paloalto TECHDOCS

Meilleures pratiques des politiques de sécurité des passerelles Internet

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

July 24, 2023

Table of Contents

Meilleures pratiques des politiques de sécurité des passerelles Internet

Une façon facile et économique pour un pirate d'obtenir accès à votre réseau est de passer par les utilisateurs qui accèdent à l'Internet. En réussissant à exploiter un terminal, un pirate peut pénétrer dans votre réseau et se déplacer latéralement jusqu'à atteindre l'objectif initial : voler le code source, exfiltrer les données sur vos clients ou faire tomber l'infrastructure. Pour protéger votre réseau contre les cyberattaques et améliorer votre niveau de sécurité global, vous n'avez qu'à mettre en œuvre une politique de sécurité des passerelles Internet exemplaire. Une telle politique vous permet de prendre en charge les applications, les utilisateurs et les contenus, en toute sécurité, en contrôlant systématiquement l'ensemble du trafic sur tous les ports.

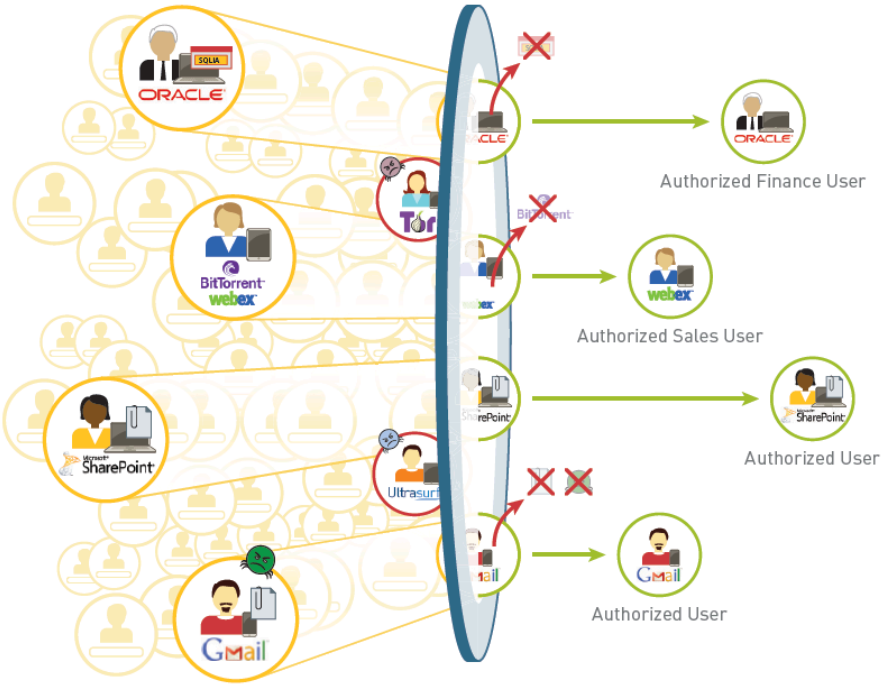
Reportez-vous à la série de livres sur les meilleures pratiques de Palo Alto Networks pour obtenir des conseils sur les meilleures pratiques sur des sujets tels que le décryptage, le DoS et la protection de zone (y compris la protection de la mémoire tampon des paquets), et bien plus encore.

Qu’est-ce qu’une meilleure pratique de la politique de sécurité des passerelles Internet ?

Une politique de sécurité des passerelles Internet exemplaire possède deux objectifs principaux en matière de sécurité :

- **Minimiser les chances de réussite d’une intrusion** : contrairement aux anciennes politiques de sécurité basées sur le port, qui bloquent tout, dans l’intérêt de la sécurité réseau, ou qui activent tout, dans l’intérêt de votre entreprise, une politique de sécurité exemplaire tire profit de App-ID, de User-ID, de Content-ID et de Device-ID (pour IoT Security, qui dépasse le cadre de ce livre) pour garantir la mise en œuvre sécuritaire des applications sur tous les ports, pour tous les utilisateurs, en tout temps, tout en analysant tout le trafic à la recherche de menaces connues et inconnues.
- **Reconnaître la présence d’un pirate** : une politique de sécurité des passerelles Internet exemplaire fournit des mécanismes intégrés qui vous aident à identifier les lacunes de la base de règles et à détecter les activités alarmantes et les menaces éventuelles sur votre réseau.

Pour atteindre ces objectifs, la politique de sécurité des passerelles Internet exemplaire se sert de règles basées sur les applications pour autoriser l’accès, par utilisateur, aux applications spécifiques, tout en analysant l’ensemble du trafic afin d’y détecter et de bloquer toutes les menaces connues et d’envoyer les fichiