillants et des outils de piratage informatique latéralement, parmi les serveurs du réseau du centre de données.
- Le trafic du centre de données vers Internet : le profil d'antivirus, parallèlement au profil anti-logiciels espions, permet d'identifier et de bloquer le trafic de contrôle et de commande ainsi que les premiers téléchargements de logiciels espions et d'outils de piratage informatique.

Création du profil d’anti-logiciels espions respectant les meilleures pratiques pour le centre de données

Attachez un profil Antispyware à toutes les règles de politique de sécurité qui autorisent le trafic du centre de données. Le profil Anti-Logiciels Espions détecte le trafic de type commandement et conduite (C2) enclenché par un logiciel espion installé sur un serveur ou sur un terminal, dont des catégories de type publiciel, cheval de Troie, prise de contrôle de navigateur, vol de données, enregistreur de frappe, et empêche les systèmes compromis d’établir des connexions sortantes depuis votre réseau.

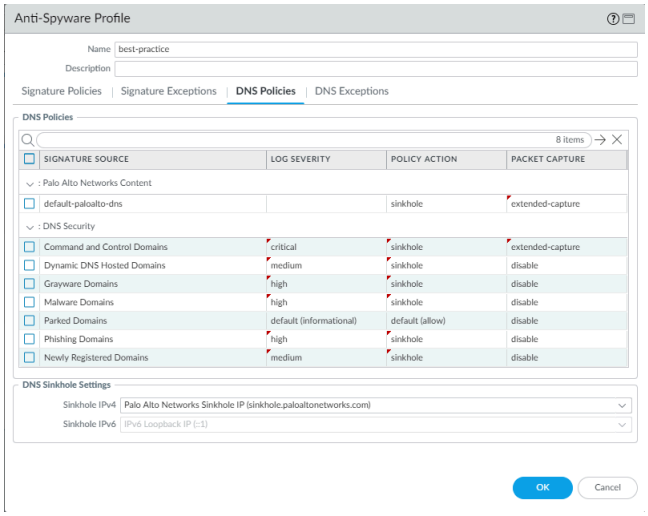
Clonez le profil Anti-Spyware strict prédéfini et modifiez-le. Pour garantir la disponibilité des applications critiques pour votre entreprise, prenez des mesures de transition sûres lorsque vous passez de votre état actuel au profil des meilleures pratiques. Si vous avez un sinkhole installé vers lequel vous pouvez rediriger du trafic pour l’analyser, activez le sinkhole DNS avec capture de paquet pour vous aider à localiser le terminal ayant essayé de résoudre le nom de domaine malveillant. Le profil Anti-Logiciels Espions respectant les meilleures pratiques conserve l’**Action** par défaut pour réinitialiser la connexion lorsque le pare-feu détecte une menace de niveau moyen, élevé ou critique, et active une capture de paquet (PCAP) unique pour ces menaces.



N’activez pas PCAP à titre informatif, car cela génère un volume relativement élevé pour ce trafic et cela n’est pas particulièrement utile, comparé à des menaces potentielles. Appliquez une PCAP étendue (en opposition à une PCAP unique) à du trafic à valeur élevée auquel vous appliquez l’Action **alert (alerter)**. Appliquez une PCAP en utilisant la même logique que vous utilisez quand vous sélectionnez le trafic à journaliser - réalisez des PCAP de trafic que vous journalisez. Appliquez une PCAP unique au trafic que vous bloquez. La quantité de paquets par défaut qu’une PCAP étendue enregistre et envoie au plan de gestion est de cinq paquets, ce qui correspond à la valeur recommandée. Dans la plupart des cas, capturer cinq paquets fournit suffisamment d’information pour analyser la menace. Si trop de trafic PCAP est envoyé au plan de gestion, alors la capture de plus de cinq paquets peut occasionner des PCAP abandonnés.

L’**Action sur Requête DNS** respectant les meilleures pratiques est de bloquer ou de rediriger les requêtes de domaines malveillants connus vers un sinkhole DNS, et lorsque vous n’avez pas de visibilité sur les requêtes DNS, d’activer PCAP.

Autorisez le trafic uniquement vers les serveurs DNS approuvés. Utilisez le service de sécurité DNS pour empêcher les connexions à des serveurs DNS malveillants.



Activer les sinkholes DNS permet d'identifier les hôtes potentiellement compromis qui tentent d'accéder à des domaines douteux en localisant les hôtes et en les empêchant d'accéder à ces domaines. Activez les sinkholes DNS lorsque le pare-feu ne peut pas voir l'initiateur de la requête DNS (ce qui est habituel quand le pare-feu se situe au nord du serveur DNS local) pour vous permettre d'identifier les hôtes infectés. N'activez pas les sinkholes DNS lorsque le pare-feu peut voir l'initiateur de la requête DNS (ce qui est habituel quand le pare-feu se situe au sud du serveur DNS local, le cas échéant les règles et journaux de blocage du pare-feu apportent de la visibilité sur le trafic) ou sur du trafic que vous pouvez bloquer.

En plus de protéger les hôtes en redirigeant des requêtes vers des sinkholes DNS, appliquez le profil Anti-Logiciels Espions respectant les meilleures pratiques à toutes les règles de politique de sécurité autorisant le trafic à identifier des hôtes infectés lorsqu'ils quittent le réseau et à arrêter des attaquants en empêchant des systèmes compromis de communiquer avec le réseau C2 malveillant. Si un système ne peut pas communiquer avec le réseau C2, celui-ci ne peut pas contrôler le système. Par exemple :

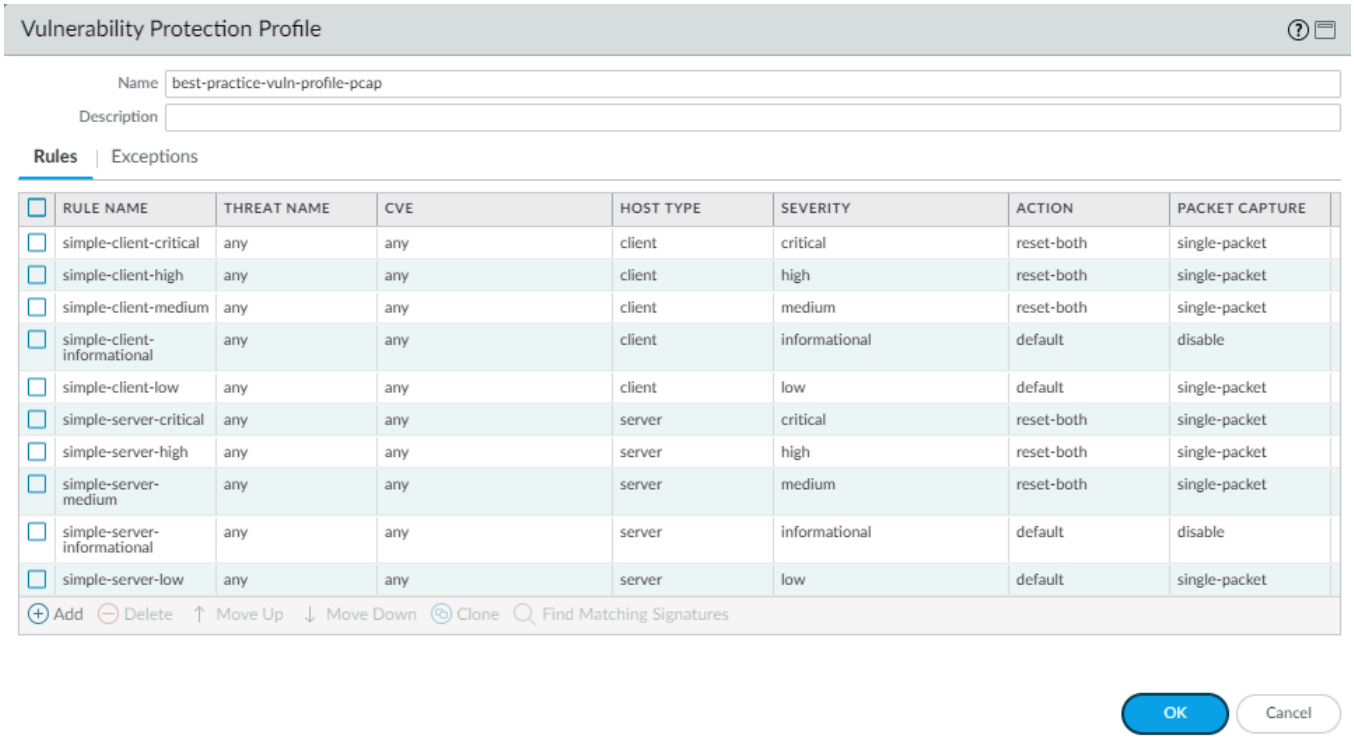
- Le trafic des utilisateurs vers le centre de données, le trafic au sein du centre de données et le trafic d'Internet vers le centre de données : le profil Anti-Logiciels Espions bloque le trafic C2 pair à pair.
- Le trafic du centre de données vers Internet : le profil Anti-Logiciels Espions, parallèlement au profil Antivirus, permet d'identifier et de bloquer le trafic C2 et les premiers téléchargements de logiciels espions et d'outils de piratage informatique.

Création du profil de protection contre les vulnérabilités du centre de données respectant les meilleures pratiques

Attachez un profil de protection contre les vulnérabilités à toutes les règles de politique de sécurité qui autorisent le trafic. Le profil de Protection contre les Vulnérabilités assure une protection contre le dépassement de capacité de la mémoire tampon, l'exécution non autorisée de code et d'autres tentatives d'exploitation des vulnérabilités côté client ou côté serveur, dans le but d'ouvrir une brèche et de se déplacer latéralement à travers le centre de données.

Clonez le profil strict prédéfini de Protection contre les Vulnérabilités. Pour garantir la disponibilité des applications critiques pour votre entreprise, prenez des mesures de transition sûres lorsque vous passez de votre état actuel au profil des meilleures pratiques. Pour le profil respectant les meilleures pratiques, pour chaque règle, hormis **simple-client-informational** et **simple-server-informational**, double-cliquez sur le **Rule Name** (Nom de la règle) et faites passer **Packet Capture** (Capture de paquets) de **disable** (désactivé) à **single-packet** (paquet unique) afin d'autoriser la capture de paquets (PCAP) pour chaque règle afin

que vous puissiez suivre la source des attaques potentielles. Ne changez pas le reste des paramètres. Téléchargez les mises à jour de contenu de manière automatique et installez-les dès que possible afin que l'ensemble des signatures soit constamment à jour.



N'activez pas PCAP à titre informatif, car cela génère un volume relativement élevé pour ce trafic et cela n'est pas particulièrement utile, comparé à des menaces potentielles. Appliquez une PCAP étendue (en opposition à une PCAP unique) à du trafic à valeur élevée auquel vous appliquez l'Action **alert (alerter)**. Appliquez une PCAP en utilisant la même logique que vous utilisez quand vous sélectionnez le trafic à journaliser - réalisez des PCAP de trafic que vous journalisez. Appliquez une PCAP unique au trafic que vous bloquez. La quantité de paquets par défaut qu'une PCAP étendue enregistre et envoie au plan de gestion est de cinq paquets, ce qui correspond à la valeur recommandée. Dans la plupart des cas, capturer cinq paquets fournit suffisamment d'information pour analyser la menace. Si trop de trafic PCAP est envoyé au plan de gestion, alors la capture de plus de cinq paquets peut occasionner des PCAP abandonnés.

Il convient d'associer ce profil de protection des vulnérabilités respectant les meilleures pratiques à toutes les règles de politique de sécurité autorisant du trafic, car sans une protection stricte contre les vulnérabilités, les pirates informatiques peuvent exploiter des vulnérabilités côté client ou côté serveur dans le but de compromettre le centre de données. Par exemple :

- Trafic au sein du centre de données : un profil strict de Protection contre les Vulnérabilités, parallèlement au profil d'Antivirus, permet d'empêcher les pirates informatiques d'utiliser des exploits pour mettre à profit des vulnérabilités et propager des logiciels malveillants et des outils de piratage informatique latéralement, entre les serveurs du réseau du centre de données.
- Trafic du centre de données vers Internet : une protection contre les vulnérabilités permet d'empêcher les serveurs du centre de données infectés de compromettre des serveurs Internet.
- Trafic d'Internet vers le centre de données : un profil strict de protection contre les vulnérabilités bloque les tentatives de compromettre les serveurs du centre de données grâce à des vulnérabilités coté serveur.

Si un serveur est compromis, la protection contre les vulnérabilités empêche les serveurs infectés d'être exploités par des clients, en isolant l'infection et en protégeant vos collaborateurs et clients d'attaques de point d'eau. La protection contre les Vulnérabilités permet également d'arrêter les attaques par force brute en utilisant l'action Blocage d'IP. Quand des signatures d'attaque par force brute déclenchent l'action, le pare-feu bloque l'adresse IP de l'assaillant pendant une période déterminée. Si l'attaque par force brute reprend après expiration de la période, les signatures déclenchent à nouveau l'action de blocage. Même si l'attaque par force brute continue, elle n'aboutit jamais.

Création du profil de blocage de fichiers respectant les meilleures pratiques pour le centre de données

Utilisez le profil de Blocage de Fichiers strict prédéfini pour bloquer les fichiers qui sont fréquemment inclus dans les campagnes d'attaques par logiciels malveillants et qui n'ont pas besoin d'être chargés ou téléchargés. En bloquant ces fichiers, vous réduisez la surface d'attaque. Le profil strict prédéfini bloque des fichiers batch, des DLLs, des fichiers de classe Java, des fichiers d'aide, des raccourcis Windows (.lnk), des fichiers BitTorrent , des fichiers .rar , des fichiers .tar, des fichiers rar cryptés et des fichiers zip cryptés, des fichiers à codage multiniveau (fichiers codés ou compressés jusqu'à quatre fois), des fichiers .hta, et des fichiers Portable Executable (PE) Windows, qui comprennent les fichiers .exe, .cpl, .dll, .ocx, .sys, .scr, .drv, .efi, .fon, et .pif. Le profil strict prédéfini envoie une alerte pour tous les autres types de fichiers afin d'obtenir une visibilité sur les autres transferts de fichiers, et afin de vous laisser décider si des modifications de politique s'imposent.

*Dans certains cas, la nécessité de supporter des applications essentielles peut vous empêcher de bloquer tous les types de fichiers du profil strict. Suivez les conseils pour une transition sécurisée pour vous aider à déterminer si vous devez faire des exceptions dans différentes zones du réseau. Analysez les journaux de filtrage des données (**Monitor [Surveillance]** > **Logs [Journaux]** > **Data Filtering [Filtrage de données]**) pour identifier les types de fichiers utilisés dans le centre de données et discutez avec les parties prenantes de l'entreprise des types de fichiers requis par leurs applications. Si nécessaire, en vous fondant sur ces renseignements, clonez le profil strict et modifiez-le, selon vos besoins, pour autoriser uniquement l(es)'autre(s) type(s) de fichier(s) requis pour supporter ces applications essentielles. Vous pouvez également utiliser les paramètres de Direction pour empêcher les types de fichiers de circuler dans les deux sens, ou pour bloquer les fichiers dans un sens et non dans l'autre.*

NAME	LOCATION	RULE NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
basic file blocking	Predefined	Block high risk file types	any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, wsf	both	block
		Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	continue
		Log all other file types	any	any	both	alert
strict file blocking	Predefined	Block all risky file types	any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
		Block encrypted files	any	encrypted-rar, encrypted-zip	both	block
		Log all other file types	any	any	both	alert

Il convient d'associer le profil de Blocage de Fichier respectant les meilleures pratiques à toutes les règles de politique de sécurité autorisant le trafic afin d'empêcher les pirates informatiques de distribuer des fichiers malveillants dans le centre de données à travers des applications de partage de fichiers et des kits

d’exploits, ou en infectant des utilisateurs ayant accès au centre de données, ou encore grâce à des clés USB.

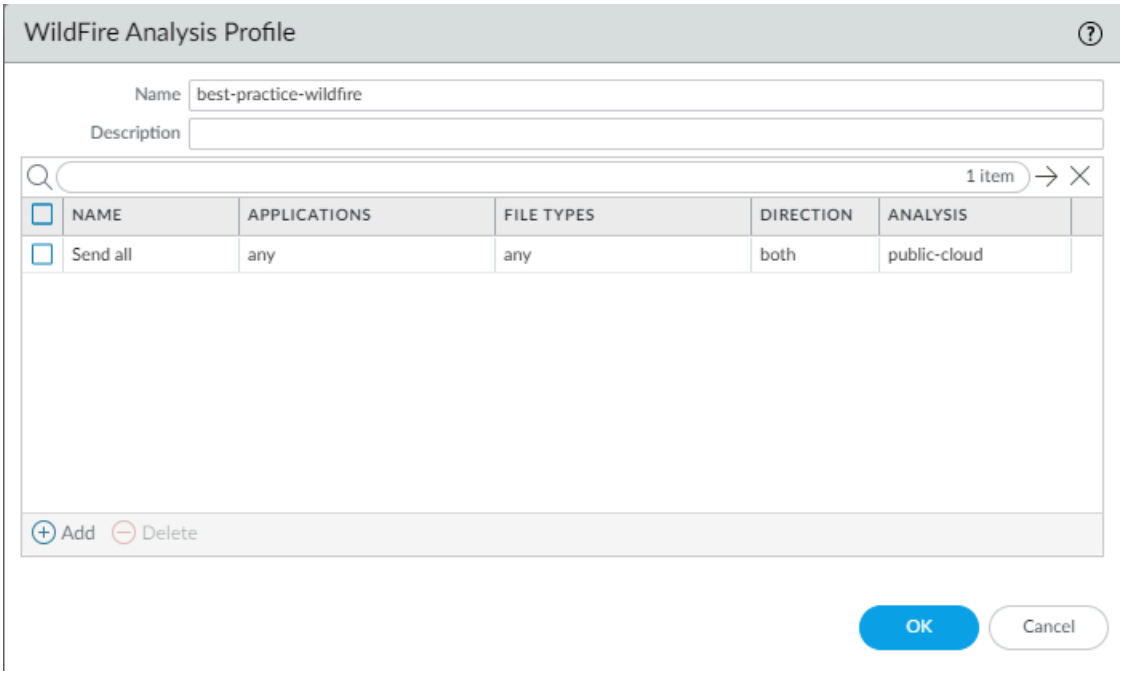
- Trafic des utilisateurs vers le centre de données : associez le profil strict de Blocage de Fichier aux règles de politique de sécurité d’applications n’impliquant pas de partage de fichiers ou de collaboration, afin de bloquer des types de fichiers dangereux risquant de distribuer des exploits ou des programmes malveillants.
- Trafic au sein du centre de données : associez le profil strict de Blocage de Fichier aux règles de politique de sécurité pour empêcher un serveur compromis de partager un logiciel malveillant avec d’autres serveurs du centre de données. Cela isole l’infection et empêche la propagation de programmes malveillants à travers le centre de données.
- Trafic du centre de données vers Internet : limitez les transferts de fichiers aux types de fichiers requis par l’application utilisée.

Si vous ne bloquez pas l’ensemble des fichiers PE Windows, envoyez tous les fichiers inconnus à WildFire pour qu’ils soient analysés. Concernant les comptes utilisateurs, définissez l’**Action** sur**continuer** pour empêcher des cas de téléchargements à la dérobée, où des sites Internet malveillants, des courriers électroniques ou encore des pop-ups peuvent entraîner des utilisateurs à télécharger des fichiers malveillants par inadvertance. Expliquez aux utilisateurs que l’apparition d’un message de réponse « Continuer » pour un transfert de fichier qu’ils n’ont pas initié peut signifier qu’ils ont été exposés à un téléchargement malveillant.

Création du profil d’analyse WildFire pour le centre de données respectant les meilleures pratiques

Les autres profils de sécurité détectent et bloquent les menaces connues. WildFire, lui, protège le centre de données de menaces *inconnues*. Configurez le pare-feu pour qu’il exécute un transfert des fichiers inconnus à WildFire pour les analyser, en utilisant un profil prédéfini par défaut. Des menaces inconnues peuvent se dissimuler dans de nombreux types de fichiers et des attaques concluantes risquent de n’être détectées que bien après avoir causé des dommages. Par exemple, WildFire peut identifier des programmes malveillants chargés sur un serveur intermédiaire avant que les pirates informatiques puissent causer des dommages, et il peut trouver des scanneurs de vulnérabilités ainsi que des outils d’assistance aux mouvements latéraux avant que les pirates informatiques n’arrivent à leurs fins. WildFire aurait pu empêcher un certain nombre de violations à grande échelle dans les entreprises ces dernières années. Toute règle de politique de sécurité contrôlant le trafic qui a eu, qui aura, ou qui pourrait avoir une activité de transfert de fichiers a intérêt à inclure un profil d’Analyse WildFire activé.

Paramétrez les mises à jour de contenu pour un appareil WildFire *pour qu’elles soient téléchargées et installées de manière automatique toutes les minutes, vous assurant ainsi le support le plus actualisé. Par exemple, les supports pour les fichiers Linux et SMB ont d’abord été distribués à travers les mises à jour de contenu pour les appareils WildFire.*



Il convient d'associer le profil d'Analyse WildFire par défaut à toutes vos règles de politique de sécurité autorisant le trafic, car WildFire fournit la meilleure défense possible contre les menaces inconnues et les menaces persistantes avancées (APT). Par exemple :

- Trafic des utilisateurs vers le centre de données : WildFire identifie les programmes malveillants hébergés sur des centres de données tels Confluence ou SharePoint.
- Trafic au sein du centre de données : WildFire identifie les programmes malveillants se propageant au sein des serveurs du centre de données, empêchant ainsi l'exfiltration de données lorsque le programme malveillant est découvert avant qu'il ne puisse causer des dommages.
- Trafic du centre de données vers Internet : étant donné que le trafic télécharge des fichiers exécutables pour des mises à jour de logiciels et de systèmes d'exploitation, il est essentiel de faire tourner WildFire sur toutes les applications pour identifier des comportements malveillants.

Configurez des alertes pour les programmes malveillants via email, SNMP, ou via un serveur syslog pour que le pare-feu puisse vous notifier immédiatement quand il rencontre un problème potentiel. Plus tôt vous isolez l'hôte compromis, plus vous baissez les probabilités de propagation du programme malveillant précédemment inconnu à d'autres appareils du centre de données, et plus il est facile d'apporter une réponse au problème.

Si nécessaire, vous pouvez restreindre les applications et les types de fichiers envoyés à des fins d'analyses en vous basant sur le sens du trafic.

*Les paramètres d'action WildFire qui sont configurés dans le profil antivirus peuvent influer sur le trafic si le trafic génère une signature WildFire qui entraîne une réinitialisation ou un abandon. Vous pouvez exclure le trafic interne comme les applications de distribution de logiciels par l'entreprise desquelles vous déployez les programmes développés sur mesure afin d'*effectuer la transition en toute sécurité *vers les pratiques exemplaires, car il se peut que WildFire identifie que les programmes sur mesure sont malveillants et génère une signature pour ceux-ci. Consultez* ***Monitor [Surveiller]*** *>* ***Logs [Journaux]*** *>* ***WildFire Submissions [Envois WildFire]*** *pour voir si des programmes sur mesure déclenchent des signatures WildFire.*

Utilisez Cortex XDR Agent pour protéger les terminaux du centre de données.

Cortex XDR Agent protège les terminaux de centre de données tels que des serveurs et des VMs contre les programmes malveillants et contre les exploits sur les terminaux eux-mêmes, tandis que le pare-feu nouvelle génération protège des menaces qui traversent le réseau (et qui doivent donc passer par le pare-feu) pour atteindre le terminal. Lorsque des programmes malveillants ou des exploits sont déjà présents sur un terminal ou atteignent un terminal, si le terminal exécute la menace (par exemple, à l'aide d'un fichier .exe ou .dll), le pare-feu ne voit pas la menace, car l'action est au niveau du terminal et aucun trafic n'a franchi le pare-feu. Pour le pare-feu, il n'y a rien à voir. En revanche, sur chaque terminal, Cortex XDR Agent voit les menaces dans les fichiers exécutables, dans les macros des documents, dans les fichiers bibliothèque de liens dynamiques (.dll), et autres. Quand ces menaces tentent de s'exécuter, Traps passe à l'action directement sur le terminal et protège le terminal.

Cortex XDR Agent et le pare-feu nouvelle génération apportent une double couche de protection aux terminaux du centre de données afin que le pare-feu protège les terminaux de menaces sur le réseau tandis que Cortex XDR Agent surveille et protège les terminaux contre les menaces résidant sur les terminaux eux-mêmes. La politique de sécurité que vous configurez pour les terminaux grâce au Gestionnaire de Sécurité du Terminal (ESM) et la politique de sécurité que vous configurez sur Panorama ou sur le pare-feu ne rentrent pas en conflit, car elles régissent différents événements à différents endroits. Cortex XDR Agent contrôle la sécurité au sein de chaque terminal individuellement. Le pare-feu contrôle la sécurité du trafic qui le traverse.

Installez Cortex XDR Agent sur chaque terminal du centre de données. Les meilleures pratiques concernant Cortex XDR Agent dans le centre de données sont les mêmes que les meilleures pratiques concernant Cortex XDR Agent sur tout terminal, car le contexte est toujours le terminal lui-même. Ainsi, le contexte « dans le centre de données » ou « dans un groupe d'utilisateurs » n'entre pas en compte : Cortex XDR Agent protège tous les terminaux de la même façon. Ainsi, le processus de déploiement, les politiques de protection contre les programmes malveillants respectant les meilleures pratiques, etc., sont les mêmes pour le centre de données que pour toute autre région du réseau.

Création des règles de blocage du trafic pour le centre de données

Avant de créer les règles d'autorisation pour les applications pour les quatre flux de trafic du centre de données, créez des règles de blocage et de journalisation pour bloquer les applications inutilisées dans le centre de données, bloquer des applications reconnues comme malveillantes, voire découvrir la présence d'applications insoupçonnées sur votre réseau. Journaliser le trafic bloqué fournit des informations sur des attaques potentielles et vous aide à enquêter sur elles.

Quand vous découvrez des applications inconnues, déterminez si elles doivent être autorisées ou si elles présentent des menaces potentielles. Si ces règles révèlent des applications qu'il convient d'autoriser, affinez les règles d'autorisation pour les applications en conséquence. Si ces règles révèlent des applications illégitimes, elles peuvent présenter des menaces potentielles et vous pouvez les examiner en utilisant les informations dans votre journal. N'appliquez pas de Profils de Sécurité à des règles de blocage car le trafic contrôlé par ces règles ne pénètre jamais dans votre réseau.

Si vous découvrez des applications inconnues qui s'avèrent être des applications propriétaires internes ou tout autre type d'applications légitimes, créez une application personnalisée pour chaque application inconnue afin de l'identifier et de lui appliquer une politique de sécurité.

La section Tri de la base de règles de la politique de sécurité du centre de données vous montre comment trier ces règles parmi toutes les autres règles créées pour les quatre flux de trafic du centre de données, afin qu'aucune règle ne fasse de l'ombre à une autre.

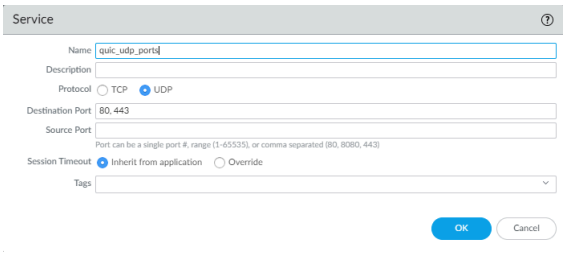
Dans le but d'appliquer une politique de sécurité cohérente sur plusieurs centres de données, vous pouvez réutiliser des modèles et des paquets de modèles, afin que les mêmes politiques s'appliquent à chaque centre de données. Les modèles utilisent des variables afin d'appliquer des valeurs spécifiques aux périphériques, telles que adresses IP, FQDN, etc., tout en maintenant une politique de sécurité globale et en réduisant la quantité de modèles et de paquets de modèles que vous devez gérer.

STEP 1 | Bloquer le protocole de connexions Internet UDP rapides (QUIC).

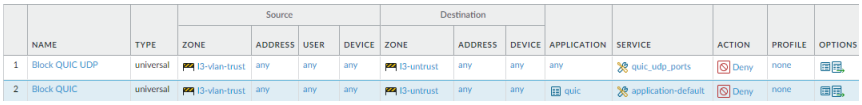
Chrome et certains autres navigateurs établissent des sessions au moyen du protocole QUIC au lieu du protocole TLS, mais QUIC utilise un cryptage propriétaire que le pare-feu ne peut déchiffrer ; le trafic potentiellement dangereux peut alors entrer sur le réseau en tant que trafic chiffré. En bloquant 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 afin que les deux premières règles de votre base de règles bloquent QUIC :



	NAME	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
1	Block QUIC UDP	universal	l3-vlan-trust	any	any	any	l3-untrust	any	any	any	quic_udp_ports	Deny	none	
2	Block QUIC	universal	l3-vlan-trust	any	any	any	l3-untrust	any	any	quic	application-default	Deny	none	

STEP 2 | Bloquez toutes les applications des zones utilisateurs sur le port par défaut de l'application afin d'identifier les applications inattendues.

Cette règle révèle les applications que les utilisateurs tentent d'utiliser à votre insu sur votre centre de données. Surveillez tout le trafic correspondant à cette règle pour déterminer s'il présente une menace potentielle ou si vous devez modifier vos règles d'autorisation pour permettre l'accès à l'application.

Assurez-vous de positionner cette règle *après* les règles d'autorisation pour les applications autorisant le trafic, à défaut de quoi cette règle bloquera le trafic que vous avez autorisé.

La règle qui suit cette règle est semblable à cette règle, à ceci près qu'elle s'applique au trafic provenant de toute source, et pas seulement au trafic provenant de zones utilisateurs. Il convient de créer des règles séparées, car des infractions à la règle des zones utilisateurs risquent d'indiquer que vous bloquez une application légitime requise par certains utilisateurs pour leurs actions professionnelles, vous pouvez donc être amené à modifier une règle d'autorisation pour les applications pour autoriser l'application pour un ensemble d'utilisateurs donné. Des infractions sur des zones non utilisateurs peuvent signifier une modification dans une application ou une attaque potentielle. Lorsque vous créez une règle séparée pour le reste du trafic, vous avez la possibilité d'afficher des journaux séparés pour le trafic utilisateur et pour tout autre trafic tentant de pénétrer votre centre de données. L'examiner et répondre à un problème potentiel s'avère plus facile.

Cette règle doit précéder la règle suivante, qui s'applique à tout trafic, afin de vous permettre de journaliser et de surveiller les tentatives d'utilisation d'applications inattendues sur des ports d'applications par défaut, quelle que soit la source, après avoir journalisé dans un premier temps des infractions aux zones utilisateurs.

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-App-from-User-Zone	User to DC BP	universal	Contractors Engineering-Users Finance-Users IT-Users	any	any	any	Web-Server-Tier-DC	any	any	any	application-default	Drop	none	

Pour appliquer cette règle :

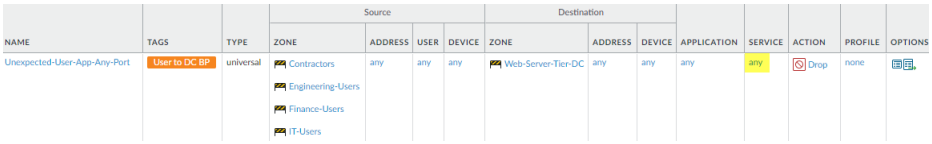
- La zone source inclut toutes les zones utilisateur et les utilisateurs (votre déploiement peut avoir plus de zones utilisateur que ce qui est indiqué dans l'exemple).
- La Zone Destination est la couche du serveur web du centre de données (**Web-Server-Tier-DC**), au périmètre du centre de données.
- Définissez l'Application sur **any (indifférent)** et le Service sur **application-default (par défaut de l'application)** afin que la règle s'applique à toutes les applications s'exécutant sur leurs ports standard.
- Définissez l'Action sur **Drop (Abandonner)** pour abandonner silencieusement le trafic sans envoyer de signal au client ou au serveur.

STEP 3 | Bloquez toutes les applications des zones utilisateurs, quel que soit le port, pour identifier les applications qui s'exécutent là où elles ne devraient pas.

Cette règle permet d'identifier des applications connues et légitimes que les utilisateurs tentent d'exécuter sur des ports non standard ainsi que des applications inconnues pour lesquelles vous devrez peut-être créer des applications personnalisées. Examinez la source de tout trafic correspondant à cette règle pour vous assurer que vous n'autorisez pas de trafic unknown-tcp, unknown-udp, ou non-syn-tcp.

Assurez-vous de positionner cette règle *après* les règles d'autorisation pour les applications autorisant le trafic, à défaut de quoi cette règle bloquera le trafic que vous avez autorisé.

*Plus tard, nous allons également créer une règle de blocage différente dans cette section, similaire à cette règle (**Unexpected-App-from-Any-Zone**), à ceci près qu'elle s'applique au trafic provenant de toute source, et pas seulement au trafic provenant de zones utilisateurs. Il convient de créer des règles séparées, car des infractions à la règle des zones utilisateurs risquent d'indiquer qu'une application légitime requise par certains utilisateurs pour leurs actions professionnelles n'a pas été conçue correctement, vous pouvez donc être amené à modifier cette application. Lorsque vous créez une règle séparée pour le reste du trafic, vous avez la possibilité d'afficher des journaux séparés pour le trafic utilisateur et pour tout autre trafic tentant de pénétrer votre centre de données. L'examiner et répondre à un problème potentiel s'avère plus facile.*



			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-User-App-Any-Port	User to DC BP	universal	Contractors Engineering-Users Finance-Users IT-Users	any	any	any	Web-Server-Tier-DC	any	any	any	any	Drop	none	

Pour appliquer cette règle :

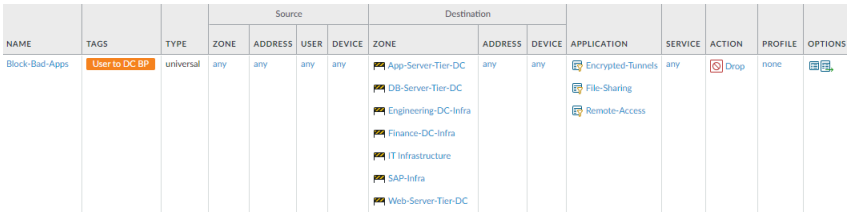
- La zone source inclut toutes les zones utilisateur et les utilisateurs (votre déploiement peut avoir plus de zones utilisateur que ce qui est indiqué dans l'exemple).
- La Zone Destination est la couche du serveur web du centre de données (**Web-Server-Tier-DC**), au périmètre du centre de données.
- Définissez l'Application sur **any (indifférent)** et le Service sur **any (indifférent)** afin que la règle s'applique à toutes les applications s'exécutant sur n'importe quel port.
- Définissez l'Action sur **Drop (Abandonner)** pour abandonner silencieusement le trafic sans envoyer de signal au client ou au serveur.

STEP 4 | Bloquez les applications conçues dans le but d'éluder ou de contourner les dispositifs de sécurité, que les pirates exploitent couramment, ou qui ne sont pas nécessaires dans le centre de données.

Cette règle protège le centre de données d'applications que vous jugez indésirables sur votre réseau. Même si l'objectif d'une politique de sécurité respectant les meilleures pratiques est une mise en place positive grâce à des règles d'autorisation pour les applications, lorsque, de manière explicite, vous bloquez et journalisez l'activité d'applications potentiellement dangereuses comme des applications non approuvées de partage de fichiers, des applications d'accès distant ou des tunnels cryptés, vous apportez de la visibilité et de l'information sur des attaques potentielles. Même après avoir constitué une liste stable d'applications de confiance, gardez cette règle de blocage d'application dans la base

de règles, car des journaux de tentatives d'infractions vous aideront dans vos enquêtes portant sur des attaques potentielles.

Utilisez cette règle pour ne bloquer que les applications que vous ne voulez en aucun cas dans votre centre de données.



NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Block-Bad-Apps	User to DC BP	universal	any	any	any	any	App-Server-Tier-DC DB-Server-Tier-DC Engineering-DC-Infra Finance-DC-Infra IT Infrastructure SAP-Infra Web-Server-Tier-DC	any	any	Encrypted-Tunnels File-Sharing Remote-Access	any	Drop	none	

Pour appliquer cette règle :

- Définissez la zone source, l'adresse et l'utilisateur sur **any (indifférent)**, car vous bloquez les applications que personne n'est autorisé à utiliser dans le centre de données.
- Définissez toutes les zones du centre de données dans la Zone de Destination pour protéger tous les serveurs du centre de données d'applications malveillantes.
- Créez un filtre d'Application pour chaque type (catégorie) d'application que vous souhaitez bloquer et spécifiez toute application supplémentaire. Cet exemple comprend des filtres d'applications pour des tunnels cryptés, des accès distants et des partages de fichiers. Bloquez les applications que vous n'utilisez pas dans le centre de données pour réduire la surface d'attaque en éliminant les applications non essentielles, ce qui réduit également le risque. L'utilisation de filtres d'applications plutôt que les groupes d'applications ou l'énumération des applications individuellement présente l'avantage de l'automatisme des mises à jour des filtres, vous évitant de les maintenir quand de nouvelles applications font leur apparition.
- Définissez le Service sur **any (indifférent)** pour saisir des applications indésirables sur des ports non standard ainsi que sur des ports par défaut.
- Définissez l'Action sur **Drop (Abandonner)** pour abandonner silencieusement le trafic sans envoyer de signal au client ou au serveur.

Les filtres d'applications montrés dans la règle d'exemple ne constituent pas une liste exhaustive. Testez la liste d'applications que vous avez créée en vous aidant de Comment Évaluer votre Centre de Données et ajoutez les applications que vous ne souhaitez pas autoriser à cette règle. Positionnez cette règle de blocage *après* les règles d'autorisation pour les applications pour permettre des exceptions à cette règle. Par exemple, le département informatique a besoin d'utiliser des applications d'accès distant pour gérer des appareils du centre de données, vous devez donc autoriser cet usage d'applications d'accès distant avant de bloquer les applications d'accès distant pour tous les autres utilisateurs. Vous pouvez également, dans un autre exemple, approuver une ou deux applications de partage de fichiers dans les règles d'autorisation pour les applications, avant l'établissement d'une règle de blocage, laissant ensuite au filtre d'applications présent dans cette règle le soin de bloquer toutes les autres applications de ce type. Si vous ne voulez en aucun cas d'un ensemble d'applications ou de certaines applications individuelles sur votre réseau, sans exception, vous pouvez établir une règle de blocage spécifique afin de bloquer uniquement ces applications et la placer en haut de la base de règles, au-dessus des règles d'autorisation pour les applications. Cependant, si vous faites cela, vous devez vous assurer qu'aucune des applications bloquées n'a d'utilisation professionnelle légitime, car vos utilisateurs ne pourront plus y accéder.

STEP 5 | Bloquez toutes les applications de n'importe quelle zone sur le port par défaut de l'application afin d'identifier les applications inattendues.

Cette règle révèle les applications de n'importe quelle zone qui s'exécutent à votre insu sur votre centre de données. Des infractions à cette règle risquent d'indiquer qu'une application a changé ou qu'une menace potentielle a été détectée. Surveillez tout le trafic correspondant à cette règle pour déterminer s'il présente une menace potentielle ou si vous devez modifier vos règles d'autorisation pour les applications afin d'autoriser l'application. Assurez-vous de positionner cette règle *après* les règles d'autorisation pour les applications autorisant le trafic ou cette règle bloquera le trafic que vous souhaitez autoriser, et après la règle de l'Étape 1, afin de ne pas saisir de trafic provenant des zones utilisateurs.

		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-App-from-Any-Zone	universal	any	any	any	any	Web-Server-Tier-DC	any	any	any	application-default	Drop	none	

Pour appliquer cette règle :

- La Source est **any (indifférente)** pour englober tout le reste du trafic qui tente de pénétrer le centre de données (la règle de l'Étape 1 bloque et identifie les applications utilisateurs inattendues avant que le trafic ne soit concerné par cette règle).
- La Zone Destination est la couche du serveur web du centre de données (**Web-Server-Tier-DC**), au périmètre du centre de données.
- Définissez l'Application sur **any (indifférent)** et le Service sur **application-default (par défaut de l'application)** afin que la règle s'applique à toutes les applications s'exécutant sur leurs ports standard.
- Définissez l'Action sur **Drop (Abandonner)** pour abandonner silencieusement le trafic sans envoyer de signal au client ou au serveur.

STEP 6 | Bloquez toutes les applications de n'importe quelle zone, quel que soit le port, pour identifier les applications qui s'exécutent là où elles ne devraient pas.

Cette règle permet d'identifier des applications connues et légitimes qui tentent de s'exécuter sur des ports non standard ainsi que des applications inconnues pour lesquelles vous devriez peut-être créer des applications personnalisées. Examinez la source de tout trafic correspondant à cette règle pour vous assurer que vous n'autorisez pas de trafic unknown-tcp, unknown-udp, ou non-syn-tcp. Assurez-vous de positionner cette règle *après* les règles d'autorisation pour les applications autorisant le trafic ou cette règle bloquera le trafic que vous souhaitez autoriser, et après la règle précédente, afin de ne pas saisir de trafic provenant des zones utilisateurs.

		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-App-Any-Port	universal	any	any	any	any	Web-Server-Tier-DC	any	any	any	any	Drop	none	

Afin de créer cette règle, utilisez les mêmes réglages que pour la règle **Unexpected-App-from-User-Zone**, à ceci près qu'au lieu de spécifier des zones utilisateurs dans la source, spécifiez **any (toute)** zone pour englober tout le reste du trafic qui tente de pénétrer le centre de données, et définissez le Service sur **any (indifférent)** pour englober tous les ports non standard.

STEP 7 | Découvrez des utilisateurs inconnus tentant d'exécuter toute application, sur tout port.

Cette règle identifie des lacunes dans la couverture de User-ID en trouvant des utilisateurs inconnus. Elle identifie également les appareils compromis ou incorporés à la communauté d'utilisateurs, qui tentent d'accéder à votre centre de données. (Les appareils incorporés n'ont pas d'interface utilisateur,

par exemple des imprimantes, des lecteurs de cartes, des appareils photo, mais des adversaires peuvent compromettre ces appareils et les utiliser dans une attaque.)

		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Discover-Unknown-Users	universal	any	any	unknown	any	any	any	any	any	any	Deny	none	

Cette règle est presque équivalente à la règle de l’interzone par défaut qui empêche les communications entre les zones (à moins qu’une autre règle autorise le trafic), à ceci près qu’au lieu d’abandonner le trafic de tous les utilisateurs, elle se contente d’abandonner le trafic d’utilisateurs inconnus. Cela vous permet d’enregistrer les correspondances de règles séparément et d’enquêter plus facilement sur les utilisateurs inconnus qui tentent d’accéder à votre centre de données.

Définition de la politique de sécurité initiale pour le trafic de l’utilisateur vers le centre de données

Définir la politique de sécurité initiale respectant les meilleures pratiques pour le trafic de l’utilisateur vers le centre de données marque le début de la mise au point d’une liste d’autorisation des applications pour le centre de données. L’objectif ultime est d’utiliser une mise en œuvre de la sécurité positive pour protéger votre centre de données avec une architecture Zero Trust. Pour ce faire, vous devez contrôler explicitement qui peut accéder au centre de données, ainsi que les applications du centre de données et les ressources qui sont accessibles. Autorisez l’accès uniquement aux utilisateurs qui ont des raisons professionnelles légitimes d’accéder au centre de données. Une fois que vous avez mis au point votre politique de sécurité respectant les meilleures pratiques, aucun utilisateur inconnu ne doit pouvoir accéder au centre de données et aucune application ou ressource inconnue ne doit être abritée dans le centre de données.

Les risques pour le centre de données liés à l’accès des utilisateurs comprennent la prise de contrôle par des attaquants d’un périphérique réseau en dehors du centre de données et son utilisation pour se déplacer latéralement dans le centre de données afin d’installer des logiciels malveillants, d’exfiltrer des données et de prendre le contrôle des périphériques du centre de données, le téléchargement accidentel de malware dans le centre de données, et l’accès non autorisé aux applications et aux ressources du centre de données.

Les sections suivantes vous montrent les types de trafic d’application à autoriser et comment les contrôler, comment authentifier les utilisateurs pour prévenir tout accès non autorisé au centre de données, et comment déchiffrer le trafic :

- Approches de la sécurité liées au trafic de l’utilisateur vers le centre de données
- Création des règles d’autorisation pour les applications concernant le trafic de l’utilisateur vers le centre de données
- Création des règles relatives à la politique d’authentification concernant l’utilisateur dans le centre de données
- Création des règles relatives à la politique de décryptage concernant l’utilisateur et le centre de données

Approches de la sécurité liées au trafic de l’utilisateur vers le centre de données

L’approche traditionnelle utilisée pour les anciens systèmes, consistant à sécuriser le trafic de l’utilisateur vers le centre de données, laisse de précieuses ressources exposées au risque, alors que l’approche respectant les meilleures pratiques protège vos ressources les plus précieuses.

L’approche traditionnelle	Risque	Approche respectant les meilleures pratiques
Les règles basées sur les ports apportent une sécurité suffisante, car le centre de données est situé	Les applications malveillantes accèdent au réseau en usurpant des numéros de port, par tunnellisation d’un port ou en utilisant le saut de port pour éviter d’être détectés.	Les règles d’autorisation pour les applications relient les applications, utilisateurs et serveurs ensemble, pour que seuls les utilisateurs légitimes utilisant des applications approuvées puissent accéder aux ensembles appropriés de serveurs du centre de données.

L’approche traditionnelle	Risque	Approche respectant les meilleures pratiques
à l’intérieur d’un réseau fiable.		*Lorsque vous passez des règles basées sur les ports aux règles basées sur les applications, dans la base des règles, positionnez la règle basée sur les applications au-dessus de la règle basée sur les ports qu’elle doit remplacer. Réinitialisez le compteur de correspondance à la règle de politique pour les deux règles. Si le trafic correspond à la règle basée sur les ports, le nombre de correspondances à la règle de politique augmente. Ajustez la règle basée sur les applications jusqu’à ce qu’aucun trafic n’atteigne la règle basée sur les ports pendant une période donnée, puis retirez la règle basée sur les ports.*
Faites confiance aux utilisateurs internes et autorisez l’application accédée par l’utilisateur à déterminer si l’accès est autorisé en se basant sur les identifiants et éventuellement sur les règles relatives aux adresses IP.	Un pirate informatique obtient l’accès au terminal d’un centre de données et se déplace ensuite latéralement à tout autre terminal du centre de données pour exploiter des identifiants volés ou des vulnérabilités côté serveur. Des utilisateurs inconnus ont accès aux terminaux du centre de données.	Activez User-ID, bloquez les utilisateurs inconnus, et autorisez l’accès aux utilisateurs approuvés. Créez des domaines d’identités séparés pour les employés, les collaborateurs et les sous-traitants. Utilisez l’authentification multifactorielle (MFA) pour les collaborateurs, les sous-traitants, et pour tout accès sensible au serveur.
Analyser les fichiers inconnus n’est pas nécessaire, car le centre de données est situé à l’intérieur d’un réseau fiable.	Les utilisateurs peuvent télécharger involontairement des logiciels malveillants à partir du partage de fichiers et d’autres applications cloud.	Transférez tous les fichiers inconnus à WildFire pour qu’ils soient analysés afin d’identifier de nouveaux programmes malveillants ou tout simplement inconnus et pour vous protéger contre eux.

L’approche traditionnelle	Risque	Approche respectant les meilleures pratiques
Un ensemble de profils de prévention des menaces de différents fournisseurs.	Un ensemble d’outils individuels laisse des failles dans votre sécurité pour les pirates informatiques et les outils risquent de ne pas bien fonctionner ensemble.	La suite d’outils de sécurité coordonnés de Palo Alto Networks fonctionne comme un tout pour boucher les trous dans votre sécurité et empêcher les attaques.

Création des règles d’autorisation pour les applications concernant le trafic de l’utilisateur vers le centre de données

Lorsque vous évaluez votre centre de données, vous accumulez assez d’informations nécessaires pour façonner un ensemble de règles d’autorisation pour les applications, en vous basant sur des choix délibérés portant sur quels accès accorder, à quelles applications, à quels ensembles de serveurs et à quelles personnes. Créez des règles d’autorisation de politique de sécurité pour les applications (**Policies [Politiques]** > **Security [Sécurité]**) pour que seuls les utilisateurs autorisés de manière expresse puissent utiliser ces applications relatives à leur activité et uniquement sur les ensembles de serveurs appropriés. N’autorisez aucun accès inutile, aucun utilisateur inconnu, et aucune application inconnue.

Marquez toutes les applications approuvées *avec le marquage prédéfini Approuvé. Panorama et les pare-feu considèrent les applications sans marquage Approuvé comme des applications non approuvées.*

La section Tri de la base des règles de la politique de sécurité du centre de données vous montre comment trier ces règles parmi toutes les autres règles créées pour les trois autres flux de trafic du centre de données ainsi que les règles de blocage, afin qu’aucune règle ne fasse de l’ombre à une autre.

Dans le but d’appliquer une politique de sécurité cohérente sur plusieurs centres de données, vous pouvez réutiliser des modèles et des paquets de modèles, afin que les mêmes politiques s’appliquent à chaque centre de données. Les modèles utilisent des variables afin d’appliquer des valeurs spécifiques aux périphériques, telles que adresses IP, FQDN, etc., tout en maintenant une politique de sécurité globale et en réduisant la quantité de modèles et de paquets de modèles que vous devez gérer.

Chacune des règles d’autorisation suivantes :

- Est jointe au groupe de profils de sécurité des meilleures pratiques, que sont les profils de sécurité des meilleures pratiques. L’utilisation d’un groupe de profils de sécurité vous permet d’appliquer tous les profils de meilleures pratiques à un règle en même temps plutôt que de préciser chaque profil individuellement. Les groupes de profils de sécurité rendent la configuration de la protection contre les logiciels malveillants, les vulnérabilités, le trafic C2, et les menaces connues et inconnues plus rapide et plus simple.
- Journalise le trafic (à la fin des sessions) afin que vous puissiez suivre et analyser les infractions de règles, et inclut le transfert des journaux. Transfère les journaux vers les serveurs de journaux et, le cas échéant, transfère les e-mails aux administrateurs appropriés.

STEP 1 | Autorisez les utilisateurs adéquats à accéder aux serveurs DNS d'entreprises internes (n'autorisez pas d'accès à des serveurs DNS externes).

Cette règle restreint l'accès à vos serveurs DNS d'entreprise, réduisant ainsi la surface d'attaque et protégeant les entrées DNS concernant les hôtes et les services. Afin d'éviter toute divulgation à travers des requêtes DNS publiques, les entrées DNS des ressources internes d'entreprises ne sont pas stockées dans des serveurs DNS accessibles par le public. Le seul moyen que possède un pirate informatique pour connaître ces entrées est de compromettre un serveur DNS d'entreprise, ce qui rend vos serveurs DNS particulièrement attractifs.

Au niveau de la passerelle Internet (le périmètre du réseau), bloquez tout trafic DNS en direction des serveurs DNS publics. N'autorisez pas de trafic DNS sortant vers Internet.

Cette règle est une exception à la meilleure pratique qui consiste à ne pas autoriser « tout » utilisateur dans les règles de politique, car les utilisateurs ont besoin d'accéder aux services DNS avant de s'identifier. Cette règle protège l'accès aux services DNS. Pour appliquer cette règle :

- Limitez l'accès à la Zone Destination pertinente dans le centre de données, **Infrastructure informatique**.
- Configurez un groupe d'adresses pour les **Serveurs DNS** et limitez cet accès à ce groupe uniquement.
- Empêchez l'accès à l'aide de n'importe quelle application sauf **DNS**.
- Il est particulièrement important d'appliquer la meilleure pratique du groupe de profils de sécurité au trafic DNS, car si un pirate informatique détourne votre serveur DNS, il peut rediriger le trafic vers des sites de hameçonnage ressemblant aux sites Internet légitimes auxquels vos utilisateurs tentent d'accéder.

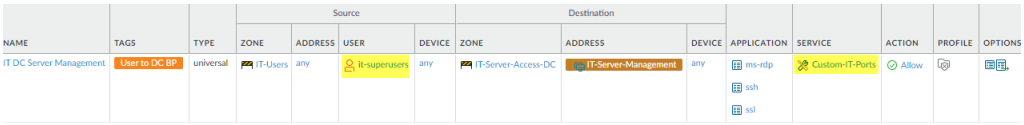
STEP 2 | Accordez au personnel informatique nécessaire un accès sécurisé et privilégié aux serveurs du centre de données pour la gestion et la maintenance.

Cette règle montre comment protéger l'accès aux systèmes essentiels aux utilisateurs ayant des comptes privilégiés. Les comptes privilégiés exigent un niveau élevé de confiance et accordent un accès administratif aux systèmes critiques qui contiennent les données les plus précieuses de votre entreprise. Vous devez donc contrôler et surveiller étroitement les comptes privilégiés. Mobilisez App-ID pour spécifier uniquement les applications dont les utilisateurs du département informatique ont besoin pour gérer les équipements du centre de données, afin que le pare-feu refuse l'accès à toutes les autres

applications. Dans cet exemple, un groupe d'utilisateurs du département informatique requiert un accès administrateur pour gérer les serveurs du centre de données.

L'accès privilégié accordé au département informatique afin de gérer les serveurs du centre de données doit être limité uniquement aux interfaces de gestion, et doit figurer sur un VLAN dédié dans le but de séparer le trafic de gestion de tout autre trafic. Les interfaces de gestion doivent être sur le même sous-réseau. N'autorisez pas ce type d'accès sur des interfaces de données. Si le groupe du département informatique utilise SSH ou RDP pour un accès de gestion, n'autorisez pas d'accès SSH ou RDP pour d'autres usages.

L'organisation de l'équipe du réseau informatique détermine à quels membres octroyer un accès privilégié. Pour chaque type d'accès privilégié, groupez les serveurs ainsi que les autres équipements par conditions d'accès. N'autorisez que les utilisateurs du département informatique nécessaire à accéder chaque ensemble de serveurs, en n'utilisant que les applications nécessaires à la gestion d'équipement.



Pour appliquer cette règle :

- Comme seul un sous-ensemble d'utilisateurs du département informatique doit gérer les serveurs du centre de données, utilisez User-ID pour créer un groupe spécifiquement pour les utilisateurs du département informatique nécessitant un accès privilégié (dans cet exemple **it-superusers**).
- Créez un groupe d'adresses statiques (**IT-Server-Management**) contenant les adresses des interfaces de gestion des serveurs que vous autorisez **it-superusers** à gérer et limitez la destination à ce groupe d'adresse dans la zone **IT-server-access-DC**.
- N'autorisez que les applications nécessaires aux super-utilisateurs-IT pour accomplir leur activité, sur leur port par défaut. Dans cet exemple, la règle autorise l'utilisation des applications **ssl**, **ssh**, et **ms-rdp**.

Ces applications autorisées servent d'exemple. Autorisez les applications utilisées par votre service informatique à gérer les serveurs du centre de données. Dans certains cas, des applications sur SSL peuvent exiger que le rajout de l'application en question soit identifié correctement par App-ID.

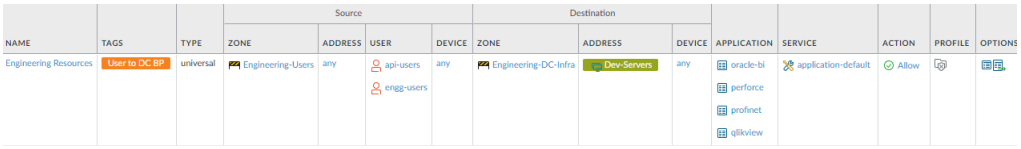
Le personnel du département informatique gère également des commutateurs, routeurs, et d'autres équipements du centre de données. Si les mêmes groupes d'utilisateurs du département informatique gèrent ces ressources à l'aide des mêmes applications, vous pouvez les ajouter à la zone et à l'adresse de destination afin que la règle autorise les super-utilisateurs-IT à accéder aux interfaces de gestion de ces équipements. Si des utilisateurs différents du département informatique gèrent différents ensembles de ressources du centre de données ou utilisent différentes applications, créez des règles de sécurité rigoureuses séparées pour chaque groupe d'utilisateur et pour chaque ensemble d'applications.

Comme les groupes d'utilisateurs bénéficiant de comptes privilégiés peuvent accéder à des systèmes essentiels, lorsque vous procédez à la Création de règles relatives à la politique d'authentification concernant l'utilisateur dans le centre de données, exigez une authentification multifactorielle (MFA)

pour interdire l'accès si des pirates informatiques compromettent leurs identifiants. Créez des règles de politique d'authentification et de politique de décryptage correspondantes pour chaque règle d'accès privilégié.

STEP 3 | Autorisez l'accès aux groupes d'utilisateurs employés ayant des raisons professionnelles légitimes de communiquer avec les serveurs du centre de données.

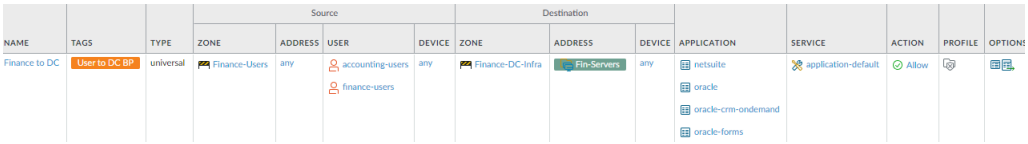
Cette règle montre comment limiter l'accès de chaque groupe d'utilisateurs (ou, dans certains cas, d'utilisateurs individuels) uniquement aux applications et serveurs nécessaires. Par exemple, les ingénieurs doivent accéder aux serveurs de développement du centre de données. Pour créer la règle de politique de sécurité, créez un groupe d'adresses dynamiques contenant les adresses IP de tous les serveurs de développement du centre de données que le groupe utilise, identifiez les applications nécessaires aux ingénieurs sur ces serveurs, et concevez les règles basées sur ces groupes.



Pour appliquer cette règle :

- Spécifiez les groupes d'utilisateurs ingénieurs ayant besoin d'un accès aux serveurs d'ingénierie du centre de données, dans cet exemple, **api-users** et **engg-users**.
- Limitez l'accès aux serveurs de développement du centre de données en leur créant un groupe d'adresses dynamiques (**Dev-Servers**) et en le définissant comme l'Adresse Destination.
- Limitez l'accès uniquement aux applications requises à des fins professionnelles, sur leur port par défaut.

Utilisez la même méthode pour créer des règles granulaires d'autorisation pour les applications pour chaque groupe d'utilisateurs (au besoin, vous pouvez également le faire pour des utilisateurs individuels), afin que chaque groupe n'utilise que des applications légitimes s'exécutant sur leur port par défaut pour n'accéder qu'aux ensembles de serveurs nécessaires à leur activité professionnelle. Par exemple, autorisez uniquement le groupe d'utilisateurs du département Finance ayant besoin d'accéder aux serveurs dédiés aux paiements par carte d'accéder à ces serveurs, en n'utilisant que les applications autorisées nécessaires à la réalisation de leurs objectifs commerciaux.



Semblable à la règle d'autorisation pour les applications pour l'accès aux serveurs du centre de données des utilisateurs de l'Ingénierie, cette règle autorise les utilisateurs des groupes **finance-users** et **accounting-users** à utiliser uniquement les applications spécifiques pour accéder uniquement aux serveurs du groupe d'adresses dynamiques **Fin-Servers**. La règle applique les profils de sécurité respectant les meilleures pratiques au trafic autorisé et journalise l'activité.

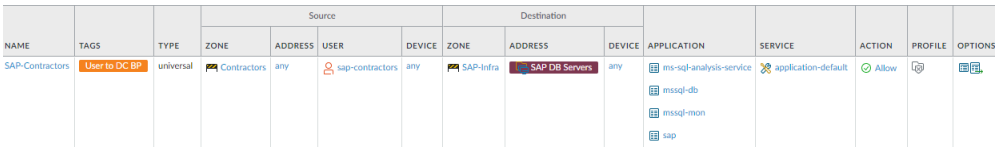
STEP 4 | Autorisez un accès ciblé et limité au centre de données aux sous-traitants, partenaires, clients et autres tiers.

Cette règle montre comment contrôler strictement l'accès aux tierces parties afin qu'elles n'utilisent que les applications requises, et uniquement sur les serveurs requis. Par exemple, une entreprise embauche un groupe de développeurs SAP sous-traitants. Les développeurs SAP ont besoin d'accéder

à la base de données SAP dans le centre de données et d'effectuer des requêtes SQL. Cependant, SQL s'exécute également sur des bases de données de production auxquelles les développeurs ne doivent pas avoir accès. L'entreprise doit contrôler trois vecteurs d'accès :

- **Groupe d'utilisateurs** : développeurs SAP sous-traitants.
- **Applications** : MS-SQL et SAP.
- **Serveurs** : serveurs de base de données SAP uniquement. Refusez l'accès à tous les autres serveurs du centre de données.

En combinant User-ID pour isoler le groupe d'utilisateurs de développeurs SAP sous-traitants, App-ID pour limiter l'utilisation des applications uniquement nécessaires au groupe, et un groupe d'adresses dynamiques limitant l'accès uniquement aux serveurs de base de données SAP du centre de données, la société réussit à fournir précisément l'accès aux sous-traitants SAP pour qu'ils puissent effectuer leurs tâches, mais pas davantage.



Pour appliquer cette règle :

- Spécifiez la zone source et l'utilisateur pour limiter l'accès aux utilisateurs dans le groupe **sap-contractors** provenant de la zone **Contractors (sous-traitants)**.
- Limitez la Destination aux serveurs de base de données SAP (groupe d'adresses dynamiques **SAP DB Server**) dans la zone **SAP-Infra**.
- Autorisez les sous-traitants SAP à utiliser uniquement les applications dont ils ont besoin pour effectuer leurs tâches professionnelles, sur les ports par défaut. Dans cet exemple, la règle autorise l'utilisation des applications **ms-sql-analysis-service**, **mssql-db**, **mssql-mon** et **sap**.

Les règles granulaires d'autorisation pour les applications empêchent tous les accès hormis celui nécessaire aux activités professionnelles et réduisent les risques en réduisant la surface d'attaque. Créez des règles semblables d'autorisation pour les applications pour chaque groupe tiers nécessitant un accès à votre centre de données.

Au lieu de compter sur les sociétés et des utilisateurs tiers pour qu'ils sécurisent leurs identifiants, exigez une authentification multifactorielle (MFA, Création de règles relatives à la politique d'authentification concernant l'utilisateur dans le centre de données), afin d'interdire l'accès si des pirates informatiques compromettent leurs identifiants. L'authentification MFA aurait pu éviter plusieurs atteintes de grande ampleur à la protection des données ces dernières années.

Vérifiez que seules les applications que vous avez explicitement autorisées dans les règles de politique de sécurité s'exécutent en affichant le rapport d'applications prédéfini (**Monitor [Surveillance]** > **Reports [Rapports]** > **Application Reports [Rapports d'application]** > **Applications**). Si vous voyez des applications non prévues dans le rapport, examinez les règles d'autorisation pour les applications et affinez-les afin qu'elles n'autorisent pas d'applications non prévues.

Création des règles relatives à la politique d’authentification concernant l’utilisateur dans le centre de données

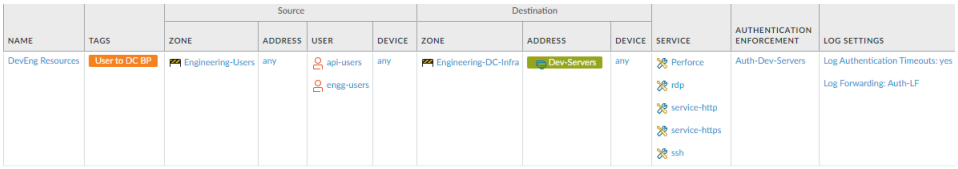
Les règles relatives à la Politique d’Authentification obligent les utilisateurs à prouver qu’ils sont bien ceux qu’ils affirment être avant de pouvoir accéder aux services, applications et autres ressources du centre de données. L’authentification est particulièrement importante pour la protection de vos ressources les plus précieuses, car si un pirate informatique vole les identifiants et s’authentifie au niveau du pare-feu, il peut réussir à accéder et à compromettre n’importe quelle ressource au sein de votre centre de données.

Pour l’accès aux serveurs sensibles et pour l’accès d’utilisateurs tiers aux serveurs (par exemple des développeurs SAP sous-traitants accédant aux serveurs SAP dans le centre de données), instaurez une authentification multifactorielle (MFA) pour empêcher les pirates informatiques d’utiliser des identifiants volés afin d’accéder à ces systèmes. Une politique d’authentification MFA aurait pu éviter plusieurs atteintes de grande ampleur à la protection des données ces dernières années.

Avant de créer des règles de politique d’authentification (**Policies [Politiques]** > **Authentication [Authentification]**), vous devez configurer les dépendances de la politique d’authentification pour relier la méthode d’authentification, le type d’authentification, la méthode d’accès au serveur d’authentification, et l’utilisation d’un portail d’authentification à une règle de politique d’authentification qui spécifiera qui peut s’authentifier, sur quels serveurs, et au moyen de quels services.

STEP 1 | Authentifiez des groupes d’utilisateurs employés et des individus ayant une raison professionnelle légitime d’utiliser les serveurs du centre de données.

Cette règle montre comment authentifier un groupe d’utilisateurs pour qu’il puisse accéder aux services nécessaires à leur activité professionnelle sur les serveurs nécessaires. Par exemple, des ingénieurs doivent s’authentifier avant de pouvoir accéder aux serveurs et aux applications de développement.



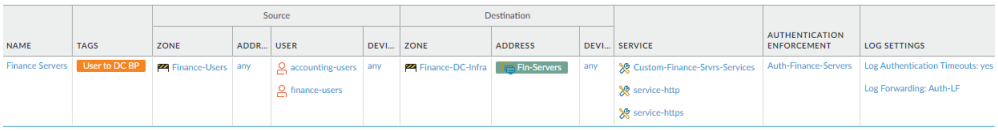
Pour appliquer cette règle :

- Spécifiez les groupes d’utilisateurs ingénieurs ayant besoin de s’authentifier avant de pouvoir accéder aux serveurs d’ingénierie du centre de données, dans cet exemple, **api-users** et **engg-users**.
- Appliquez l’authentification à ces groupes d’utilisateurs pour les requêtes d’accès aux serveurs de développement du centre de données en leur créant un groupe d’adresses dynamiques (**Dev-Servers**) et en le définissant comme l’adresse de destination.
- Appliquez la règle d’Authentification aux services que les groupes d’ingénieurs ont besoin d’utiliser pour leur activité professionnelle, dans cet exemple **Perforce**, **rdp**, **service-http**, **service-https**, et **ssh** (les développeurs peuvent avoir besoin d’utiliser SSH et RDP pour accéder à des serveurs Linux

et doivent s'authentifier avant de pouvoir être autorisés à accéder à ces serveurs). Les services inclus dans vos règles d'authentification dépendent des services que les groupes ont besoin d'utiliser.

- Configurez un Objet d'Application de l'Authentification (**Auth-Dev-Servers**) qui spécifie la méthode d'authentification et le profil d'Authentification, et rajoutez-le à la règle.
- Journalisez l'activité afin de suivre et d'analyser toute infraction à la règle, indiquant éventuellement une tentative d'agression.

Un autre cas d'utilisation est un groupe nécessitant un accès à un ensemble spécifique de services. Par exemple, les utilisateurs du Département Finance ont besoin d'accéder à des informations sur les paiements par carte (PCI) en utilisant des services spécifiques, et doivent s'authentifier avant d'obtenir l'accès. Pour authentifier des utilisateurs pour ces services, cette règle utilise un Groupe de services (**Objects [Objets]** > **Service Groups [Groupe de services]**) qui ne comprend que les services pour lesquels le pare-feu doit authentifier des utilisateurs du service des finances.



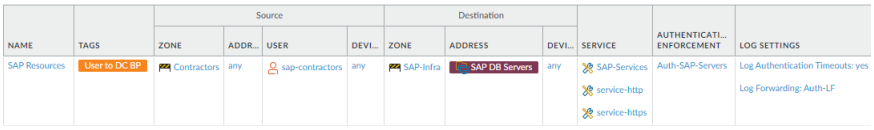
Pour appliquer cette règle :

- Spécifiez les groupes d'utilisateurs ayant besoin de s'authentifier avant de pouvoir accéder aux serveurs du département finance du centre de données, dans cet exemple, **accounting-users** et **finance-users**.
- Appliquez l'authentification à ces groupes d'utilisateurs pour les requêtes d'accès aux serveurs du département finance du centre de données en leur créant un groupe d'adresses dynamiques (**Fin-Servers**) et en le définissant comme l'adresse de destination.
- Appliquez la règle d'Authentification aux services que les utilisateurs ont besoin d'utiliser pour leur activité professionnelle, dans cet exemple **service-http**, **service-https**, ainsi que les services définis dans le groupe de services personnalisés **Custom-Finance-Srvrs-Services**, afin que les utilisateurs aient à s'authentifier avant de pouvoir accéder ces services.
- Configurez un Objet d'Application de l'Authentification (**Auth-Finance-Servers**) qui spécifie la méthode d'authentification et le profil d'Authentification, et rajoutez-le à la règle.
- Journalisez l'activité afin de suivre et d'analyser toute infraction à la règle, indiquant éventuellement une tentative d'agression.

STEP 2 | Authentifiez sous-traitants, collaborateurs, clients et autres groupes de non employés nécessitant un accès au centre de données.

Cette règle requiert une MFA pour des groupes d'utilisateurs tiers comme des sous-traitants, des collaborateurs et des clients, car vous avez moins de contrôle sur les pratiques professionnelles et les politiques de sécurité de leurs sociétés ainsi que sur leur personnel que vous n'en avez sur vos propres

employés. En exigeant de la part de ces utilisateurs une authentification à deux facteurs au moins, vous assurez la protection de votre centre de données contre le vol d'identifiants par une tierce partie.



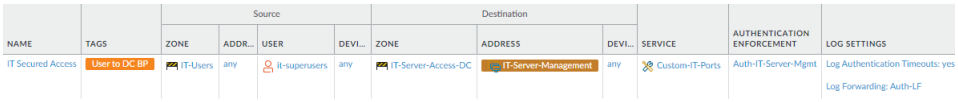
Pour appliquer cette règle :

- Appliquez la règle d'Authentification aux services que les sous-traitants SAP ont besoin d'utiliser pour leur activité professionnelle. Créez un groupe de services personnalisés (**Sap-Services**) pour définir les ports sur lesquels les sous-traitants SAP peuvent s'authentifier et rajoutez d'autres services nécessaires, dans cet exemple, **service-http** et **service-https**.
- Configurez un Objet d'Application de l'Authentification (**Auth-SAP-Servers**) qui spécifie la méthode d'authentification et le profil d'Authentification, et rajoutez-le à la règle. Dans ce cas, le type d'authentification doit prendre en charge la MFA, et vous devez **Ajouter** un profil de serveur MFA au Profil d'Authentification (onglet**Factors**) et effectuer le reste des étapes pour configurer MFA.

  Configurez MFA pour authentifier tous les utilisateurs et tous les groupes d'utilisateurs accédant à des systèmes sensibles, dans le but d'assurer une protection contre les pirates informatiques en possession d'identifiants volés.
- Journalisez l'activité afin de suivre et d'analyser toute infraction à la règle, indiquant éventuellement une tentative d'agression.

STEP 3 | Authentifiez les utilisateurs qui ont besoin d'un accès spécialisé, tels que le personnel informatique qui a besoin d'un accès sécurisé aux serveurs du centre de données pour la gestion et la maintenance.

Cette règle vous montre comment configurer l'authentification pour les utilisateurs bénéficiant de comptes privilégiés, ce qui leur accorde un accès administrateur à des systèmes critiques. Puisque compromettre les identifiants d'un utilisateur privilégié revient à remettre les clés du royaume de vos données aux pirates informatiques avec tout ce qu'il contient comme précieuses ressources, vous devez vous protéger contre le vol d'identifiants en imposant au moins deux facteurs pour l'authentification, dans le but de vous assurer que seuls les utilisateurs légitimes puissent y accéder. Cet exemple montre comment authentifier les utilisateurs informatiques appropriés pour accéder aux interfaces de gestion des serveurs du centre de données.



Pour appliquer cette règle :

- Spécifiez les comptes d'utilisateurs privilégiés ayant besoin de s'authentifier avant de pouvoir accéder aux interfaces de gestion des serveurs du centre de données, dans cet exemple, le groupe **it-superusers**.
- Appliquez l'authentification à ces groupes d'utilisateurs pour les requêtes d'accès aux interfaces de gestion des serveurs du centre de données en leur créant un groupe d'adresses dynamiques (groupe d'adresses statiques **IT-Server-Management**) et en le définissant comme l'Adresse Destination.
- Appliquez la règle d'Authentification aux services que le personnel privilégié du département informatique a besoin d'utiliser pour son activité professionnelle, dans cet exemple, le groupe de

services personnalisés **Custom-IT-Ports**, qui identifie tous les ports de gestion du serveur (qu'il convient de placer sur le même sous-réseau).

- Configurez et appliquez un Objet d'Application de l'Authentification (**Auth-IT-Server-Mgmt** dans cet exemple) qui impose la MFA à deux facteurs pour l'authentification. **Ajoutez** un profil de serveur MFA au Profil d'Authentification (onglet **Factors**) et effectuez le reste des étapes pour configurer MFA. Il est essentiel d'utiliser MFA, car vous devez être certain de l'identité de chaque utilisateur du département informatique bénéficiant d'un compte privilégié, puisqu'ils ont accès à la gestion de périphériques.

  Pour réduire encore plus les possibilités du pirate informatique de compromettre le centre de données en utilisant des identifiants volés ou en profitant d'un moment opportun où une station de travail serait sans surveillance et non verrouillée, lorsque vous configurez MFA, configurez les horodatages d'authentification pour les facteurs d'authentification. Si votre centre de données contient des ressources précieuses, il convient de hiérarchiser la sécurisation de services et d'applications.
- Journalisez l'activité afin de pouvoir suivre et analyser toutes les violations de règles.

Le personnel du département informatique gère également des commutateurs, routeurs, et d'autres équipements du centre de données. Si les mêmes groupes d'utilisateurs du département informatique gèrent ces ressources, vous pouvez les ajouter à la zone et à l'adresse de destination afin que la règle authentifie les super-utilisateurs-IT avant qu'ils puissent accéder aux interfaces de gestion de ces équipements. Si différents groupes d'utilisateurs du département informatique gèrent différents ensembles de ressources du centre de données, créez des règles de politique de sécurité rigoureuses séparées pour chaque groupe d'utilisateur ainsi que des règles de politique d'authentification et décryptage correspondants.

Ne transmettez pas d'identifiants en clair. Par exemple, si vous utilisez RADIUS, utilisez une méthode EAP prise en charge pour le transport d'identifiants de manière sécurisée au sein de TLS.

Création des règles relatives à la politique de décryptage concernant l'utilisateur et le centre de données

Créez des règles de politique de décryptage pour le trafic entrant dans le centre de données provenant d'utilisateurs, afin de fournir de la visibilité et vous permettre d'inspecter le trafic et protéger vos ressources les plus précieuses. Lorsque vous créez une règle de politique de Sécurité autorisant l'accès d'un groupe d'utilisateurs (ou d'un utilisateur en particulier) à un ensemble de serveurs du centre de données, créez également une règle de politique de décryptage pour décrypter ce trafic.

Étant donné que le centre de données héberge vos actifs les plus précieux, décryptez tout le trafic du centre de données que vous pouvez. Commencez par décrypter le trafic vers les serveurs les plus essentiels, en décryptant les catégories de trafic à haut risque, et en décryptant le trafic provenant des segments de réseau qui inspirent le moins de confiance (par exemple, donnez la priorité au décryptage du trafic provenant de parties tierces comme les collaborateurs, les clients, les sous-traitants plutôt qu'au décryptage de trafic en provenance d'un segment interne digne de confiance), et élargissez vos efforts jusqu'à avoir appliqué le décryptage au trafic en direction de toutes les ressources de votre centre de données. Décryptez autant de trafic que possible tout en conservant des performances acceptables.

Exclusion de tout trafic inapproprié du décryptage du centre de données. *Les réglementations et la conformité des informations personnelles diffèrent d'un pays à l'autre et même entre les régions d'un même pays. Les entreprises peuvent avoir des règles de conformité différentes concernant les informations personnelles. Décryptez autant de trafic que possible, mais si votre centre de données héberge des informations que les réglementations ou les règles de l'entreprise exemptent de décryptage, ne décryptez pas ce trafic.*

Dans Création des règles d'autorisation pour les applications concernant le trafic de l'utilisateur vers le centre de données, nous avons créé des règles de politique de sécurité qui autorisent un accès DNS, les utilisateurs ingénieurs à accéder aux serveurs de développement ingénieur, les développeurs SAP sous-traitants à accéder uniquement aux serveurs de développement SAP, et un ensemble d'utilisateurs spécifique du service informatique à accéder à la gestion du serveur du centre de données. Dans le cas présent, nous créons des règles de politique de décryptage(**Policies [Politiques]** > **Decryption [Décryptage]**) afin de déchiffrer le trafic autorisé par ces règles.

Les règles de politique de décryptage présentent des caractéristiques communes par rapport à ces flux de trafic :

- Lorsque vous créez une règle de politique de décryptage, l'objectif est de décrypter le trafic afin que la règle de politique de Sécurité puisse l'examiner et l'autoriser, ou le bloquer en fonction de la règle. Pour y parvenir, la règle de politique de décryptage doit utiliser la (les) même(s) zone(s) et utilisateur(s) source(s) que la règle de politique de sécurité analogue, et la même zone et adresse de destination (souvent définies par un groupe d'adresses dynamiques pour pouvoir mettre à jour le pare-feu sans opération de validation au fur et à mesure que vous ajoutez ou retirez des serveurs). Définir la même source et la même destination dans la politique de Sécurité et dans la politique de décryptage permet d'appliquer les deux politiques au même trafic.
- L'Action pour toutes ces règles est le décryptage, sauf dans le cas d'informations personnelles sensibles comme montré dans l'Étape 4.
- Pour chaque règle, configurez le décryptage de journalisation et le transfert des journaux. Journalisez autant de décryptage de trafic que les ressources de votre pare-feu le permettent.
- Les règles de décryptage utilisant l'Inspection SSL Entrante pour examiner le trafic entrant nécessitent un certificat serveur adéquat.
- Toutes ces règles de décryptage utilisent le profil de décryptage du centre de données respectant les meilleures pratiques montré dans Création des profils de décryptage du centre de données respectant les meilleures pratiques.

STEP 1 | Décryptez le trafic autorisé de groupes d'utilisateurs employés vers les serveurs du centre de données.

Cette règle montre comment décrypter le trafic d'un groupe d'utilisateurs vers les serveurs du centre de données auquel le groupe est autorisé à accéder afin de fournir de la visibilité dans le trafic. Par exemple, les règles d'autorisation pour les applications que nous avons créées comprennent une règle de politique de sécurité qui autorise les ingénieurs à accéder aux serveurs de développement dans le

centre de données. Pour protéger les serveurs de développement, décryptez le trafic entrant afin que le pare-feu puisse l'inspecter et appliquer les profils de prévention de menaces.

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Engg to Dev Servers	User to DC BP	Engineering-Users	api-users engg-users	Engineering-DC-Infra	Dev-Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

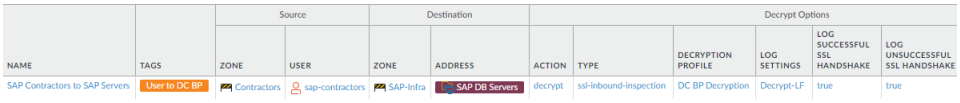
Pour appliquer cette règle :

- Définissez la même source et la même destination que dans la règle de politique de sécurité analogue. Dans ce cas, les utilisateurs Source sont les groupes d'utilisateurs **api-users** et **engg-users** dans la zone **Engineering-Users**, et la destination est les serveurs spécifiés dans le groupe d'adresses dynamiques **Dev-Servers** dans la zone **Engineering-DC-Infra**.
- Dans l'onglet Options, définissez l'Action sur **Decrypt (Décrypter)** et le Type de Décryptage sur **SSL Inbound Inspection (Inspection SSL entrante)**. Spécifiez le certificat serveur pour les serveurs de développement et appliquez le profil de décryptage du centre de données respectant les meilleures pratiques pour appliquer l'inspection SSL entrante et les paramètres du protocole SSL au trafic.

Créez une règle de politique de décryptage similaire pour le trafic autorisé du centre de données pour chaque groupe d'utilisateurs (ou utilisateur individuel, le cas échéant) basée sur la zone source et le groupe d'utilisateur (ou utilisateur) et sur la zone destination et le groupe de serveurs (comme défini dans l'adhésion au groupe d'adresses dynamiques).

STEP 2 | Décryptez le trafic autorisé provenant des sous-traitants, des partenaires, des clients et d'autres tiers.

Cette règle montre comment décrypter le trafic provenant de groupes tiers vers les serveurs du centre de données auxquels ils sont autorisés à accéder. Par exemple, les règles d'autorisation pour les applications comprennent une règle de politique de sécurité qui autorise les développeurs SAP sous-traitants à accéder aux serveurs de bases de données SAP dans le centre de données. Décryptez le trafic entrant pour permettre au pare-feu de l'inspecter, appliquez-lui les profils de prévention des menaces, et protégez les serveurs SAP dans le centre de données.



		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
SAP Contractors to SAP Servers	User to DC BP	Contractors	sap-contractors	SAP-Infra	SAP DB Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

Pour appliquer cette règle :

- Spécifiez la même source et la même destination du trafic à décrypter que dans la règle de politique de sécurité analogue. Dans ce cas, les utilisateurs Source sont les groupes d'utilisateurs **sap-contractors** dans la zone **Contractors (Sous-traitants)**, et la destination est les serveurs spécifiés dans le groupe d'adresses dynamiques **SAP DB Servers** dans la zone **SAP-Infra**.
- Dans l'onglet Options, définissez l'Action sur **Decrypt (Décrypter)** et le Type de Décryptage sur **SSL Inbound Inspection (Inspection SSL entrante)**. Spécifiez le certificat serveur pour les serveurs de développement et appliquez le profil de décryptage du centre de données respectant les meilleures pratiques pour appliquer l'inspection SSL entrante et les paramètres du protocole SSL au trafic.

Créez une règle de politique de décryptage similaire pour le trafic autorisé du centre de données pour chaque groupe tierce partie basée sur la zone source et le groupe d'utilisateur, et sur la zone destination et le groupe de serveurs (comme défini dans l'adhésion au groupe d'adresses dynamiques).

STEP 3 | Décryptez l'accès autorisé privilégié aux serveurs du centre de donnée (excepté le trafic relatif aux informations personnelles si les règlementations et vos règles de conformité vous l'interdisent).

Cette règle montre comment décrypter le trafic pour l'accès privilégié, car le but est de décrypter autant de trafic que possible pour apporter la visibilité nécessaire à la défense du centre de données, quel que soit le niveau de confiance que vous accordez aux utilisateurs. Si vous ne décryptez pas le trafic autorisé, vous ne pouvez pas appliquer de profils de prévention de menaces, et si le trafic dissimule des programmes malveillants ou d'autres menaces, vous ne serez pas en mesure de le voir. Cet exemple fait référence à la règle d'autorisation pour les applications créée précédemment autorisant un accès aux interfaces de gestion des serveurs du centre de données pour les super-utilisateurs du département informatique.

Si le groupe informatique qui gère et assure la maintenance des serveurs du centre de données utilise SSH, vous ne pouvez pas décrypter le trafic SSH. Vous pouvez configurer un proxy SSH *pour bloquer les tunnels SSH et empêcher SSH de tunneliser les applications et le contenu potentiellement malveillants. Si le groupe du département informatique utilise SSL, créez une règle de Politique de Décryptage en utilisant un Proxy de Transfert SSL plutôt qu'une Inspection SSL Entrante. Tout simplement parce que l'Inspection SSL Entrante nécessite un certificat serveur pour effectuer un décryptage. Comme le département informatique gère plusieurs serveurs du centre de données, créer des règles d'Inspection SSL Entrante pour chaque serveur s'avère onéreux et difficile à gérer. Le décryptage à l'aide d'un Proxy de Transfert SSL est plus adapté à ce cas.*

L'exemple suivant montre la règle de politique de décryptage pour le cas d'utilisation du Proxy de Transfert SSL.

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
IT DC Management	User to DC BP	IT-Users	it-superusers	IT-Server-Access-DC	IT-Server-Management	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

Pour appliquer cette règle :

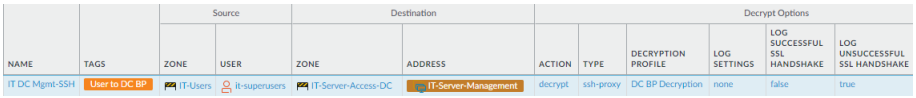
- Spécifiez la même source et la même destination du trafic à décrypter que dans la règle de politique de sécurité analogue. Dans ce cas, les utilisateurs Source sont les groupes d'utilisateurs **it-superusers** dans la zone **IT-Users**, et la destination est les serveurs spécifiés dans le groupe d'adresses statiques **IT-Server-Management** dans la zone **IT-server-access-DC**.
- Dans l'onglet Options, définissez l'Action sur **Decrypt (Décrypter)** et le type de décryptage sur **SSL Forward Proxy (Proxy de transfert SSL)**. Appliquez le profil de décryptage du centre de données respectant les meilleures pratiques pour appliquer les paramètres du proxy de transfert SSL et du protocole SSL dans le trafic.

Si d'autres groupes nécessitent un accès privilégié, créez des règles de Politique de Décryptage semblables pour chaque groupe.

Le personnel du département informatique gère également des commutateurs, routeurs, et d'autres équipements du centre de données. Si les mêmes groupes d'utilisateurs du département informatique gèrent ces ressources, vous pouvez les ajouter à la zone et à l'adresse de destination afin que la règle décrypte le trafic des connexions aux interfaces de gestion de ces équipements. Si différents groupes d'utilisateurs du département informatique gèrent différents ensembles de ressources du centre de

données, créez des règles de sécurité rigoureuses séparées pour chaque groupe d'utilisateurs ainsi que des règles de politique de décryptage et d'authentification correspondants.

L'exemple suivant montre la règle de politique de décryptage pour le cas d'utilisation du Proxy SSH. Vous pouvez également choisir de ne pas décrypter le trafic au lieu d'utiliser le décryptage via Proxy SSH.



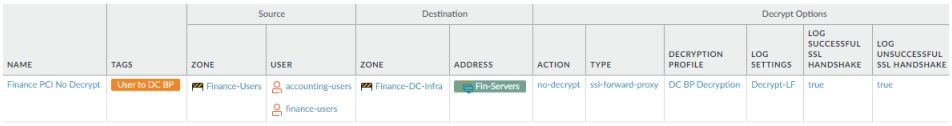
Pour appliquer cette règle :

- Le trafic source et destination sont les mêmes que pour l'exemple précédent de règle de cas d'utilisation de Proxy de Transfert SSL.
- Dans l'onglet Options, définissez l'Action sur **Decrypt (Décrypter)** et le Type de Décryptage sur **SSH Proxy (Proxy SSH)**. Appliquez le Profil de Décryptage du centre de données respectant les meilleures pratiques pour appliquer le Proxy SSH et les paramètres du protocole SSL dans le trafic.

  Le personnel du département informatique gère également les commutateurs du centre de données, les routeurs, et d'autres équipements. Si les mêmes groupes d'utilisateurs du département informatique gèrent ces ressources, vous pouvez les ajouter à la zone et à l'adresse de destination afin que la règle décrypte le trafic des connexions aux interfaces de gestion de ces équipements. Si différents groupes d'utilisateurs du département informatique gèrent différents ensembles de ressources du centre de données, créez des règles de sécurité rigoureuses séparées pour chaque groupe d'utilisateurs ainsi que des règles de politique de décryptage et d'authentification correspondants.

STEP 4 | Ne décryptez pas d'informations personnelles sensibles si les règlementations et vos règles de conformité vous l'interdisent.

Cette règle montre comment Créer une exclusion du décryptage basée sur une politique si vous avez besoin d'exclure du trafic du décryptage pour des raisons de règlementations et de règles de conformité. Cet exemple fait référence à la règle d'autorisation pour les applications créée précédemment autorisant un accès aux serveurs du département Finance pour les utilisateurs du département Finance. Si la réglementation ou la conformité vous permettent de décrypter ce trafic, décryptez-le afin que le pare-feu puisse voir le trafic et vous protéger contre les menaces.



Pour appliquer cette règle :

- Spécifiez la même source et la même destination du trafic à décrypter que dans la règle de politique de sécurité analogue. Dans ce cas, les utilisateurs source sont les groupes d'utilisateurs **accounting-users** et **finance-users** dans la zone **Finance-Users**, et la destination est les serveurs spécifiés dans le groupe d'adresses dynamiques **Fin-Servers** dans la zone **Finance-DC-Infra**.

- Dans l’onglet Options, définissez l’action sur **No Decrypt (Aucun décryptage)**. Appliquez la meilleure pratique du centre de données Profil de non-décryptage pour le protéger des problèmes de certificat.

  N’appliquez pas un profil de non-décryptage au trafic TLSV1.3, car les informations du certificat sont cryptées, afin que le pare-feu ne puisse pas bloquer les sessions basées sur les informations de certificat.

Définition de la politique de sécurité initiale du trafic d'Internet vers le centre de données

Tout comme pour les autres flux de trafic vers le centre de données, exercez un contrôle strict sur le trafic circulant d'Internet vers le centre de données avec des règles de politique de sécurité d'autorisation pour les applications, afin qu'aucun trafic utilisant des applications inconnues ou non approuvées ne pénètre dans le centre de données. En complément, protégez les serveurs web du centre de données contre des attaques par déni de service (DoS) en appliquant des règles relatives à la politique de protection DoS au trafic externe à destination de la couche serveur web du centre de données, à l'aide de profils de Protection DoS.

Les risques pour le centre de données liés au trafic Internet incluent le téléchargement de logiciels malveillants depuis un serveur externe infecté, le téléchargement d'un logiciel de commande et contrôle « call home » qui permet à un attaquant d'accéder aux actifs du centre de données et de les contrôler, et l'autorisation involontaire d'accéder au centre de données depuis Internet. Pour réduire la surface d'attaque, autorisez uniquement les applications, les utilisateurs et les services dont vous avez besoin à des fins professionnelles dans le centre de données. Décryptez, inspectez et journalisez tout le trafic autorisé par les réglementations locales, les lois et les besoins de votre entreprise. De plus, suivez les meilleures pratiques DoS et de protection de zone pour empêcher les attaquants de perturber le centre de données (en particulier les serveurs web) avec des attaques DoS.

Les sections suivantes vous montrent le type de trafic à autoriser et comment le contrôler, comment décrypter le trafic et comment protéger les actifs de votre centre de données contre les attaques DoS :

- Approches de la sécurité liée au trafic d'Internet vers le centre de données
- Création des règles d'autorisation pour les applications concernant le trafic d'Internet vers le centre de données
- Création des règles relatives à la politique de protection DoS concernant le trafic d'Internet vers le centre de données
- Création des règles de politique de décryptage du trafic d'Internet vers le centre de données

Approches de la sécurité liée au trafic d'Internet vers le centre de données

L'approche traditionnelle utilisée pour les anciens systèmes, consistant à sécuriser le trafic du centre de données circulant vers le centre de données depuis Internet, laisse de précieuses ressources exposées au risque, alors que l'approche respectant les meilleures pratiques protège vos ressources les plus précieuses. Les plus grands risques qui peuvent se rencontrer dans le trafic entrant dans le centre de données sont le téléchargement par inadvertance d'un logiciel espion depuis un serveur externe infecté ou le placement par inadvertance d'un logiciel espion provenant d'un centre de données compromis sur un serveur externe.

L'approche traditionnelle	Risque	Approche respectant les meilleures pratiques
Créez une politique de sécurité basée sur les ports.	Les applications malveillantes accèdent au réseau en usurpant des numéros de port, par tunnellisation	Les règles d'autorisation pour les applications empêchent les applications de s'exécuter sur des ports non standard.

L'approche traditionnelle	Risque	Approche respectant les meilleures pratiques
	d'un port ou en utilisant le saut de port pour éviter d'être détectés.	Enregistrez et surveillez les infractions de la liste d'autorisation. *Lorsque vous passez des règles basées sur les ports aux règles basées sur les applications, dans la base des règles, positionnez la règle basée sur les applications au-dessus de la règle basée sur les ports qu'elle doit remplacer. Réinitialisez le compteur de correspondance à la règle de politique pour les deux règles. Si le trafic correspond à la règle basée sur les ports, le nombre de correspondances à la règle de politique augmente. Ajustez la règle basée sur les applications jusqu'à ce qu'aucun trafic n'atteigne la règle basée sur les ports pendant une période donnée, puis retirez la règle basée sur les ports.*
Un système de prévention des intrusions (IPS) est souvent déployé à la place d'un système de détection des intrusions (IDS).	Un IPS est un système de détection et de prévention en bande, alors qu'un IDS est un système de détection hors bande. En déployant un IPS à la place d'un IDS, vous retirez la détection d'intrusion de la voie de communication directe entre la source et la destination, la prévention en temps réel ne peut donc pas aboutir et les menaces peuvent pénétrer dans le centre de données.	Présents sur le pare-feu, les outils App-ID, User-ID, et Content-ID de Palo Alto Networks permettent de créer des politiques de sécurité d'autorisation pour les applications qui contrôlent l'accès de manière stricte. Appliquez les profils de sécurité pour bloquer les menaces connues et nouvelles.
Un pare-feu applicatif web suffit à protéger le centre de données.	Un pirate informatique place un logiciel de commandement et conduite (C2) sur un terminal compromis du centre de données, ouvrant votre réseau à des attaques et se lançant éventuellement des	Empêchez les pirates informatiques de placer des logiciels C2 sur les terminaux du centre de données en affectant simplement le profil de sécurité strict anti-logiciels espions à la règle de politique de sécurité contrôlant le trafic. Ce profil

L'approche traditionnelle	Risque	Approche respectant les meilleures pratiques
	exploits côté client grâce à une attaque de point d'eau.	fait partie des fonctionnalités comprises dans le pare-feu, il n'y a donc aucun coût supplémentaire pour appliquer cette protection.

Création des règles d'autorisation pour les applications concernant le trafic d'Internet vers le centre de données

Les plus grands risques qui peuvent se rencontrer dans le trafic entrant dans le centre de données depuis Internet sont le téléchargement par inadvertance d'un logiciel espion depuis un client externe infecté ou le placement par inadvertance d'un logiciel espion sur un serveur externe si un client extrait des données d'un serveur compromis dans votre centre de données. Protégez le trafic depuis Internet vers le centre de données afin de ne pas télécharger par inadvertance de logiciel malveillant qui tirerait profit de vulnérabilités du serveur, ou afin de ne pas autoriser un client à télécharger un logiciel malveillant d'un des serveurs de votre société, qui pourrait infecter des collaborateurs, des clients ou encore finir sur un site Internet utilisé par votre secteur d'activité (pour y réaliser une attaque de point d'eau).

Assurez-vous que la source du trafic entrant dans le centre de données ne provient pas d'adresses IP malveillantes ou d'autres sources potentiellement à risque, et autorisez uniquement les applications nécessaires à votre activité professionnelle. N'autorisez pas d'applications inutiles (à plus forte raison inconnues) dans le centre de données. Comment procéder :

- Créez des règles d'autorisation pour les applications qui contrôlent les applications approuvées et autorisées que les appareils externes peuvent utiliser pour communiquer avec votre centre de données.

  Marquez toutes les applications approuvées *avec le marquage prédéfini Approuvé. Panorama et les pare-feu considèrent les applications sans marquage Approuvé comme des applications non approuvées.*

- Créez une liste dynamique externe pour identifier les adresses IP malveillantes et utilisez-la pour les empêcher d'accéder à votre centre de données.
- Créez une application personnalisée pour toute application propriétaire afin d'identifier l'application et lui appliquer des mesures de sécurité.

  Si vous avez déjà des politiques de Contrôle Prioritaire pour des Applications, créées uniquement pour définir des délais d'expiration de session personnalisés pour un ensemble de ports, convertissez ces politiques de Contrôle Prioritaire pour des Applications existantes en politiques basées sur des applications, en configurant des délais d'expiration de session basés sur le service, afin de conserver un délai d'expiration personnalisé pour chaque application et de migrer ensuite la règle vers une règle basée sur des applications. Les politiques de Contrôle Prioritaire pour des Applications sont basées sur le port. Lorsque vous utilisez des politiques de Contrôle Prioritaire pour des Applications pour conserver des délais d'expiration de session personnalisés pour un ensemble de ports, vous perdez de la visibilité sur les applications dans ces flux, et vous ne savez pas quelles applications utilisent les ports et vous ne pouvez pas non plus les contrôler. Les délais d'expiration de session basés sur le service permettent d'avoir des délais d'expiration de session personnalisés tout en conservant une visibilité sur les applications.

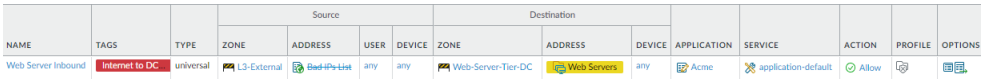
- Appliquez le groupe de profils de sécurité des meilleures pratiques qui signifie que les profils de sécurité des meilleures pratiques autorisent les règles à protéger contre les logiciels malveillants, les vulnérabilités, le trafic C2 et les menaces connues et inconnues.
- Journalisez tout le trafic autorisé à la fin de la session pour suivre et analyser les infractions. Transfère les journaux vers les serveurs de journaux et, le cas échéant, transfère les e-mails aux administrateurs appropriés.

La section Tri de la base des règles de la politique de sécurité du centre de données vous montre comment trier ces règles parmi toutes les autres règles créées pour les trois autres flux de trafic du centre de données ainsi que les règles de blocage, afin qu'aucune règle ne fasse de l'ombre à une autre.

Dans le but d'appliquer une politique de sécurité cohérente sur plusieurs centres de données, vous pouvez réutiliser des modèles et des paquets de modèles, afin que les mêmes politiques s'appliquent à chaque centre de données. Les modèles utilisent des variables afin d'appliquer des valeurs spécifiques aux périphériques, telles que adresses IP, FQDN, etc., tout en maintenant une politique de sécurité globale et en réduisant la quantité de modèles et de paquets de modèles que vous devez gérer.

Autorisez le trafic d'applications approuvées provenant de fournisseurs, sous-traitants et clients, en les limitant aux seules applications nécessaires.

Cette règle montre comment sécuriser le trafic d'application entrant dans le centre de données depuis des sources externes, en contrôlant de manière stricte les applications autorisées, en les autorisant uniquement sur leur port défaut, en bloquant les sources que vous avez définies comme malveillantes, et en utilisant une Liste Dynamique Externe pour identifier les adresses IP malveillantes.



Pour appliquer cette règle :

- Empêchez les sources malveillantes connues de tenter d'accéder au centre de données. Utilisez l'option **Negate (Refuser)** dans la **Source Address (Adresse Source)** de la règle de Politique de Sécurité pour bloquer les connexions provenant d'adresses IP malveillantes. Cet exemple utilise une Liste Dynamique Externe (**Bad IPs List)**) pour identifier les adresses IP malveillantes connues et les bloquer. (Le texte barré dans l'adresse source indique qu'elle est refusée au lieu d'être autorisée.)
- Limitez l'(les) application(s) à la (aux) seule(s) application(s) nécessaire(s) à votre activité professionnelle et autorisez-les à s'exécuter uniquement sur leur port par défaut (**application-default**), afin d'empêcher les logiciels malveillants utilisant des techniques d'évasion de s'exécuter sur des ports non standard. Dans cet exemple, le fournisseur utilise une application propriétaire nommée **Acme**. Nous avons créé une application personnalisée pour identifier l'application propriétaire **Acme** afin que le pare-feu puisse classer le trafic et appliquer la politique de Sécurité adéquate.
- Limitez la destination du trafic de l'application **Acme** au groupe d'adresse dynamique **Web-Servers** dans la zone **Web-Server-Tier-DC**. Si l'adresse de destination ne se trouve pas dans la couche du serveur web, le pare-feu abandonne le trafic.

Vérifiez que seules les applications que vous avez autorisées dans les règles de politique de sécurité s'exécutent en affichant le rapport d'applications prédéfini (**Monitor [Surveillance]** > **Reports [Rapports]** > **Application Reports [Rapports d'Application]** > **Applications**). Si vous voyez des

applications non prévues dans le rapport, examinez les règles d'autorisation pour les applications et affinez-les afin qu'elles n'autorisent pas d'applications non prévues.

Création des règles de politique de décryptage du trafic d'Internet vers le centre de données

Créez des règles de politique de décryptage pour vous fournir de la visibilité sur le trafic entrant dans le centre de données en provenance d'Internet, afin d'appliquer une politique de Sécurité à ce trafic. Lorsque vous créez une règle de politique de Sécurité autorisant l'accès à un ensemble de serveurs du centre de données, créez également une règle de politique de décryptage pour décrypter ce trafic. Dans Création des règles d'autorisation pour les applications concernant le trafic d'Internet vers le centre de données, nous avons créé une règle de politique de sécurité qui permet l'accès aux couches du serveur web depuis Internet dans le centre de données, en utilisant seulement les applications autorisées. Dans ce cas, nous créons une règle de politique de décryptage (**Policies** > **Decryption**) afin de décrypter le trafic autorisé par cette règle.

Pour décrypter le trafic, et permettre ainsi à la règle de politique de Sécurité de l'examiner afin de l'autoriser ou de le bloquer en fonction de la politique, la règle de politique de décryptage doit utiliser la (les) même(s) zone(s) et utilisateur(s) source(s) que la règle de politique de sécurité analogue, et la même zone et adresse de destination (souvent définies par un groupe d'adresses dynamiques pour pouvoir mettre à jour le pare-feu sans opération de validation au fur et à mesure que vous ajoutez ou retirez des serveurs). Définir la même source et la même destination dans la politique de Sécurité et dans la politique de décryptage permet d'appliquer les deux politiques au même trafic.

Cette règle de décryptage utilise le profil de décryptage du centre de données respectant les meilleures pratiques montré dans Création des profils de décryptage du centre de données respectant les meilleures pratiques.

Pour chaque règle, configurez le décryptage de journalisation et le transfert des journaux. Journalisez autant de décryptage de trafic que les ressources de votre pare-feu le permettent.

STEP 1 | Décryptez le trafic autorisé en provenance d'Internet vers les serveurs web du centre de données.

Cette règle montre comment décrypter le trafic enclenché par des connexions externes vers le centre de données. Par exemple, les règles d'autorisation pour les applications que nous avons créées autorisent l'accès aux serveurs web du centre de données par le trafic externe uniquement à travers certaines applications. Pour protéger les serveurs web du centre de données, décryptez le trafic afin que le pare-feu puisse l'inspecter et appliquer les profils de prévention de menaces.

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Internet to DC	Internet to DC BP	L3-External	any	Web-Server-Tier-DC	Web Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

Pour appliquer cette règle :

- Définissez la même source et la même destination que dans la règle de politique de sécurité analogue. Dans ce cas, la Source est la zone **L3-External**, et la Destination les serveurs spécifiés dans le groupe d'adresses dynamiques **Web-Servers** dans la zone **Web-Server-Tier-DC**.
- Dans l'onglet Options, définissez l'Action sur **Decrypt (Décrypter)** et le Type de Décryptage sur **SSL Inbound Inspection (Inspection SSL entrante)**. Spécifiez le certificat serveur pour les serveurs web et appliquez le profil de décryptage du centre de données respectant les meilleures pratiques pour appliquer l'inspection SSL entrante et les paramètres du protocole SSL au trafic.

STEP 2 | Créez des règles de politique de décryptage similaires pour le trafic en provenance d'Internet et en direction de tout autre groupe de serveur, si un tel accès est autorisé, ainsi que pour les autres applications que vous autorisez.

Création des règles relatives à la politique de protection DoS concernant le trafic d'Internet vers le centre de données

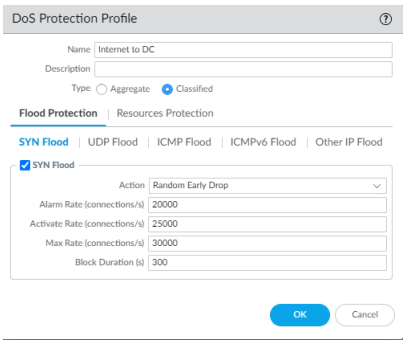
Une méthode utilisée par les pirates informatiques pour déstabiliser un réseau est l'attaque par Denial-of-Service (déni de service - DoS), destinée à saturer les systèmes ciblés connectés à Internet, les neutraliser et les rendre indisponibles à tous vos utilisateurs et services légitimes. Les serveurs web de centres de données sont des cibles tentantes, car les neutraliser empêche la plupart des accès au centre de données.

Protégez la couche du serveur web du centre de données en appliquant une Politique de Protection DoS classée au trafic allant d'Internet à destination de ces serveurs. Une politique de Protection DoS classée applique un Profil de Protection DoS qui contrôle la quantité de connexions entrantes dans le trafic défini par la politique.

En complément, configurez la protection du tampon du paquet pour chaque zone afin de protéger le pare-feu d'attaques DoS sur une session unique pouvant saturer le tampon du paquet du pare-feu et causer des chutes de trafic légitime, particulièrement sur des pare-feu protégeant des services essentiels.

STEP 1 | Créez un profil de Protection DoS classé qui protège les serveurs web du centre de données d'attaques DoS en limitant la quantité de connexions par seconde, afin d'empêcher une attaque SYN flood.

Ce profil de Protection DoS limite la quantité de connexions par seconde (CPS) pour le trafic défini dans les règles de politique de Protection DoS auxquelles le profil est lié, afin d'empêcher une attaque DoS de neutraliser vos serveurs web. Le profil définit des seuils CPS progressifs pour vous alerter, activer le Random Early Drop (Abandon anticipé aléatoire) et bloquer les nouvelles connexions, ainsi que la durée pendant laquelle elles sont bloquées. Les seuils CPS que vous configurez pour protéger les serveurs web de votre centre de données dépendent de la capacité de vos serveurs web.



Pour créer ce profil :

- Dans **Objects (Objets)** > **Security Profiles (Profils de Sécurité)** > **DoS Protection (Protection DoS)**, cliquez sur **Add (Ajouter)** un profil de protection DoS classé.
- **Nommez** ce profil, sélectionnez**Classified (Classé)** pour le **Type** de profil, fixez les valeurs CPS pour vous alerter (**Alarm Rate** [Taux d'alarme]), activez RED (**Activate Rate** [Activer le taux]), lancez le blocage de nouvelles sessions (**Max Rate** [Taux maximal]), et fixez la durée en secondes

pour bloquer ces nouvelles sessions (**Block Duration** [Durée de blocage]) quand le taux CPS atteint le seuil **Max Rate** (Taux maximal).

Si vous n'utilisez pas de protocoles comme UDP ou d'autres protocoles IP, limitez-les en utilisant une combinaison de règles de politique de sécurité pour autoriser des applications ainsi que des profils de protection de zone, afin de bloquer les protocoles inutilisés en fixant la protection CPS contre les saturations à zéro paquet pour les protocoles que vous souhaitez bloquer.

STEP 2 | Créez une règle de politique de Protection DoS pour définir les serveurs que vous souhaitez protéger d'une attaque DoS et attribuez le profil de Protection DoS à cette règle.

Cette règle empêche une attaque SYN flood d'arrêter la couche du serveur web de votre centre de données. Cet exemple applique le profil de protection DoS classifié au trafic externe autorisé à se connecter à la couche du serveur web.

		Source			Destination				Protection		
NAME	TAGS	ZONE/INTERFACE	ADDRESS	USER	ZONE/INTERFACE	ADDRESS	SERVICE	ACTION	AGGREGATE	CLASSIFIED	LOG FORWARDING
DC Web Server Protection	Internet to DC BP	L3-External	~~Bad IPs List~~	any	Web-Server-Tier-DC	Web Servers	service-http service-https	protect	none	profile: Internet to DC destination-ip-only	DoS-LF

Pour appliquer cette règle :

- Pour appliquer une protection DoS au trafic destiné à la couche du serveur web, la politique de Protection DoS doit s'appliquer au même trafic que la règle de Politique de Sécurité qui autorise le trafic. Dans cet exemple, cette règle DoS protège le trafic que nous avions autorisé dans Création des règles d'autorisation pour les applications concernant le trafic d'Internet vers le centre de données.
- Dans l'onglet Option/Protection, spécifiez les services web (**service-http** et **service-https**), définissez l'action sur **protect (protéger)** pour appliquer les seuils SYN flood du profil de protection DoS au trafic, fixez la méthode de transfert de journaux (en partant du principe que vous avez procédé à la configuration du transfert de journal), et sélectionnez le profil de protection DoS classé que nous avons configuré pour le trafic à l'étape précédente (**Internet to DC** [Internet vers centre de données]).

Pour vous protéger d'attaques SYN flood provenant de sources internes, créez une règle de politique de Protection DoS séparée, qui spécifie vos zones internes comme des zones sources au lieu de **L3-External**. En créant des règles séparées pour des sources d'attaques externes et internes, vous obtenez des rapports distincts qui rendent vos enquêtes sur des tentatives d'attaques plus aisées.

Définition de la politique de sécurité initiale du trafic du centre de données vers Internet

Selon l'architecture de votre centre de données, les serveurs au sein du centre de données peuvent faire appel à Internet pour récupérer des mises à jour logicielles ou pour vérifier auprès d'un serveur le statut d'un certificat de révocation. Le centre de données est la cachette idéale pour vos adversaires, car les stratégies de sécurité se concentrent souvent sur la communication entre utilisateurs et ignorent les serveurs qui communiquent avec Internet. Quand des serveurs de centre de données engagent la communication directement avec Internet, vous devez assurer une protection contre plusieurs risques de sécurité :

- **Exfiltration de données** : les pirates informatiques utilisent des applications légitimes comme FTP ou HTTP, ainsi que d'autres méthodes comme les tunnels DNS, pour voler des données. Créez un liste de règle de politique de sécurité d'autorisation pour les applications qui autorise uniquement les applications nécessaires aux mises à jour de serveur afin que toutes les autres applications soient bloquées, même si ce sont des applications légitimes en d'autres circonstances. Des règles d'applications trop souples offrent des opportunités aux pirates informatiques.
- **Commandement et conduite (C2) à l'aide d'applications légitimes** : si les serveurs du centre de données sont autorisés à communiquer avec Internet au moyen d'applications légitimes non destinées à des mises à jour logicielles, les pirates informatiques peuvent utiliser ces applications par ailleurs légitimes pour des activités de C2. Par exemple, autoriser la navigation web sur des ports non standard crée des opportunités pour les attaquants. Les serveurs ne doivent communiquer avec Internet qu'en utilisant des applications spécifiques requises pour les mises à jour logicielles, sur leur port par défaut, et aucune autre application, même si ces autres applications sont légitimes et validées pour d'autres utilisations.
- **Téléchargement de programmes malveillants additionnels** : si un pirate informatique compromet un serveur de centre de données, le programme malveillant présent sur le serveur peut télécharger d'autres programmes malveillants depuis Internet en « téléphonant à la maison » ou à l'aide d'autres procédés. Une règle stricte d'autorisation autorisant uniquement des communications avec les serveurs appropriés de mises à jour et utilisant uniquement les applications nécessaires aux mises à jour empêche des pirates informatiques de contacter des sites web abritant des programmes malveillants et d'exfiltrer des données. En complément, installez Cortex XDR Agent sur les serveurs du centre de données (et sur tous vos terminaux) pour empêcher les programmes malveillants déjà présents sur un serveur de s'exécuter.

- Approches de la sécurité liée au trafic du centre de données vers Internet
- Création des règles d'autorisation pour les applications concernant le trafic du centre de données vers Internet
- Création des règles relatives à la politique de décryptage concernant le trafic du centre de données vers Internet

Approches de la sécurité liée au trafic du centre de données vers Internet

L'approche traditionnelle utilisée pour les anciens systèmes, consistant à sécuriser le trafic du centre de données circulant vers Internet, laisse de précieuses ressources exposées au risque, alors que l'approche respectant les meilleures pratiques protège vos ressources les plus précieuses.

L’approche traditionnelle	Risque	Approche respectant les meilleures pratiques
Créez des règles basées sur le port ou des règles basées sur l’IP, qui fournissent un niveau de sécurité suffisant dans un réseau de confiance.	Les règles basées sur le port et celles basées sur l’IP ne peuvent pas contrôler quelles applications sont autorisées à se connecter à Internet. Si un port est ouvert, n’importe quelle application peut l’utiliser.	Créez des règles strictes d’autorisation pour les applications qui autorisent uniquement les serveurs du centre de données récupérant des mises à jour à utiliser uniquement des applications légitimes pour communiquer uniquement avec des serveurs légitimes de mises à jour. Enregistrez et surveillez les infractions des règles d’autorisation.  *Quand vous effectuez la transition de règles basées sur le port à des règles basées sur les applications, dans la base des règles, positionnez la règle basée sur l’application au-dessus de la règle basée sur le port qu’elle doit remplacer. Réinitialisez le* compteur de correspondance à la règle de politique *pour les deux règles. Si le trafic correspond à la règle basée sur les ports, le nombre de correspondances à la règle de politique augmente. Ajustez la règle basée sur l’application jusqu’à ce qu’aucun trafic n’atteigne la règle basée sur le port pendant une certaine période, puis retirez la règle basée sur le port.*
Les serveurs de centre de données ne font appel qu’à des serveurs dignes de confiance comme des serveurs de mises à jour, il n’est donc pas nécessaire de décrypter ce trafic.	Un programme malveillant ou un logiciel de commandement et conduite déjà présent sur le centre de données peut tenter de communiquer avec des serveurs externes pour télécharger encore plus de programmes malveillants afin d’exfiltrer des données.	Décryptez tout trafic allant du centre de données vers Internet. Créez une catégorie d’URL personnalisées définissant les URL que les serveurs de centre de données sont autorisés à contacter, et utilisez-la dans la politique de sécurité pour limiter l’accès à Internet pour les serveurs externes. Utilisez la même URL personnalisée dans la politique de décryptage pour décrypter le trafic vers ces serveurs externes.
Mélangez les profils de prévention des	Un mélange d’outils individuels laisse des trous dans votre sécurité pour	La suite d’outils de sécurité coordonnés de Palo Alto Networks fonctionne comme un tout

L’approche traditionnelle	Risque	Approche respectant les meilleures pratiques
menaces par blocage et alerte de plusieurs fournisseurs.	les pirates informatiques et risquent de ne pas bien fonctionner ensemble.	pour boucher les trous dans votre sécurité et empêcher les attaques.

Création des règles d’autorisation pour les applications concernant le trafic du centre de données vers Internet

Les serveurs du centre de données se connectent principalement à des serveurs sur Internet pour la mise à jour de logiciels ou l’obtention du statut d’un certificat. Le plus grand risque est de se connecter au mauvais serveur, notamment dans le cas de mises à jour Linux, où l’abondance d’URL de parties tierces est telle qu’il est facile de s’y connecter par mégarde. Assurez-vous que les serveurs de votre centre de données reçoivent des mises à jour de la part de serveurs de mises à jour légitimes, en utilisant les applications requises uniquement sur leurs ports par défaut.

Pour y parvenir, créez des règles strictes d’autorisation pour les applications, qui limitent les serveurs externes auxquels les serveurs du centre de données se connectent et les applications que les serveurs du centre de données utilisent lorsqu’ils se connectent à des serveurs externes. Marquez toutes les applications approuvées avec le marquage prédéfini *Approuvé*. (Panorama et les pare-feu considèrent les applications sans marquage Approuvé comme des applications non approuvées.) Un ensemble de règles strictes d’autorisation pour les applications contre les attaques potentielles :

- En empêchant un logiciel espion déjà présent sur le serveur du centre de données de se connecter à un serveur externe compromis (*communiquer à l’extérieur*) et de télécharger des données supplémentaires, car les règles d’autorisation pour les applications n’autorisent pas les connexions à ces serveurs.
- En empêchant les pirates informatiques d’utiliser des applications légitimes comme les tunnels FTP, HTTP ou DNS pour exfiltrer des données, ou d’utiliser des applications légitimes comme des navigateurs web ou des ports non standard pour des opérations de commandement et conduite (C2), car les règles d’autorisation pour les applications n’autorisent pas les serveurs du centre de données à communiquer avec Internet en utilisant ces applications. Un moyen supplémentaire pour empêcher une exfiltration est d’utiliser le contrôle de **Direction** du profil de Blocage de Fichiers pour bloquer les fichiers de mises à jour sortants, afin de n’autoriser que le téléchargement des mises à jour logicielles.

Créez une stricte règle d’autorisation pour les applications pour chaque application nécessitant des mises à jour logicielles provenant d’un ensemble varié de serveurs externes. Dans de nombreux cas, App-ID ne suffit pas à protéger les serveurs du centre de données. Par exemple, pour des mises à jour de serveur Linux, il ne suffit pas de limiter le trafic à une application de mise à jour de type *yum* ou *apt-get*, car cela n’empêche pas les connexions à des serveurs illégitimes. La meilleure pratique consiste à identifier les URL auxquelles les serveurs du centre de données doivent se connecter, de créer des catégories d’URL personnalisées (**Objects [Objets]** > **Custom Objects [Objets personnalisés]** > **URL Category [Catégorie d’URL]**) qui définissent les sites Internet à utiliser, et de les associer à App-ID dans vos règles de politique de sécurité. L’association d’App-ID et de catégories d’URL personnalisées verrouille les serveurs externes auxquels les serveurs du centre de données peuvent se connecter en empêchant l’utilisation d’applications illégitimes et en empêchant les connexions à des serveurs de mises à jour qui ne figurent pas dans la catégorie d’URL personnalisée. Par exemple, dans le cadre d’une règle de politique de Sécurité autorisant les serveurs du centre de données à se connecter aux serveurs de mise à jour de CentOS,

vous pouvez créer une catégorie d'URL personnalisée nommée *CentOS-Update-Servers* et ajouter à cette catégorie personnalisée les sites de mises à jour de CentOS que votre serveur utilise.

Pour trouver les URL des serveurs légitimes de mises à jour Linux et d'autres serveurs de mises à jour, collaborez avec les départements Ingénierie, Développement et autres groupes ayant recours à des mises à jour logicielles, afin de connaître les endroits où ils se procurent leurs mises à jour. Vous pouvez également journaliser des sessions de navigation Internet, rassembler les URL auxquelles se connecte le Développement, et porter ces URL à l'Ingénierie pour filtrer les bonnes URL et les incorporer à votre politique de Sécurité.

N'utilisez pas le Profil de Filtrage d'URL (PAN-DB URL Filtering) dans les règles de politique de Sécurité pour des serveurs de centre de données qui ne communiquent pas avec Internet, car il n'est pas recommandé d'autoriser l'ensemble des serveurs de mises à jour. Réduisez les communications afin que les serveurs du centre de données ne fassent appel qu'aux serveurs où ils récupèrent des mises à jour.

De plus, toutes les communications autorisées doivent utiliser les ports standard propres à chaque application. Aucune application ne doit utiliser de port non standard. Comme avec tout trafic de centre de données, surveillez les infractions aux règles d'autorisation, car elles indiquent soit que vous devez actualiser la politique de sécurité pour autoriser du trafic légitime, soit qu'un agresseur a pénétré ou tente de pénétrer le réseau.

La section Tri de la base des règles de la politique de sécurité du centre de données vous montre comment trier ces règles parmi toutes les autres règles créées pour les trois autres flux de trafic du centre de données ainsi que les règles de blocage, afin qu'aucune règle ne fasse de l'ombre à une autre.

Dans le but d'appliquer une politique de sécurité cohérente sur plusieurs centres de données, vous pouvez réutiliser des modèles et des paquets de modèles, afin que les mêmes politiques s'appliquent à chaque centre de données. Les modèles utilisent des variables afin d'appliquer des valeurs spécifiques aux périphériques, telles que adresses IP, FQDN, etc., tout en maintenant une politique de sécurité globale et en réduisant la quantité de modèles et de paquets de modèles que vous devez gérer.

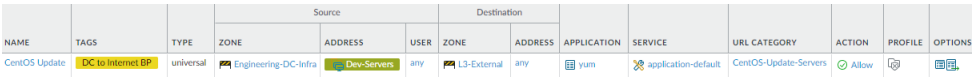
Chacune des règles d'autorisation suivantes :

- Est jointe au groupe de profils de sécurité des meilleures pratiques, que sont les profils de sécurité des meilleures pratiques. L'utilisation d'un groupe de profils de sécurité vous permet d'appliquer tous les profils de meilleures pratiques à un règle en même temps plutôt que de préciser chaque profil individuellement. Les groupes de profils de sécurité rendent la configuration de la protection contre les logiciels malveillants, les vulnérabilités, le trafic C2, et les menaces connues et inconnues plus rapide et plus simple.
- Journalise le trafic (à la fin des sessions) afin que vous puissiez suivre et analyser les infractions de règles, et inclut le transfert des journaux. Transfère les journaux vers les serveurs de journaux et, le cas échéant, transfère les e-mails aux administrateurs appropriés.

STEP 1 | Autorisez les serveurs du centre de données à accéder aux serveurs de mises à jour logicielles.

Cette règle montre comment restreindre l'accès aux serveurs de mises à jour logicielles sur le net afin que les serveurs du centre de données ne communiquent qu'avec des serveurs connus et légitimes, et qu'ils ne communiquent pas avec d'autres serveurs de mises à jour externes. Cet exemple autorise les serveurs du centre de données du département ingénierie informatique à accéder aux serveurs de mises

à jour de CentOS et restreint les communications en n'autorisant que les applications nécessaires à établir des connexions vers un unique groupe approuvé de serveurs de mises à jour.



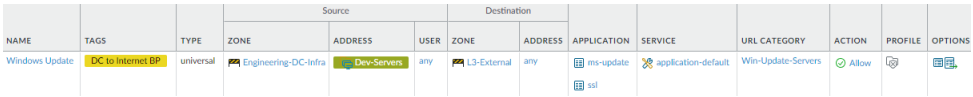
NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	ZONE	ADDRESS						
CentOS Update	DC to Internet BP	universal	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	yum	application-default	CentOS-Update-Servers	Allow		

Pour appliquer cette règle :

- Limitez la source de requêtes de mises à jour CentOS aux seuls serveurs du centre de données ayant besoin de récupérer des mises à jour, dans cet exemple le groupe d'adresses dynamiques **Dev-Servers** dans la zone **Engineering-DC-Infra**.
- Limitez l' (les) application(s) que les serveurs du centre de données peuvent utiliser pour communiquer avec des serveurs externes de mises à jour à la (aux) seule(s) application(s) nécessaire(s), dans cet exemple, **yum** pour des mises à jour CentOS. Autorisez uniquement l' (les) application(s) à s'exécuter sur son (leur) port par défaut, pour empêcher les logiciels malveillants utilisant des techniques d'évasion de tenter de passer par des ports non standard.
- Créez une catégorie d'URL personnalisée pour définir les URL des serveurs de mises à jour auxquelles les serveurs du centre de données peuvent se connecter. Dans cet exemple, la catégorie d'URL personnalisée **CentOS-Update-Servers** définit les URL du serveur de mises à jour auxquelles les serveurs du centre de données peuvent accéder.

Cette association de restrictions permet également d'empêcher les pirates informatiques ayant déjà compromis un serveur du centre de données d'atteindre d'autres destinations et d'utiliser d'autres applications pour exfiltrer des données ou pour télécharger des logiciels malveillants supplémentaires.

De la même façon, une règle autorisant les mêmes serveurs à communiquer avec les serveurs de mises à jour de Microsoft Windows utilise une construction identique.



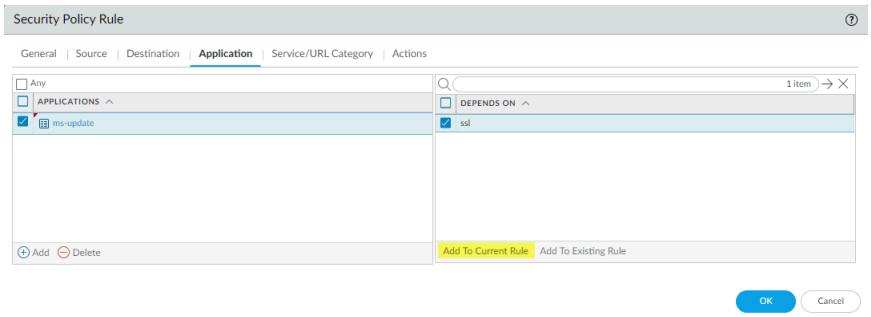
NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	ZONE	ADDRESS						
Windows Update	DC to Internet BP	universal	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	ms-update ssl	application-default	Win-Update-Servers	Allow		

La zone et l'adresse sources sont identiques à celles de la règle de mise à jour CentOS précédente. Voici les différences :

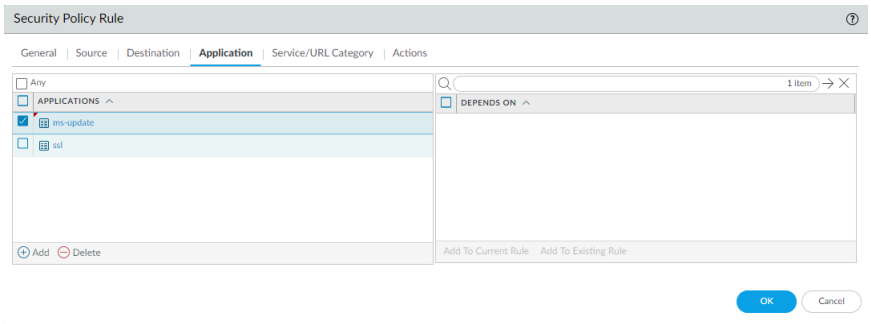
- La catégorie d'URL personnalisée (**Win-Update-Servers**) contient l'URL des mises à jour Windows, interdisant ainsi le contact avec d'autres URL.
- Les applications se rapportent aux mises à jour Microsoft. En plus de l'application **ms-update**, les mises à jour Microsoft nécessitent l'application **ssl**, car ms-update utilise le protocole SSL. Comme pour la règle concernant les mises à jour CentOS, seuls les ports standard sont valides.

  Certaines applications dépendent d'autres applications. Pour une application donnée, les applications dépendantes doivent être autorisées ou l'application ne peut pas fonctionner. L'interface utilisateur montre les dépendances d'application lorsque vous créez une règle de

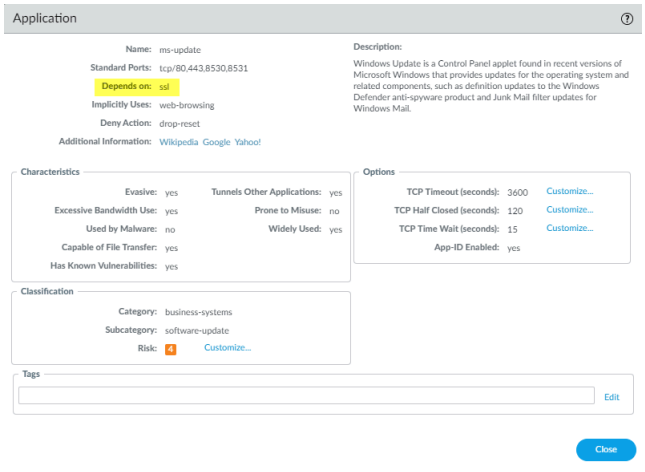
politique de sécurité. Par exemple, lorsque vous précisez l'application ms-update dans la règle, l'interface indique que ms-update dépend également de l'autorisation du SSL :



Cliquez sur **Add to Current Rule** (Ajouter à la règle actuelle) pour ajouter la/les applications(s) sélectionnée(s) à la règle.



*Vous pouvez également utiliser la fonction Search (Rechercher) (**Objects** > **Applications**) pour trouver les dépendances d'application. Par exemple, pour trouver les dépendances pour l'application ms-update, recherchez **ms-update**, cliquez sur l'application **ms-update** dans la liste des résultats d'application puis vérifiez le champ **Depends on:** (Dépend de :).*



STEP 2 | Autorisez les serveurs du centre de données à accéder aux serveurs de mises à jour DNS et NTP.

Cette règle montre comment restreindre l'accès aux serveurs de mises à jour DNS et NTP sur le net afin que les serveurs du centre de données ne communiquent qu'avec des serveurs connus et légitimes. Cet exemple autorise les serveurs du centre de données du département informatique à accéder aux serveurs de mises à jour DNS et NTP et restreint les communications en n'autorisant que les applications nécessaires à établir des connexions vers un unique groupe approuvé de serveurs de mises à jour.

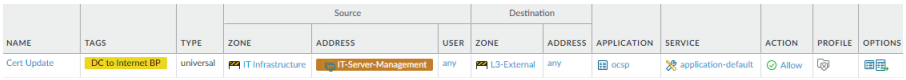
Autorisez le trafic uniquement vers les serveurs DNS approuvés. Utilisez le service de sécurité DNS pour empêcher les connexions à des serveurs DNS malveillants.

Pour appliquer cette règle :

- Limitez la source de requêtes de mises à jour DNS et NTP aux seuls serveurs du centre de données ayant besoin de récupérer des mises à jour, dans cet exemple le groupe d'adresses dynamiques **DNS-NTP-Servers** dans la zone **Engineering-DC-Infra**.
- Limitez les applications que les serveurs du centre de données peuvent utiliser pour communiquer avec des serveurs externes de mises à jour aux seules applications nécessaires, dans cet exemple, **dns** et **ntp**. Autorisez les applications à s'exécuter sur leur port par défaut, pour empêcher les logiciels malveillants utilisant des techniques d'évasion de tenter de passer par des ports non standard.
- Créez une catégorie d'URL personnalisée pour définir les URL des serveurs de mises à jour auxquelles les serveurs du centre de données peuvent se connecter. Dans cet exemple, la catégorie d'URL personnalisée **NTP-DNS-Update-Servers** définit les URL du serveur de mises à jour auxquelles les serveurs du centre de données peuvent accéder.

STEP 3 | Autorisez les serveurs du centre de données à accéder à des serveurs de l'autorité de certification pour obtenir l'état de révocation de certificats numériques et garantir leur validité.

Cette règle permet aux serveurs du centre de données de se connecter à un répondeur (serveur) Online Certificate Status Protocol (OCSP) sur le net pour vérifier l'état de révocation de certificats d'authentification. Un répondeur OCSP fournit le statut de certificat le plus récent, contrairement aux mises à jour web des listes de révocations de certificats (CRL), qui dépendent de la fréquence des mises à jour web des CRL pour être à jour des révocations de certificats. Les CRL ont davantage tendance à être obsolètes qu'un répondeur OCSP. Quand vous configurez un profil de certificat dans le pare-feu, vous pouvez mettre en place une vérification de statut CRL comme méthode de repli à l'OCSP au cas où le répondeur OCSP ne serait pas joignable.



Pour appliquer cette règle :

- Limitez la source de requêtes de vérification de révocation de certificat aux seuls serveurs du centre de données ayant besoin de vérifier la validité des certificats, dans cet exemple le groupe d'adresses dynamiques **IT-Server-Management** dans la zone **IT-Infrastructure**.
- Limitez les applications que les serveurs du centre de données peuvent utiliser pour communiquer avec des serveurs externes de révocation de certificats aux seules applications nécessaires. Cet

exemple sécurise la connexion entre les serveurs du centre de données et les répondeurs OCSP, donc la seule application à définir est **ocsp**. Autorisez l'application à s'exécuter sur son port par défaut, pour empêcher les logiciels malveillants utilisant des techniques d'évasion de tenter de passer par des ports non standard.

Vérifiez que seules les applications que vous avez explicitement autorisées dans les règles de politique de sécurité s'exécutent en affichant le rapport d'applications prédéfini (**Monitor [Surveillance]** > **Reports [Rapports]** > **Application Reports [Rapports d'application]** > **Applications**). Si vous voyez des applications non prévues dans le rapport, examinez les règles d'autorisation pour les applications et affinez-les afin qu'elles n'autorisent pas d'applications non prévues.

Création des règles relatives à la politique de décryptage concernant le trafic du centre de données vers Internet

Créez des règles de politique de décryptage pour apporter de la visibilité dans le trafic allant des serveurs du centre de données vers Internet. Décryptez tout trafic allant des serveurs du centre de données vers Internet. Les seuls comptes à l'origine de connexions à Internet depuis l'intérieur du centre de données sont des comptes de service et la majorité du trafic concerne des mises à jour logicielles, donc aucune question relative à la protection de la vie privée n'est à prendre en compte. Il est primordial de décrypter et d'inspecter le trafic, car si un serveur de mises à jour est compromis, les serveurs du centre de données risquent de télécharger un logiciel malveillant et de le propager à travers le processus de mise à jour logicielle. En inspectant le trafic et en appliquant des profils de prévention de menaces respectant les meilleures pratiques, vous protégez votre centre de données contre les logiciels malveillants qui pourraient être téléchargés depuis un serveur de mises à jour légitime, à l'aide d'une application légitime.

Dans Création des règles d'autorisation pour les applications concernant le trafic du centre de données vers Internet, nous avons créé des règles de politique de Sécurité autorisant les serveurs du centre de données à démarrer des connexions vers des serveurs de mise à jour sur Internet pour mettre à jour le système d'exploitation, DNS, NTP, et pour vérifier des certificats. Ici, nous créons des règles de politique de décryptage analogues, pour décrypter le trafic autorisé par la politique de Sécurité des mises à jour.

Ne décryptez pas le trafic allant vers des serveurs de révocation de certificat (répondeurs en ligne). Le trafic Online Certificate Status Protocol (OCSP) utilise habituellement le protocole HTTP, il circule donc en clair et n'est pas crypté. De plus, le décryptage du Proxy de Transfert SSL risque d'interrompre le processus de mise à jour, car le pare-feu agit en tant que proxy intermédiaire et remplace le certificat client avec un certificat proxy, que le répondeur OCSP risque de ne pas valider.

Les règles de politique de décryptage présentent des caractéristiques communes par rapport à ces flux de trafic :

- Lorsque vous créez une règle de politique de décryptage, l'objectif est de décrypter le trafic afin que la règle de politique de Sécurité puisse l'examiner et l'autoriser, ou le bloquer en fonction de la règle. Pour y parvenir, la règle de politique de décryptage doit utiliser la (les) même(s) zone(s) et utilisateur(s) source(s) que la règle de politique de sécurité analogue, et la même zone et adresse de destination (souvent définies par un groupe d'adresses dynamiques pour pouvoir mettre à jour le pare-feu sans opération de validation au fur et à mesure que vous ajoutez ou retirez des serveurs). Définir la même source et la même destination dans la politique de Sécurité et dans la politique de décryptage permet d'appliquer les deux politiques au même trafic.
- L'Action pour toutes ces règles est le décryptage.

- Pour chaque règle, configurez le décryptage de journalisation et le transfert des journaux. Journalisez autant de décryptage de trafic que les ressources de votre pare-feu le permettent.
- Toutes ces règles de décryptage utilisent le profil de décryptage du centre de données respectant les meilleures pratiques montré dans Création des profils de décryptage du centre de données respectant les meilleures pratiques.

Dans beaucoup de cas, les exemples de règles de politique de décryptage comprennent une catégorie d'URL personnalisée (**Objects (Objets)** > **Custom Objects (Objets Personnalisés)** > **URL Category (Catégorie d'URL)**) afin de limiter le champ de trafic à décrypter. Chaque règle de politique de décryptage utilise la même catégorie d'URL personnalisée (ainsi que la source et la destination) que la règle de politique de Sécurité analogue, afin que les politiques de Sécurité et de décryptage s'appliquent exactement au même trafic. L'association d'App-ID et d'une catégorie d'URL personnalisée donne la possibilité au pare-feu de décrypter uniquement le trafic autorisé par la règle d'autorisation pour les applications, ce qui permet d'économiser des cycles de traitement en n'ayant pas à décrypter le trafic bloqué par le pare-feu. (Le décryptage doit se dérouler en amont de l'évaluation par la règle de politique de Sécurité.)

STEP 1 | Décryptez le trafic entre les serveurs du centre de données et les serveurs de mises à jour logicielles présents sur Internet.

Cette règle montre comment décrypter le trafic concernant les mises à jour logicielles et les serveurs du centre de données pour apporter de la visibilité sur des menaces qui pourraient être présentes dans des serveurs de mises à jour sur Internet, afin de permettre au pare-feu de les bloquer. Cet exemple décrypte le trafic autorisé entre les serveurs du centre de données et les serveurs de mises à jour CentOS sur Internet, en se basant sur la règle d'autorisation pour les applications analogue créée dans Création des règles d'autorisation pour les applications concernant le trafic du centre de données vers Internet.

		Source		Destination			Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	ZONE	ADDRESS	URL CATEGORY	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
CentOS Update Decrypt	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	L3-External	any	CentOS-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

Pour appliquer cette règle :

- Définissez la même source et la même destination que dans la règle de politique de Sécurité analogue. Dans ce cas, la source est le groupe d'adresses dynamiques **Dev-Servers** dans la zone**Engineering-DC-Infra**, et la destination est Internet (**L3-External** zone).
- Définissez la même catégorie d'URL personnalisée que dans la règle de politique de sécurité analogue (**CentOS-Update-Servers**) pour limiter le champ de décryptage au trafic autorisé par la règle d'autorisation pour les applications, afin d'éviter au pare-feu de gaspiller des cycles de traitement à décrypter du trafic qui sera écarté.
- Dans l'onglet Options, définissez l'Action sur **Decrypt (Décrypter)** et le type de décryptage sur **SSL Forward Proxy (Proxy de transfert SSL)**. Appliquez le profil de décryptage du centre de données respectant les meilleures pratiques pour appliquer les paramètres du proxy de transfert SSL et du protocole SSL dans le trafic.

Créez une règle de politique de décryptage similaire pour le trafic autorisé du centre de données pour chaque groupe de serveurs du centre de données ayant besoin de se connecter à des serveurs de mises à jour sur Internet, basée sur la même source et la même destination, ainsi que la même catégorie d'URL personnalisée que dans la règle de politique de Sécurité analogue. Par exemple, la règle de politique de décryptage pour les serveurs du centre de données ayant besoin de communiquer avec des serveurs de

mises à jour Microsoft Windows, qui se base sur la règle de politique de sécurité analogue, ressemble à ceci :

		Source		Destination			Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	ZONE	ADDRESS	URL CATEGORY	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Win Update Decrypt	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	L3-External	any	Win-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

STEP 2 | Décryptez le trafic entre les serveurs du centre de données et les serveurs de mises à jour NTP et DNS présents sur Internet.

Cette règle montre comment décrypter le trafic concernant les mises à jour NTP et DNS et les serveurs du centre de données pour apporter de la visibilité sur des menaces qui pourraient être présentes dans ces serveurs Internet, afin de permettre au pare-feu de les bloquer. Cet exemple décrypte le trafic autorisé, en se basant sur la règle d'autorisation pour les applications analogue créée dans Création des règles d'autorisation pour les applications concernant le trafic du centre de données vers Internet.

		Source		Destination			Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	ZONE	ADDRESS	URL CATEGORY	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
DNS-NTP Update Decrypt	DC to Internet BP	IT Infrastructure	DNS-NTP-Servers	L3-External	any	NTP-DNS-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

Pour appliquer cette règle :

- Définissez la même source et la même destination que dans la règle de politique de Sécurité analogue. Dans ce cas, la source est le groupe d'adresses dynamiques **DNS-NTP-Servers** dans la zone **IT-Infrastructure**, et la destination est Internet (**L3-External** zone).
- Définissez la même catégorie d'URL personnalisée que dans la règle de politique de Sécurité analogue (**NTP-DNS-Update-Servers**) pour limiter le champ de décryptage au trafic autorisé par la règle d'autorisation pour les applications, afin de limiter le champ de trafic à décrypter au trafic autorisé par la règle d'autorisation pour les applications.
- Dans l'onglet Options, définissez l'Action sur **Decrypt (Décrypter)** et le type de décryptage sur **SSL Forward Proxy (Proxy de transfert SSL)**. Appliquez le profil de décryptage du centre de données respectant les meilleures pratiques pour appliquer les paramètres du proxy de transfert SSL et du protocole SSL dans le trafic.

Définition de la politique de sécurité initiale du trafic au sein du centre de données

Le trafic au sein du centre de données circule entre les couches d'applications et les serveurs du centre de données. Vous pourriez partir du principe que l'ensemble du périmètre du centre de données est digne de confiance et qu'il n'y a pas lieu d'inspecter ce trafic. Pourtant, si un pirate informatique compromet un serveur du centre de données et si le trafic entre couches d'applications ne passe pas par des pare-feu, le pirate informatique peut se déplacer latéralement entre les serveurs essentiels du centre de données et télécharger d'autres programmes malveillants, réaffecter des serveurs et exfiltrer des données en utilisant des applications légitimes qui n'ont aucune raison de figurer dans le centre de données, comme cela s'est produit pour de graves atteintes à la sécurité des données ces dernières années.

La meilleure défense contre les programmes malveillants qui réussissent à prendre pied dans le centre de données est de sécuriser le trafic avec des règles strictes, spécifiques, d'autorisation pour les applications, et d'inspecter le trafic avec des pare-feu nouvelle génération placés entre les couches d'applications.

De plus, n'autorisez aucune application inconnue dans le centre de données. La présence d'applications inconnues peut signifier qu'un pirate informatique a pu accéder à votre centre de données. Procédez à la création d'applications personnalisées pour vos applications propriétaires internes afin de les identifier à l'aide d'App-ID et d'appliquer des mesures de sécurité à ce trafic. Si vous ne créez pas d'applications personnalisées pour vos applications propriétaires, le pare-feu les voit comme du trafic unknown-tcp ou unknown-udp. Le problème est que le pare-feu traite les applications propriétaires de la même façon qu'il traite d'autres applications inconnues, et vous avez tout intérêt à bloquer les applications inconnues, car elles peuvent être l'outil d'un pirate informatique. Si vous autorisez des applications inconnues dans votre centre de données, vous pourriez remettre les clés de votre royaume d'actifs à un attaquant.

Concernant des applications commerciales inconnues, vous pouvez soumettre une requête *à Palo Alto Networks dans le but de créer une App-ID.*

Si vous avez déjà des politiques de Contrôle Prioritaire pour des Applications, créées uniquement pour définir des délais d'expiration de session personnalisés pour un ensemble de ports, convertissez ces politiques de Contrôle Prioritaire pour des Applications existantes en politiques basées sur des applications, en configurant des délais d'expiration de session basés sur le service, afin de conserver un délai d'expiration personnalisé pour chaque application et de migrer ensuite la règle vers une règle basée sur des applications. Les politiques de Contrôle Prioritaire pour des Applications sont basées sur le port. Lorsque vous utilisez des politiques de Contrôle Prioritaire pour des Applications pour conserver des délais d'expiration de session personnalisés pour un ensemble de ports, vous perdez de la visibilité sur les applications dans ces flux, et vous ne savez pas quelles applications utilisent les ports et vous ne pouvez pas non plus les contrôler. Les délais d'expiration de session basés sur le service permettent d'avoir des délais d'expiration de session personnalisés tout en conservant une visibilité sur les applications.

- Approches de la sécurité liée au trafic au sein du centre de données
- Création des règles d'autorisation pour les applications concernant le trafic au sein du centre de données
- Création des règles relatives à la politique de décryptage concernant le trafic au sein du centre de données

Approches de la sécurité liée au trafic au sein du centre de données

L'approche traditionnelle utilisée pour les anciens systèmes, consistant à sécuriser le trafic est-ouest entre serveurs du centre de données, laisse de précieuses ressources exposées au risque, alors que l'approche respectant les meilleures pratiques protège vos ressources les plus précieuses.

L'approche traditionnelle	Risque	Approche respectant les meilleures pratiques
Vous n'avez pas besoin de segmenter le trafic qui ne traverse pas le périmètre du centre de données donc le trafic entre couches d'applications ne doit pas passer à travers les infrastructures de sécurité.	Un attaquant qui compromet un serveur du centre de données peut se déplacer latéralement vers les serveurs critiques du centre de données et les réutiliser. Des pirates informatiques au cœur du centre de données peuvent se déplacer comme ils l'entendent sans crainte d'être découverts.	Segmentez le trafic entre les couches d'applications en utilisant des règles strictes d'autorisation pour les applications, dans le but d'empêcher toute communication inutile, de réduire la surface d'attaque, et d'empêcher un pirate informatique de se déplacer latéralement au cœur du centre de données. Enregistrez et surveillez les infractions de la liste d'autorisation.
Le centre de données est sécurisé au sein d'un réseau fiable, il n'est donc pas urgent de corriger rapidement les serveurs du centre de données.	Les vulnérabilités restent ouvertes plus longtemps et offrent des vecteurs d'attaque aux pirates informatiques.	Installez rapidement les correctifs sur les serveurs du centre de données afin d'éliminer les vulnérabilités. Créer des règles de politique de sécurité d'autorisation pour les applications vous permet de comprendre ce qui s'exécute sur votre centre de données et où s'exécutent des services non corrigés.
Mélangez les profils de prévention des menaces par blocage et alerte de plusieurs fournisseurs.	Un mélange d'outils individuels laisse des trous dans votre sécurité pour les pirates informatiques et risquent de ne pas bien fonctionner ensemble.	La suite d'outils de sécurité coordonnées de Palo Alto Networks travaille de concert pour colmater les trous de sécurité, empêcher les attaques, et identifier les programmes malveillants qui tentent de se propager parmi les serveurs du centre de données.

En outre :

- Créez un compte de service unique pour chaque fonction. Par exemple, autorisez uniquement des comptes de services spécifiques à répliquer des messageries d'échange, et autorisez uniquement des

comptes de services sur des serveurs web à envoyer des requêtes aux bases de données MySQL. N'utilisez pas un seul compte de service pour les deux fonctions.

- Surveillez les comptes de service.
- N'autorisez pas les comptes d'utilisateurs habituels dans le centre de données.

Quand vous effectuez la transition de règles basées sur le port à des règles basées sur les applications, dans la base des règles, positionnez la règle basée sur l'application au-dessus de la règle basée sur le port qu'elle doit remplacer. Réinitialisez le compteur de correspondance à la règle de politique *pour les deux règles. Si le trafic correspond à la règle basée sur les ports, le nombre de correspondances à la règle de politique augmente. Ajustez la règle basée sur l'application jusqu'à ce qu'aucun trafic n'atteigne la règle basée sur le port pendant une certaine période, puis retirez la règle basée sur le port.*

Création des règles d'autorisation pour les applications concernant le trafic au sein du centre de données

Le trafic du centre de données est la plupart du temps un trafic d'application multicouches qui circule entre différentes couches de serveur pour fournir des services pour des applications telles que SharePoint, WordPress, des applications de confidentialité interne, etc. L'architecture d'applications multicouches la plus courante est composée de serveurs web (couche de présentation), de serveurs d'application (couche d'application) et de serveurs de base de données (couche de données). Le chapitre Création d'une stratégie de segmentation du centre de données fournit des recommandations sur la façon de positionner des pare-feu entre couches d'applications et sur la façon de segmenter un centre de données.

La façon dont vous traitez le trafic entre les serveurs du centre de données dépend du trafic. Pour la plupart du trafic d'applications, ajoutez un profil de prévention des menaces aux règles d'autorisation pour la politique de sécurité afin de contrôler le trafic. Par exemple, appliquez toujours les Profils de Sécurité respectant les meilleures pratiques pour protéger le trafic entre couches web, applications et serveurs des applications des départements Finance, Ingénierie Informatique, etc. L'exception à l'application de ces profils de prévention des menaces est le trafic pour des applications à volume élevé et faible valeur, de type duplication de messagerie et flux de sauvegardes. L'accès à ces applications est toujours autorisé par des règles, mais comme un pare-feu a déjà inspecté le trafic avant duplication, appliquer des profils de prévention des menaces consomme des cycles du processeur de votre pare-feu sans apporter de valeur ajoutée.

Le profil de sécurité WildFire identifie les logiciels malveillants inconnus qui tentent de se propager parmi les serveurs du centre de données afin d'empêcher l'exfiltration de données, en découvrant les logiciels malveillants avant qu'ils ne causent des dommages. Si vous n'avez pas accès au cloud global WildFire*, vous pouvez déployer un* cloud privé WildFire *ou un* cloud hybride WildFire.

L'exemple de règles de politique de sécurité de cette section montre comment autoriser le trafic d'applications financières d'un centre de données multicouche qui nécessite l'utilisation des couches serveur web, des couches d'applications et des couches de données pour le fonctionnement de ses applications. L'exemple comprend deux applications propriétaires internes pour lesquelles nous avons procédé à une Création d'applications personnalisées : **Billing-App (Application de facturation)** et **Payment-App (Application de paiement)**. La création d'App-ID personnalisés pour ces applications permet au pare-feu de les identifier, de les contrôler et de leur appliquer une politique de sécurité.

N’autorisez pas d’applications inconnues dans le centre de données, car vous ne pouvez pas les identifier et leur appliquer des mesures de sécurité, et elles peuvent révéler un adversaire dans votre centre de données. Chaque application de centre de données doit avoir un App-ID.

*Autorisez les applications uniquement sur leur port (**application-default (d’application par défaut)**). Dans certains cas, des besoins commerciaux peuvent nécessiter de votre part une exception et l’autorisation de ports non standard par certaines applications entre clients et serveurs spécifiques. Dans ces cas, ayez connaissance du trafic de l’application s’exécutant sur des ports non standard, et assurez-vous d’être au courant de chaque instance d’applications s’exécutant sur un port non standard. Les applications s’exécutant sur des ports non standard pour lesquelles vous n’avez pas effectué d’exception expresse (connue) peuvent indiquer la présence de logiciel malveillant utilisant des techniques d’évasion.*

Marquez toutes les applications approuvées *avec le marquage prédéfini Approuvé. Panorama et les pare-feu considèrent les applications sans marquage Approuvé comme des applications non approuvées.*

La section Tri de la base des règles de la politique de sécurité du centre de données vous montre comment trier ces règles parmi toutes les autres règles créées pour les trois autres flux de trafic du centre de données ainsi que les règles de blocage, afin qu’aucune règle ne fasse de l’ombre à une autre.

Dans le but d’appliquer une politique de sécurité cohérente sur plusieurs centres de données, vous pouvez réutiliser des modèles et des paquets de modèles, afin que les mêmes politiques s’appliquent à chaque centre de données. Les modèles utilisent des variables afin d’appliquer des valeurs spécifiques aux périphériques, telles que adresses IP, FQDN, etc., tout en maintenant une politique de sécurité globale et en réduisant la quantité de modèles et de paquets de modèles que vous devez gérer.

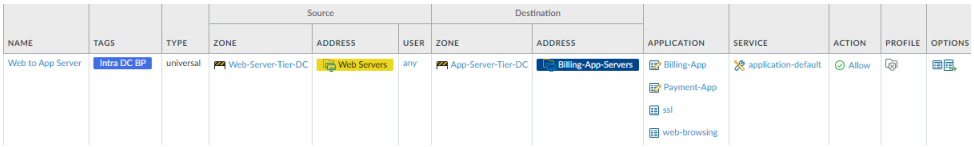
Chacune des règles d’autorisation suivantes :

- Est jointe au groupe de profils de sécurité des meilleures pratiques, que sont les profils de sécurité des meilleures pratiques. L’utilisation d’un groupe de profils de sécurité vous permet d’appliquer tous les profils de meilleures pratiques à un règle en même temps plutôt que de préciser chaque profil individuellement. Les groupes de profils de sécurité rendent la configuration de la protection contre les logiciels malveillants, les vulnérabilités, le trafic C2, et les menaces connues et inconnues plus rapide et plus simple.
- Journalise le trafic (à la fin des sessions) afin que vous puissiez suivre et analyser les infractions de règles, et inclut le transfert des journaux. Transfère les journaux vers les serveurs de journaux et, le cas échéant, transfère les e-mails aux administrateurs appropriés.

STEP 1 | Autorisez le trafic des applications financières entre la couche serveur web et la couche d’applications.

Cette règle limite le trafic pouvant circuler entre la couche serveur web et la couche d’applications pour les serveurs de facturation du département Finance, afin que seul le trafic d’applications légitimes puisse accéder aux serveurs de facturation. (Nous créons également une règle pour limiter l’accès de l’utilisateur Finance au centre de données lorsque nous Création des règles d’autorisation pour les applications concernant le trafic de l’utilisateur vers le centre de données, afin que seuls les utilisateurs approuvés du service des finances puissent accéder au centre de données.) La règle utilise des groupes d’adresses dynamiques pour spécifier les serveurs dans chaque couche d’application :**Web-Servers (Serveur Web)** spécifie les adresses des serveurs dans la couche des serveurs web et **Billing-App-**

Servers (Serveurs de facturation) spécifie les adresses des serveurs dans la couche des serveurs d'applications du service facturation du département Finance.



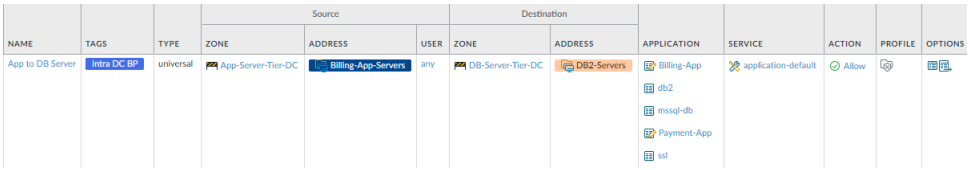
Pour appliquer cette règle :

- Limitez la source du trafic de l'application financière aux serveurs web (**Web-Servers**) dans la zone **Web-Server-Tier-DC**.
- Limitez la destination du trafic de l'application financière aux serveurs de facturation (**Billing-App-Servers**) dans la zone **App-Server-Tier-DC**.
- Limitez les applications que les serveurs web peuvent utiliser pour accéder aux serveurs d'applications de facturation et autorisez uniquement les applications sur leurs ports par défaut. Dans cet exemple, les applications incluent deux applications propres à l'entreprise, **Billing-App (Application de facturation)** et **Payment-App (Application de paiement)**, pour lesquelles vous spécifiez les ports par défaut lorsque vous créez les applications. Le service des finances utilise ces applications propriétaires pour les services de facturation et de paiement.

Créez des règles similaires pour contrôler les applications et le trafic entre la couche serveur web et la couche d'applications.

STEP 2 | Autorisez le trafic des applications financières entre la couche d'applications et la couche base de données.

Cette règle limite le trafic pouvant circuler entre la couche d'applications et la couche base de données pour les serveurs de facturation du département Finance, afin que seul le trafic d'applications légitimes puisse circuler entre les serveurs des applications de facturation et les serveurs des bases de données de facturation. La règle utilise des groupes d'adresses dynamiques pour spécifier les serveurs dans chaque couche d'application :**Billing-App-Servers (Serveur Facturation)** spécifie les adresses des serveurs dans la couche des serveurs d'applications et **DB2-Servers (Serveurs de base de données)** spécifie les adresses des serveurs dans la couche des serveurs de base de données du département Finance.



Pour appliquer cette règle :

- Limitez la source du trafic de l'application financière aux serveurs de facturation (**Billing-App-Servers**) dans la zone **App-Server-Tier-DC**.
- Limitez la destination du trafic de l'application financière aux serveurs de base de données (**DB2-Servers**) dans la zone **DB-Server-Tier-DC**.
- Limitez les applications que les serveurs d'applications de facturation peuvent utiliser pour accéder aux serveurs de base de données et autorisez uniquement les applications sur leurs ports par défaut ou sur leurs ports non par défaut connus.

Créez des règles similaires pour contrôler les applications et le trafic entre la couche d'applications et la couche base de données pour d'autres applications.

Vérifiez que seules les applications que vous avez autorisées dans les règles de politique de sécurité s'exécutent en affichant le rapport d'applications prédéfini (**Monitor [Surveillance]** > **Reports [Rapports]** > **Application Reports [Rapports d'Application]** > **Applications**). Si vous voyez des applications non prévues dans le rapport, examinez les règles d'autorisation pour les applications et affinez-les afin qu'elles n'autorisent pas d'applications non prévues.

Création des règles relatives à la politique de décryptage concernant le trafic au sein du centre de données

Pourquoi déchiffrer le trafic à l'intérieur du centre de données ? Après tout, il ne compte pas d'utilisateur et le centre de données est un environnement sûr se trouvant au plus profond d'un réseau sécurisé. Mais rien ne pourrait être plus éloigné de la vérité. Pour un pirate informatique, le centre de données est l'endroit idéal où se cacher précisément parce que la plupart des gens pensent qu'il est sûr et ne regardent pas dedans. Néanmoins, le même principe de base qui s'avère exact pour le reste du réseau l'est également pour le centre de données : vous ne pouvez pas vous protéger contre une menace que vous ne voyez pas. Décryptez le trafic au sein du centre de données pour que le pare-feu puisse inspecter le trafic, contrôler l'accès, rendre des menaces visibles, et protéger vos ressources les plus précieuses.

Certains trafics du centre de données ne sont pas chiffrés (texte en clair). N'activez pas de décryptage sur les flux en clair, car il n'y a rien à décrypter.

Dans Création des règles d'autorisation pour les applications concernant le trafic au sein du centre de données, nous avons créé des règles de politique de sécurité qui autorisent les serveurs fonctionnant avec des applications du service des finances situées dans d'autres couches d'applications à communiquer entre eux. Ici, nous créons des règles de politique de décryptage analogues, pour décrypter le trafic autorisé par ces règles.

Pour chaque règle, configurez le décryptage de journalisation et le transfert des journaux. Journalisez autant de décryptage de trafic que les ressources de votre pare-feu le permettent.

STEP 1 | Décryptez le trafic des applications financières entre la couche serveur web et la couche d'applications.

Cette règle décrypte le trafic circulant entre la couche serveur web et la couche d'applications des serveurs de facturation du département Finance, afin que le pare-feu puisse voir ce trafic et protéger les serveurs, dans chaque couche, contre des menaces potentielles.

		Source			Destination		Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Web to App	Intra DC BP	Web-Server-Tier-DC	Web Servers	any	App-Server-Tier-DC	Billing-App-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

Pour appliquer cette règle :

- Définissez la même source et la même destination que dans la règle de politique de Sécurité analogue. Dans cet exemple, la source est le groupe d'adresses dynamiques **Web-Servers** dans la zone **Web-Server-Tier-DC**, et la destination est le **Billing-App-Servers (Serveurs de Facturation)** dans la zone **App-Server-Tier-DC**.
- Dans l'onglet Options, définissez l'Action sur **Decrypt (Décrypter)** et le type de décryptage sur **SSL Forward Proxy (Proxy de transfert SSL)**. Appliquez le profil de décryptage du centre de données respectant les meilleures pratiques pour appliquer les paramètres du proxy de transfert SSL et du protocole SSL dans le trafic.

STEP 2 | Décryptez le trafic des applications financières entre la couche d'applications et la couche base de données.

Cette règle décrypte le trafic circulant entre la couche d'applications et la couche base de données des serveurs de facturation du département Finance, afin que le pare-feu puisse voir ce trafic et protéger les serveurs, dans chaque couche, contre des menaces potentielles.

		Source			Destination		Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
App to DB	Intra DC BP	App-Server-Tier-DC	Billing-App-Servers	any	DB-Server-Tier-DC	DB2-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

Pour appliquer cette règle :

- Définissez la même source et la même destination que dans la règle de politique de Sécurité analogue. Dans cet exemple, la source est le groupe d'adresses dynamiques **Billing-App-Servers (Serveurs de Facturation)** dans la zone **App-Server-Tier-DC**, et la destination est **DB2-Servers** dans la zone **DB-Server-Tier-DC**.
- Dans l'onglet Options, définissez l'Action sur **Decrypt (Décrypter)** et le type de décryptage sur **SSL Forward Proxy (Proxy de transfert SSL)**. Appliquez le profil de décryptage du centre de données respectant les meilleures pratiques pour appliquer les paramètres du proxy de transfert SSL et du protocole SSL dans le trafic.

Tri de la base de règles de la politique de sécurité du centre de données

Ce sujet offre un aperçu de l'exemple de la base de règle de politique de sécurité qui indique l'ordre des règles pour les quatre flux de trafic du centre de données. Les sections précédentes traitaient de chacune des règles de politique de sécurité en détail (ainsi que les règles de politique de Décryptage et, lorsque nécessaire, la politique d'authentification ainsi que les règles de politique de protection DoS).

L'ordre des règles de politique de sécurité est essentiel. Aucune règle ne doit faire de l'ombre à une autre. Par exemple, les règles de blocage ne devraient pas bloquer le trafic que vous souhaitez autoriser, vous devez donc placez les règles d'autorisation *avant* que la règle qui bloquerait le trafic soit effective. Dans le même ordre d'idée, une règle d'autorisation ne doit pas autoriser du trafic que vous voulez bloquer. En créant des règles d'autorisation très spécifiques, vous contrôlez fermement les applications autorisées et qui peut et ne peut pas les utiliser.

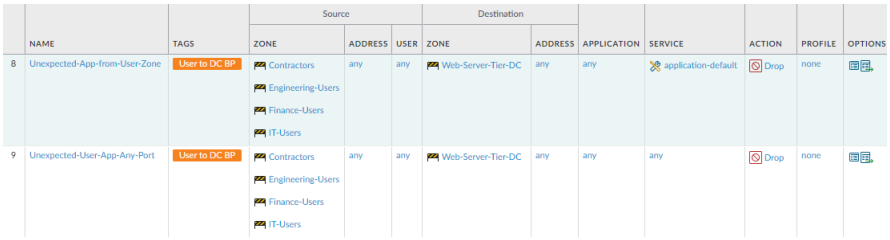
Règles 1-7 : Les deux premières règles bloquent l'application QUIC pour l'empêcher de bloquer le trafic ou d'interdire le décryptage. Les cinq prochaines règles autorisent l'accès DNS des utilisateurs, et autorisent des applications et un accès aux serveurs spécifiques pour des groupes d'utilisateurs spécifiques. Ce sont les règles configurées dans Création des règles d'autorisation pour les applications concernant le trafic de l'utilisateur vers le centre de données.

			Source			Destination						
	NAME	TAGS	ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
1	Block QUIC UDP	none	any	any	any	L3-External	any	any	quic_udp_ports	Deny	none	
2	Block QUIC	none	any	any	any	L3-External	any	quic	application-default	Deny	none	
3	DNS Services	User to DC BP	any	any	any	IT Infrastructure	DNS-Servers	dns	application-default	Allow		
4	IT DC Server Management	User to DC BP	IT-Users	any	it-superusers	IT-Server-Access-DC	IT-Server-Management	ms-rdp ssh ssl	Custom-IT-Ports	Allow		
5	Engineering Resources	User to DC BP	Engineering-Users	any	api-users engg-users	Engineering-DC-Infra	Dev-Servers	oracle-bi perforce profinet qlikview	application-default	Allow		
6	Finance to DC	User to DC BP	Finance-Users	any	accounting-users finance-users	Finance-DC-Infra	Fin-Servers	netsuite oracle oracle-crm-ondemand oracle-forms	application-default	Allow		
7	SAP-Contractors	User to DC BP	Contractors	any	sap-contractors	SAP-Infra	SAP DB Servers	ms-sql-analysis-service mssql-db mssql-mon sap	application-default	Allow		

Figure 1: Règles du centre de données 1-7

Seuls les utilisateurs spécifiés peuvent utiliser les applications spécifiées sur leurs ports par défaut pour accéder aux serveurs de destination du centre de données spécifiés (adresses). Les profils de sécurité protègent l'ensemble de ces règles d'autorisation contre les menaces. Ces règles précèdent des règles de blocage qui révèlent des applications et des utilisateurs inconnus sur le réseau, car ces règles sont très spécifiques et elles empêchent les applications et utilisateurs autorisés de correspondre à des règles plus globales situées plus bas dans la base de règles.

Règles 8-9 : Tandis que les règles précédentes autorisent les applications autorisées, les deux prochaines règles, crées dans la section Création des règles de blocage du trafic pour le centre de données, découvrent et bloquent les applications inattendues des utilisateurs sur les ports standard et bloquent toutes les applications ou les ports non standards. (Votre déploiement peut comporter plusieurs zones utilisateur que ce qui est indiqué dans l'exemple.)

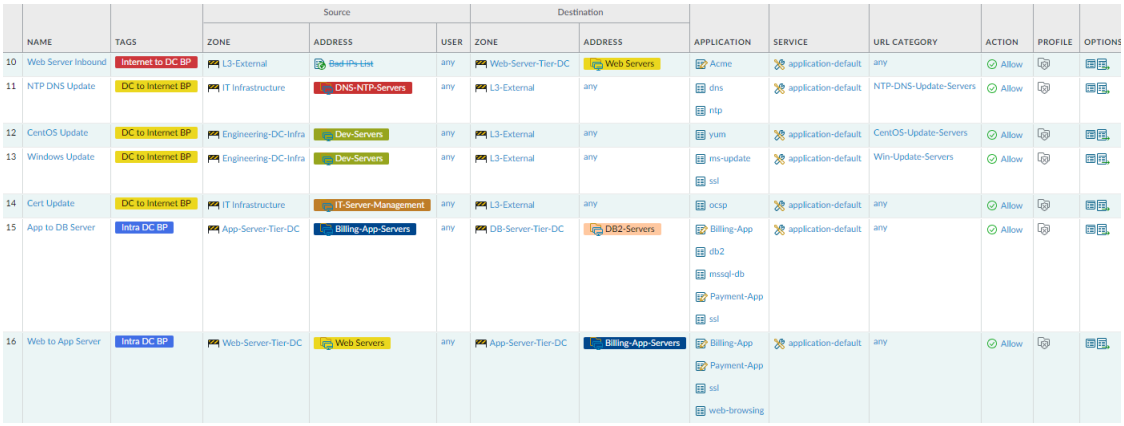


	NAME	TAGS	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
8	Unexpected-App-from-User-Zone	User to DC BP	Contractors Engineering-Users Finance-Users IT-Users	any	any	Web-Server-Tier-DC	any	any	application-default	Drop	none	
9	Unexpected-User-App-Any-Port	User to DC BP	Contractors Engineering-Users Finance-Users IT-Users	any	any	Web-Server-Tier-DC	any	any	any	Drop	none	

Figure 2: Règles du centre de données 8-9

Le trafic provenant de zones non utilisateur ne correspond pas à ces règles. Placez donc ces règles au-dessus des règles de blocage d'applications (règles 18 et 19) ou bien elles feront de l'ombre à ces règles. (Le trafic correspondant à ces deux règles peut également correspondre aux règles de blocage d'applications plus globales. Si les règles de blocage d'applications arrivent en premier et correspondent à du trafic correspondant également à ces règles, le trafic ne correspondra pas à ces règles et ne sera pas journalisé séparément, les règles ne joueront donc pas leur rôle prévu de distinction entre blocage résultant de l'activité d'un utilisateur employé et entre blocage résultant de l'activité des zones non utilisateur.)

Règles 10-16 : Les sept prochaines règles autorisent le trafic entre le centre de données et Internet et au sein du centre de données (créé dans Création des règles d'autorisation pour les applications concernant le trafic d'Internet vers le centre de données, Création des règles d'autorisation pour les applications concernant le trafic du centre de données vers Internet et Création des règles d'autorisation pour les applications concernant le trafic au sein du centre de données). Les profils de sécurité protègent l'ensemble de ces règles d'autorisation contre les menaces.



	NAME	TAGS	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
10	Web Server Inbound	Internet to DC BP	L3-External	Bad IPs List	any	Web-Server-Tier-DC	Web Servers	Acme	application-default	any	Allow		
11	NTP DNS Update	DC to Internet BP	IT Infrastructure	DNS-NTP-Servers	any	L3-External	any	dns ntp	application-default	NTP-DNS-Update-Servers	Allow		
12	CentOS Update	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	yum	application-default	CentOS-Update-Servers	Allow		
13	Windows Update	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	ms-update ssl	application-default	Win-Update-Servers	Allow		
14	Cert Update	DC to Internet BP	IT Infrastructure	IT-Server-Management	any	L3-External	any	ocsp	application-default	any	Allow		
15	App to DB Server	Intra DC BP	App-Server-Tier-DC	Billing-App-Servers	any	DB-Server-Tier-DC	DB2-Servers	Billing-App db2 mssql-db Payment-App ssl	application-default	any	Allow		
16	Web to App Server	Intra DC BP	Web-Server-Tier-DC	Web Servers	any	App-Server-Tier-DC	Billing-App-Servers	Billing-App Payment-App ssl web-browsing	application-default	any	Allow		

Figure 3: Règles du centre de données 10-16

Règles 17-20 : Les quatre dernières règles, que nous avons configurées dans la section Création des règles de blocage de trafic pour le centre de données, bloquent les applications que vous ne voulez en aucun cas dans votre centre de données ainsi que les applications inattendues, et révèlent des utilisateurs inconnus sur votre réseau.

		Source			Destination						
	NAME	ZO...	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
17	Block-Bad-Apps	any	any	any	App-Server-Tier-DC DB-Server-Tier-DC Engineering-DC-Infra Finance-DC-Infra IT Infrastructure SAP-Infra Web-Server-Tier-DC	any	Encrypted-Tunnels File-Sharing Remote-Access	any	Drop	none	
18	Unexpected-App-from-Any-Zone	any	any	any	Web-Server-Tier-DC	any	any	application-default	Drop	none	
19	Unexpected-App-Any-Port	any	any	any	Web-Server-Tier-DC	any	any	any	Drop	none	
20	Discover-Unknown-Users	any	any	unknown	any	any	any	any	Deny	none	

La règle 17 bloque les applications que vous ne voulez en aucun cas dans votre centre de données. Cette règle vient après les règles d'autorisation pour les applications pour autoriser l'accès aux exceptions. Par exemple, vous pouvez approuver une ou deux applications de partage de fichiers dans les règles d'autorisation pour les applications qui précèdent cette règle de blocage, laissant ensuite au filtre d'applications présent dans cette règle le soin de bloquer toutes les autres applications de ce type, pour empêcher l'utilisation non approuvée d'applications de partage de fichiers. Si vous ne voulez en aucun cas d'un ensemble d'applications ou de certaines applications individuelles sur votre réseau, sans exception, par exemple BitTorrent, vous pouvez établir une règle de blocage spécifique afin de bloquer uniquement ces applications et la placer au sommet de la base de règles, au-dessus des règles d'autorisation pour les applications. Cependant, si vous faites cela, vous devez vous assurer qu'aucune des applications bloquées n'a d'utilisation professionnelle légitime, car les utilisateurs ne pourront plus y accéder.

Les règles 18 et 19 sont analogues aux règles 8 et 9, qui révèlent des applications utilisateurs inattendues (le trafic auquel s'appliquent ces règles provient uniquement de zones utilisateurs). Les règles 18 et 19 révèlent des applications inattendues de toutes les autres zones. Le fait d'avoir des règles séparées vous permet de journaliser des correspondances avec des règles de blocage de manière plus granulaire.

La règle 20 révèle des utilisateurs inconnus, pour vous permettre de journaliser ces tentatives d'accès séparément, pour mener plus facilement votre enquête.

Comme pour toutes les bases des règles de politique de sécurité, les deux dernières règles seront les règles par défaut de Palo Alto Networks concernant le trafic intrazone (autorisé) et le trafic interzone (rejeté).

Journalisation et surveillance du trafic du centre de données

Les outils de journalisation et de surveillance du pare-feu révèlent les applications, les utilisateurs et les modèles de trafic sur votre réseau, y compris les applications et les utilisateurs dont vous ignoriez peut-être l'existence. Journaliser et surveiller fournit des informations pertinentes à toutes les étapes de la transition vers une politique de sécurité du centre de données respectant les meilleures pratiques ainsi qu'à sa maintenance, car cela révèle également des utilisateurs inconnus (non identifiés par User-ID), des applications inconnues, ainsi que du trafic sur des ports inattendus, indiquant tous qu'une règle de politique de Sécurité n'a pas été correctement ou strictement élaborée. Les informations de journalisation et de surveillance vous aident à déterminer quelles applications doivent être autorisées et quels utilisateurs doivent avoir accès à quelles applications et à quels périphériques. Elles vous aident également à enquêter sur de potentiels problèmes de sécurité.

Lorsque vous évaluez votre centre de données, vous capturez des mesures de référence. Comparez régulièrement la mesure de référence avec sa mesure prise durant l'étape de planification afin d'évaluer le progrès accompli, identifier les modifications apportées, et trouver des aspects à améliorer tandis que vous mettez en place la politique de sécurité de votre centre de données respectant les meilleures pratiques.

Si vous gérez des pare-feu avec Panorama, vous pouvez surveiller la santé des pare-feu pour comparer les périphériques par rapport à leur rendement de base et entre eux, pour identifier les écarts par rapport à leur comportement normal.

Configurez le transfert de journaux des pare-feu vers Panorama ou vers des services externes comme un serveur Trap SNMP ou un serveur syslog pour centraliser les journaux de plusieurs pare-feu, pour une visualisation et une analyse plus pratiques (un pare-feu ne peut qu'afficher les journaux et rapports locaux, et non les journaux et rapports d'autres pare-feu). Lorsque vous configurez le transfert de journaux, configurez l'envoi de notifications pour vérifier que les destinations des journaux que vous avez configurés reçoivent bien les journaux des pare-feu.

Liste des meilleures pratiques pour la journalisation et la surveillance du centre de données :

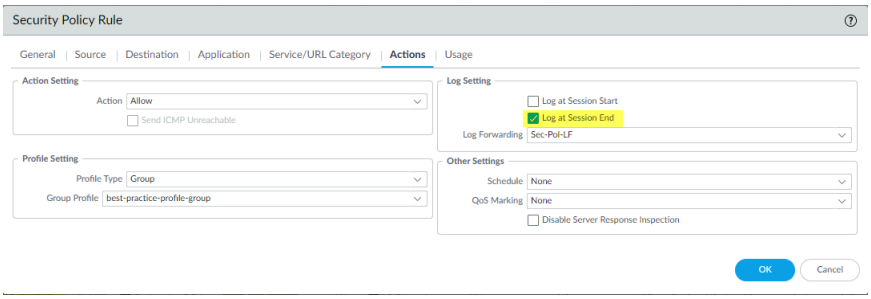
- Choix du trafic du centre de données à journaliser et à surveiller
- Surveillance des règles de blocage pour le centre de données et affinage de la base de règles
- Journalisation du trafic du centre de données ne correspondant à aucune règle d'autorisation de l'interzone
- Journalisation du trafic au sein du centre de données correspondant à la règle d'autorisation de l'intrazone

Choix du trafic du centre de données à journaliser et à surveiller

Le pare-feu nouvelle génération de Palo Alto Networks crée des journaux par défaut, mais vous devez configurer la journalisation pour d'autres trafics. La meilleure pratique consiste à journaliser l'ensemble du trafic du centre de données et de surveiller les journaux à la recherche d'applications, d'utilisateurs, de trafic, et de comportements inattendus.

Par défaut, le pare-feu journalise le trafic correspondant aux règles de sécurité configurées explicitement et ne journalise pas le trafic correspondant aux règles prédéfinies intrazone-default (autorisant le trafic avec source et destination dans la même zone) et interzone-default (la dernière règle de la base des règles, refusant le trafic ne correspondant à aucune des règles précédentes) au bas de la base des règles.

Lorsque vous créez une règle de politique de sécurité, le pare-feu journalise le trafic en fin de la session par défaut :



Cependant, le pare-feu ne transfère pas les journaux par défaut et n'applique pas les profils de sécurité par défaut. L'exemple précédent montre la meilleure pratique relative au transfert de journaux vers les serveurs de journaux et administrateurs et à l'application de la meilleure pratique relative aux profils de sécurité.

La meilleure pratique pour la plupart du trafic est de **journaliser en fin de session**, car les applications changent souvent au cours du cycle de vie d'une session. Par exemple, l'App-ID initiale pour une session peut être web-browsing, mais une fois que le pare-feu a traité quelques paquets, le pare-feu peut trouver une App-ID plus spécifique pour l'application et changer l'App-ID. Il existe plusieurs cas d'utilisation pour journaliser le trafic au début d'une session, y compris les sessions de tunnel de longue durée telles que les tunnels GRE (vous ne pouvez pas voir ces sessions actives dans l'ACC à moins de vous **connecter à la fois au début** et **à la fin de la session**), lorsque vous avez besoin d'informations dès le début de la session pour le dépannage, et pour gagner en visibilité sur les sessions OT/ICS (Operational Technology/Industrial Control Systems), qui sont également des sessions de longue durée.

La journalisation du trafic enregistre des informations sur le trafic autorisé par une règle et sur le trafic qu'une règle refuse ou supprime (violations de règles), de sorte que le pare-feu fournit des informations précieuses quelle que soit la manière dont il traite le trafic. Les violations de règles mettent l'accent sur des attaques potentielles ou sur des règles d'autorisation qui doivent être adaptées pour autoriser une application commerciale légitime.

Lorsque vous examinez le trafic bloqué dans les journaux, faites la différence entre le trafic bloqué par le pare-feu à titre préventif avant que tout système puisse être compromis, comme le fait de bloquer une application non autorisée, et le trafic bloqué par le pare-feu après un incident de compromission, par exemple la tentative par un programme malveillant déjà présent dans le centre de données de contacter un serveur externe pour télécharger d'autres programmes malveillants ou d'exfiltrer des données.

Le pare-feu propose un large éventail d'outils de surveillance, de journaux et de rapports de journaux pour vous permettre d'analyser votre réseau :

- **Monitor (Surveillance)** > **Logs (Journaux)** fournit des journaux de trafics, menaces, User-ID, et de nombreux autres types de journaux, y compris des journaux **Unified (Unifiés)**, qui affichent plusieurs type de journaux sur un même écran pour que vous n'ayez pas à examiner différents types de journaux séparément. Lorsque la synthèse comprend une loupe, vous pouvez cliquer dessus pour creuser dans l'entrée du journal.
- **Monitor (Surveillance)** > **PDF Reports (Rapports au format PDF)** fournit des rapports prédéfinis que vous pouvez consulter et la possibilité de créer des groupes de rapports composés de rapports prédéfinis et personnalisés. Par exemple, vous pouvez examiner l'activité du trafic ou prendre des

mesures de référence pour comprendre l'utilisation de la bande passante et le flux de trafic dans chaque segment du centre de données, par zone ou interface.

- **Monitor (Surveillance)** > **Manage Custom Reports (Gérez les rapports personnalisés)** vous donne la possibilité de créer des rapports personnalisés vous permettant de visualiser les informations concernant des règles de blocage, des règles d'autorisation, ou tout autre sujet d'intérêt.
- **Monitor (Surveillance)** > **Packet Capture (Capture de Paquet)** vous permet de réaliser des captures de paquet de trafic traversant l'interface de gestion du pare-feu et les interfaces du réseau.
- Le Application Command Center (Centre de commande des applications, **ACC**) propose des widgets qui affichent une synthèse interactive et graphique des applications, utilisateurs, URL, menaces, et contenu parcourant le réseau. Par exemple, vous pouvez examiner et évaluer les applications sur le réseau (**ACC** > **Network Activity** > **Application Usage** > **Threats**) pour voir s'il y a des changements dans l'application ou si l'application montre des signes de comportement à risque. Si vous voyez des applications inattendues dans la liste, évaluez comment les gérer.

  Les informations d'ACC peuvent également vous aider à identifier des comptes utilisateurs compromis ainsi que des systèmes hôtes compromis. Analysez les menaces ainsi que les noms d'utilisateur qui y sont associés à l'aide du widget **ACC** > **Network Activity (Activité du réseau)** > **User Activity (Activité utilisateurs)** > **Threats (Menaces)**, puis utilisez les journaux des menaces pour isoler le problème exact.
- Le tableau de bord (**Dashboard**) propose des widgets affichant des informations globales sur le pare-feu et jusqu'aux 10 entrées les plus récentes dans les journaux de menaces, configuration, et système.
- Utilisez Panorama pour surveiller la santé du pare-feu et comparez les mesures de performance avec les nouveaux périphériques, mais aussi pour suivre la performance du pare-feu après un évènement, tel qu'une validation, une mise à jour de logiciel, des mises à jour du contenu, des modifications de règles, ou l'ajout de nouvelles applications, etc. Si la performance s'écarte de la référence d'un périphérique, vous pouvez voir et réparer manuellement ou ouvrir un ticket automatique pour effectuer une enquête.
- Sur Panorama ou sur un pare-feu individuel, utilisez le compteur de correspondances à la règle de politique pour analyser les changements apportés à la base de règles. Par exemple, lorsque vous ajoutez une nouvelle application, avant d'autoriser le trafic de cette application dans le réseau, ajoutez la règle d'autorisation dans la base des règles. Si le trafic atteint la règle et augmente le compteur, cela indique que le trafic correspondant à la règle est peut-être déjà sur le réseau bien que vous n'ayez pas encore activé l'application, ou que vous devez affiner la règle. Un autre exemple consiste à remplacer les règles basées sur les ports par des règles basées sur les applications en plaçant la règle basée sur les applications avant la règle basée sur les ports et en notant si du trafic atteint la règle basée sur les ports. Si du trafic atteint la règle basée sur les ports, vous devez alors affiner la règle basée sur les applications pour saisir ce trafic.

  À l'aide du compteur de connexion pour les règles de politique, vérifiez le widget **ACC** > **Threat Activity (Activité de menace)** > **Applications Using Non Standard Ports (Applications utilisant des ports non standard)** et le widget **ACC** > **Threat Activity (Activité de menace)** > **Rules Allowing Apps On Non Standard Ports (Règles autorisant des applications sur des ports non standard)** pour voir si le trafic sur des ports non standard peut avoir causé la connexion avec la règle.

  La secret pour tirer parti du compteur de connexion pour les règles de politique est de réinitialiser le compteur à chaque modification, comme le fait d'introduire une nouvelle application ou de modifier le sens d'une règle. Réinitialiser le compteur vous permet de voir le résultat de la modification elle-même, et non des résultats intégrant les modifications et les événements survenus avant la modification.

Surveillance des règles de blocage pour le centre de données et affinage de la base de règles

Développer une politique de sécurité respectant les meilleures pratiques est un processus itératif. Dès que vous créez des règles de blocage du trafic pour le centre de données, commencez à surveiller le trafic correspondant aux règles de blocage conçues pour identifier les lacunes dans la politique, les comportements inattendus, ainsi que les attaques potentielles. Affinez vos règles d'autorisation pour les applications pour prendre en compte le trafic qui correspond aux règles de blocage mais qui doivent être autorisées, et enquêtez sur le trafic qui pourrait indiquer une attaque.

Les rapports sur le trafic bloqué contiennent des informations précieuses que vous pouvez utiliser pour enquêter sur de potentiels problèmes. Conservez les règles de blocage dans la base de règles pour protéger les précieux actifs de votre centre de données et fournissez ces informations lorsque le trafic correspond à une règle de blocage.

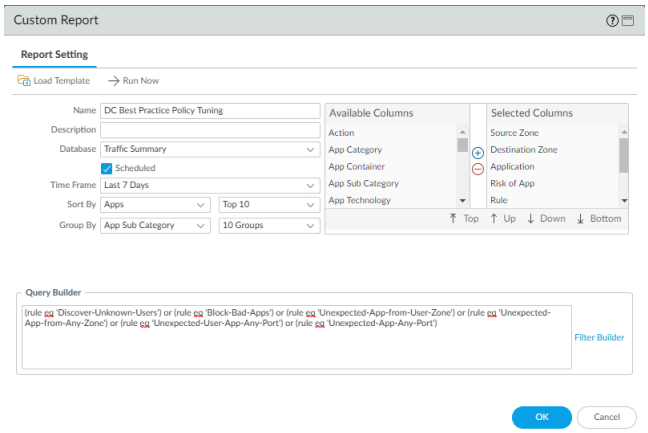
Suivez les meilleures pratiques de mise à jour du contenu pour maintenir votre protection par pare-feu à jour. La section Maintien de la base de règles du centre de données respectant les meilleures pratiques comprend des pratiques exemplaires spécifiques pour les pare-feu du centre de données.

STEP 1 | Créez des rapports personnalisés pour surveiller le trafic qui correspond aux règles de blocage conçues pour identifier les lacunes des politiques et les attaques potentielles.

1. Sélectionnez **Monitor (Surveillance)** > **Manage Custom Reports (Gérer les rapports personnalisés)**.
2. **Add (Ajoutez)** un rapport et donnez-lui un **Name (Nom)** décrivant l'objectif du rapport, dans cet exemple **DC Best Practice Policy Tuning (Affinage de la politique du centre de données respectant les meilleures pratiques)**.
3. Définissez la **Database (Base de données)** sur **Traffic Summary (Récapitulatifs du trafic)**. Cela modifie également les options des **Available Columns** (Colonnes disponibles).
4. Dans **Available Columns** (Colonnes disponibles), ajoutez une **Source Zone** (Zone source), une **Destination Zone** (Zone de destination), des **Sessions**, des **Bytes** (Octets), une **Application**, un **Risk of App** (Risque d'application, une **Rule** (Règle) et une **Threat** (Menace) à la liste de **Selected Columns** (Colonnes sélectionnées. S'il existe d'autres types d'informations que vous souhaitez surveiller, sélectionnez-les également.
5. Cochez la case **Scheduled (Planifié)**.
6. Définissez les valeurs souhaitées (**Time Frame [Délai d'exécution]**, **Sort By [Trier par]** et **Group By [Regrouper par]**). Dans cet exemple, nous configurons le champ **Time Frame** (Intervalle de temps) sur **Last 7 Days** (7 derniers jours), le champ **Sort By** (Trier par) sur **Apps** (Applications) et le champ **Group By** (Regrouper par) sur **App Sub Category** (Sous catégorie d'application).
7. Définissez la requête pour faire correspondre le trafic répondant aux règles conçues pour détecter les lacunes des politiques et les attaques potentielles. Vous pouvez créer un seul rapport pour le trafic correspondant à l'une ou l'autre de ces règles à l'aide de l'opérateur **or (ou)**, ou créer des rapports individuels pour surveiller chaque règle. Dans le **Générateur de requêtes**, spécifiez le nom de chaque règle que vous souhaitez inclure dans le rapport. Cet exemple utilise les six règles de blocage

et utilise l'opérateur **Or (Ou)** pour inclure des informations sur le trafic correspondant à l'une ou l'autre des règles suivantes :

- **(rule eq 'Discover-Unknown-Users') (découverte d'utilisateurs inconnus)**
- **(rule eq 'Block-Bad-Apps') (blocage des mauvaises applications)**
- **(rule eq 'Unexpected-App-from-User-Zone') (application inattendue de la zone utilisateur)**
- **(rule eq 'Unexpected-App-from-Any-Zone') (application inattendue de n'importe quelle zone)**
- **(rule eq 'Unexpected-User-App-Any-Port') (application utilisateur inattendue de n'importe quel port)**
- **(rule eq 'Unexpected-App-Any-Port') (application inattendue de n'importe quel port)**



STEP 2 | Consultez régulièrement le ou les rapports pour vous assurer que vous comprenez pourquoi le trafic correspond à chaque règle de blocage et mettez à jour la politique pour inclure les applications et utilisateurs légitimes, ou utilisez les informations pour évaluer le risque de trafic correspondant aux règles.

Journalisation du trafic au sein du centre de données correspondant à la règle d'autorisation de l'intrazone

Par défaut, l'ensemble du trafic intrazone (dont source et destination sont dans la même zone) est autorisé. Une fois que le pare-feu a évalué la politique de sécurité, il autorise le trafic contrôlé par les règles d'autorisation pour les applications, et il refuse le trafic contrôlé par les règles de blocage, ou, si le trafic intrazone ne correspond à aucune règle, le pare-feu l'autorise par défaut. (Le pare-feu bloque le trafic interzone par défaut.) En raison de la grande valeur des ressources du centre de données, la meilleure pratique consiste à surveiller l'ensemble du trafic au sein du centre de données, entre serveurs du centre de données, y compris le trafic autorisé par la règle d'autorisation par défaut.

Pour obtenir de la visibilité sur le trafic, activez la journalisation dans la règle par défaut de l'intrazone quand elle s'applique au trafic au sein de zones, à l'intérieur du centre de données. Enregistrer ce trafic vous donne la possibilité d'examiner tout accès que vous n'avez pas explicitement autorisé et que vous

pouvez vouloir explicitement autoriser en modifiant une règle d'autorisation pour les applications, ou la bloquer explicitement.

Dans la section Définition de la politique de sécurité initiale du trafic au sein du centre de données, nous avons utilisé trois zones exemples au sein du centre de données : Web-Server-Tier-DC, App-Server-Tier-DC et DB-Server-Tier-DC. Dans cet exemple, nous créons un rapport personnalisé pour recueillir des informations des journaux sur le trafic intra-zone du centre de données dans ces trois zones internes du centre de données.

STEP 1 | Sélectionnez la ligne des règles de base correspondant à l'intrazone par défaut et cliquez sur **Override (Appliquer un contrôle prioritaire)** pour permettre la modification de la règle.

STEP 2 | Sélectionnez le nom de la règle d'**intrazone-default (interzone par défaut)** pour ouvrir la règle aux fins de modification.

STEP 3 | Dans l'onglet Actions, sélectionnez **Log at Session End (Journaliser en fin de session)** et cliquez sur **OK**.

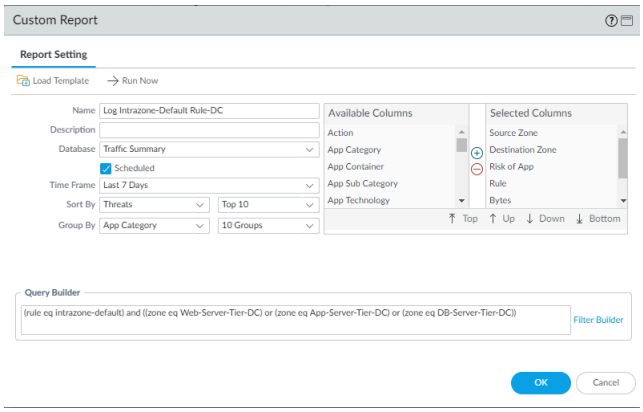
STEP 4 | Créez un rapport personnalisé pour surveiller le trafic qui respecte cette règle pour les zones internes du centre de données.

1. Sélectionnez **Monitor (Surveillance)** > **Manage Custom Reports (Gérer les rapports personnalisés)**.
2. **Add (Ajoutez)** un rapport et donnez-lui un **Name (Nom)** descriptif. Dans cet exemple, le nom est **Log Intrazone-Default Rule-DC (Journal intra-zone-Règle par défaut)**.
3. Définissez la **Database (Base de données)** sur **Traffic Summary (Récapitulatifs du trafic)**.
4. Dans **Available Columns** (Colonnes disponibles), ajoutez une **Source Zone** (Zone source), une **Destination Zone** (Zone de destination), des **Sessions**, des **Bytes** (Octets), une **Application**, un **Risk of App** (Risque d'application, une **Rule** (Règle) et une **Threat** (Menace) à la liste de **Selected Columns** (Colonnes sélectionnées. S'il existe d'autres types d'informations que vous souhaitez surveiller, sélectionnez-les également.
5. Cochez la case **Scheduled (Planifié)**.
6. Définissez les valeurs souhaitées **Time Frame (Délai d'exécution)**, **Sort By (Trier par)** et **Group By (Regrouper par)**. Dans cet exemple, les valeurs sélectionnées sont respectivement **Threats (Menaces)** et **App Category (Catégorie d'application)**.
7. Définissez la requête pour faire correspondre le trafic à la règle intra-zone par défaut dans les zones du centre de données :

```
(rule eq intrazone-default) et ((zone eq Web-Server-Tier-DC) ou
 (zone eq App-Server-Tier-DC) ou (zone eq DB-Server-Tier-DC))
```

La requête filtre le trafic correspondant à la règle par défaut de l'interzone et correspondant également à une des trois zones internes du centre de données que nous avons définies. Étant donné que les **colonnes sélectionnées** par défaut incluent les zones, le rapport affiche la zone pour chaque

session. Dans un centre de données réel, vous auriez probablement plus de zones et ajouteriez chaque zone à la requête. Les paramètres du rapport personnalisé résultants ressemblent à ceci :



8. **Commit (Validez)** les modifications.

Journalisation du trafic du centre de données ne correspondant à aucune règle d'autorisation de l'interzone

Le trafic qui ne correspond à aucune des règles de politique de sécurité que vous définissez est mis en correspondance avec la règle de blocage interzone par défaut prédéfinie au bas des règles de base, et se trouve bloquée. Pour obtenir de la visibilité sur le trafic ne correspondant à aucune règle que vous configuré explicitement, activez journaliser dans la règle par défaut de l'interzone. Enregistrer le trafic vous donne la possibilité d'examiner les tentatives d'accès que vous n'avez pas explicitement autorisées, ce qui peut vous permettre d'identifier les tentatives d'attaques, ou du trafic que vous voulez autoriser pour lequel vous voulez modifier une règle d'autorisation.

STEP 1 | Sélectionnez la ligne des règles de base correspondant à l'interzone par défaut et cliquez sur **Override (Appliquer un contrôle prioritaire)** pour permettre la modification de la règle.

STEP 2 | Sélectionnez le nom de la règle d'**interzone-default (interzone par défaut)** pour ouvrir la règle aux fins de modification.

STEP 3 | Dans l'onglet Actions, sélectionnez **Log at Session End (Journaliser en fin de session)** et cliquez sur **OK**.

STEP 4 | Créez un rapport personnalisé pour surveiller le trafic qui atteint cette règle.

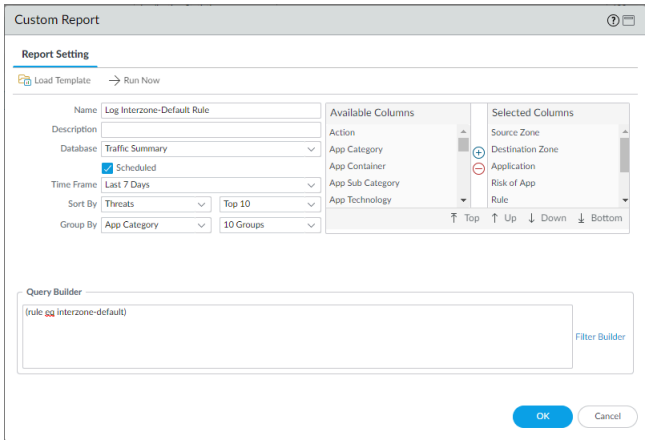
1. Sélectionnez **Monitor (Surveillance)** > **Manage Custom Reports (Gérer les rapports personnalisés)**.
2. **Add (Ajoutez)** un rapport et donnez-lui un **Name (Nom)** descriptif. Dans cet exemple, le nom est **Log Interzone-Default Rule (Journal interzone-Règle par défaut)**.
3. Définissez la **Database (Base de données)** sur **Traffic Summary (Récapitulatifs du trafic)**.
4. Dans **Available Columns** (Colonnes disponibles), ajoutez une **Source Zone** (Zone source), une **Destination Zone** (Zone de destination), des **Sessions**, des **Bytes** (Octets), une **Application**, un **Risk of App** (Risque d'application, une **Rule** (Règle) et une **Threat** (Menace) à la liste de **Selected**

Columns (Colonnes sélectionnées. S'il existe d'autres types d'informations que vous souhaitez surveiller, sélectionnez-les également.

5. Cochez la case **Scheduled (Planifié)**.
6. Définissez les valeurs souhaitées **Time Frame (Délai d'exécution)**, **Sort By (Trier par)** et **Group By (Regrouper par)**. Dans cet exemple, les valeurs sélectionnées sont **Last 7 Days** (7 derniers jours), **Threats** (Menaces) et **App Category** (Catégorie Application), respectivement.
7. Définissez la requête pour faire correspondre le trafic qui correspond à la règle interzone par défaut :

```
(rule eq interzone-default)
```

Les paramètres du rapport personnalisé résultants ressemblent à ceci :



8. **Commit (Validez)** les modifications.

Maintien de la base de règles du centre de données respectant les meilleures pratiques

Les applications sont en constante évolution, votre liste d'autorisation pour les applications doit donc évoluer avec elles. Étant donné que les règles de meilleures pratiques se servent des objets de la politique pour simplifier l'administration, l'ajout de support pour une nouvelle application ou la suppression d'une application de votre liste d'autorisation se traduit généralement par la modification conséquente du groupe d'applications ou du filtre d'application correspondant.

Palo Alto Networks vous fait parvenir des mises à jour de contenu que vous avez tout intérêt à télécharger automatiquement et pour lesquelles vous devez prévoir une installation sur les pare-feu dans les meilleurs délais. La plupart des mises à jour de contenu comprennent des mises à jour concernant les menaces (antivirus, vulnérabilités, anti-logiciels espions, etc.) et peuvent également contenir des App-IDs modifiées. Le troisième mardi de chaque mois, les mises à jour de contenu comprennent également de nouvelles App-IDs. Vous pouvez fixer des seuils différents pour reporter l'installation de mises à jour habituelles de contenu et pour reporter l'installation de mises à jour mensuelles comprenant les nouvelles App-IDs pour une durée déterminée après le téléchargement. Reporter l'installation vous permet d'installer des mises à jour de contenu ne comprenant pas de nouvelles App-IDs aussi rapidement que possible afin de bénéficier des dernières signatures de menaces, tout en fournissant plus de temps pour examiner les nouvelles App-IDs avant de les installer.

Les mises à jour de contenu du troisième mardi de chaque mois comprenant de nouvelles App-IDs peuvent occasionner des modifications dans l'application des politiques de Sécurité. Avant d'installer de nouvelles App-IDs ou des App-IDs modifiées, passez en revue l'impact de la politique, organisez des mises à jour pour tester l'impact, et modifiez des règles de politique de Sécurité existantes si nécessaire. La façon la plus efficace de contrôler le téléchargement et l'installation de mises à jour de contenu sur les pare-feu est de les charger sur Panorama et de les distribuer depuis Panorama si vous l'utilisez.

Suivez les bonnes pratique concernant les mises à jour de contenu, qui aborde le sujet de manière synthétique, mais gardez à l'esprit que la disponibilité du centre de données est généralement très critique, il est donc peut-être préférable de ne pas déployer les mises à jour de contenu aussi rapidement dans le centre de données que vous ne le feriez sur des pare-feu faisant face à Internet :

- Testez rapidement les mises à jour du contenu dans un endroit sûr du réseau avant de les installer dans le centre de données.
- Pour les mises à jour de contenu ne comprenant pas de nouvelles App-IDs, fixez le seuil d'installation à un maximum de huit heures après le téléchargement automatique et conduisez des tests pendant ce laps de temps.
- Pour les mises à jour de contenu comprenant de nouvelles App-IDs, fixez le seuil d'installation à un maximum de huit jours après le téléchargement automatique et conduisez des tests pendant ce laps de temps.
- Configurez le Transfert de Journaux pour toutes les mises à jour de contenu.

STEP 1 | Avant d'installer une nouvelle mise à jour de contenu, revoyez les nouvelles App-IDs et celles modifiées pour déterminer si elles ont un effet sur la politique.

STEP 2 | Si nécessaire, modifiez les règles de politique de Sécurité existantes pour satisfaire aux modifications d'App-ID.

Vous pouvez désactiver les App-IDs sélectionnées si certaines App-IDs exigent plus de tests, et installer le reste des nouvelles App-IDs. Achevez de tester toute révision de politique nécessaire avant l'arrivée de la version de contenu du mois suivant avec les nouvelles App-IDs (le troisième mardi de chaque mois) pour éviter qu'elles ne se chevauchent.

Au fil du temps, la liste d'applications utilisées dans le centre de données parvient généralement à se stabiliser, donc de moins en moins de nouvelles App-IDs sont pertinentes. (La plupart des nouvelles App-IDs appartiennent aux applications communiquant avec Internet.) Cela réduit le risque de problèmes liés à l'apparition de nouvelles App-IDs dans le centre de données et peut vous permettre d'installer des mises à jour de contenu comprenant de nouvelles App-IDs plus rapidement.

STEP 3 | Préparez des mises à jour de politique afin de tenir compte des changements d'App-ID compris dans une version de contenu ou pour ajouter de nouvelles applications autorisées à vos règles relatives à la liste des applications de confiance ou pour en supprimer de ces règles.

Liste d'autres moyen de conserver une base de règles respectant les meilleures pratiques :

- Utilisez les outils d'évaluation et d'examen de Palo Alto Networks afin d'identifier les vides dans la couverture de sécurité.
- Les retours des utilisateurs concernant les applications auxquelles ils ne peuvent plus accéder peuvent vous permettre d'identifier les lacunes dans la base de règles ainsi que les applications à risque utilisées avant qu'un renforcement positif n'empêche leur utilisation.
- Comparez l'inventaire de ressources que vous avez dressé lorsque vous avez évalué votre centre de données aux ressources elles-mêmes pour vous assurer que ces ressources sont protégées correctement.
- Utilisez les outils de journalisation et de surveillance de Palo Alto Networks tels que le Centre de Commande de l'Application (ACC) pour trouver et enquêter sur une activité inattendue, qui pourrait être le signe d'une règle mal configurée ou manquante. Exécutez régulièrement des rapports afin de vérifier que le niveau de sécurité souhaité est bien appliqué.

Si vous gérez des pare-feu avec Panorama, vous pouvez surveiller la santé des pare-feu pour comparer les périphériques par rapport à leur rendement de base et entre eux, pour identifier les écarts par rapport à leur comportement normal.

Utilisez les Outils d'Évaluation et d'Examen de Palo Alto Networks

L'équipe au service de la réussite des clients chez Palo Alto Networks a mis au point une architecture de prévention, accompagnée d'outils et de ressources vous permettant d'évaluer et d'examiner les risques pour la sécurité de votre réseau, ainsi que votre capacité à utiliser le pare-feu et les autres outils pour sécuriser votre réseau. Contactez votre représentant Palo Alto Networks pour programmer les évaluations et examens (un ingénieur commercial de Palo Alto Networks mène les études pour vous fournir son expertise sur l'état du dispositif de sécurité de votre réseau). À la date de la publication de ce document, les outils disponibles de prévention des risques pour la sécurité comprennent :

- **Examen de posture de prévention (PPA)** : le PPA est un ensemble de questionnaires qui vous permet de révéler les lacunes dans votre prévention des risques pour la sécurité à travers toutes les régions de votre réseau et dans votre architecture de sécurité. Le PPA aide non seulement à identifier tous les risques de sécurité, mais il fournit également des suggestions détaillées sur la manière de prévenir les risques et de combler les lacunes. L'examen, mené par un ingénieur commercial expérimenté de Palo Alto Networks, vous permet de déterminer les régions présentant les risques les plus grands et les endroits où vous devriez concentrer vos activités de prévention. Vous pouvez exécuter le PPA sur les pare-feu et sur Panorama.
- **Outil d'examen des meilleures pratiques (BPA)** : le BPA destiné aux pare-feu nouvelle génération et à Panorama évalue la configuration d'un périphérique en mesurant l'adoption des fonctionnalités, en validant si les politiques respectent les meilleures pratiques et en proposant des recommandations et des instructions sur la façon de remédier aux pratiques ayant échoué à être exemplaires.

  Le composant Security Policy Adoption Heatmap (Carte thermique d'adoption des politiques de sécurité) filtre les informations par groupes de périphériques, numéros de série, zones, régions d'architecture, et autres catégories. Les résultats contiennent des données sur les tendances, et montrent le taux d'amélioration de votre sécurité au fur et à mesure que vous adoptez de nouvelles fonctionnalités, que vous comblez les lacunes, et que vous vous rapprochez d'un réseau Zéro Confiance.

  Le composant BPA effectue plus de 200 contrôles de sécurité sur une configuration de pare-feu ou Panorama et fournit un score de réussite/échec pour chaque vérification. Chaque vérification est une meilleure pratique identifiée par les experts en sécurité de Palo Alto Networks. Lorsqu'une vérification renvoie une mauvaise note, l'outil apporte une explication à la mauvaise note et explique comment résoudre le problème.

Palo Alto Networks est constamment en train de développer de nouveaux outils et d'affiner ses outils existants. Contactez votre représentant Palo Alto Networks pour découvrir ce que les outils les plus récents peuvent faire pour renforcer la sécurité du réseau de votre centre de données.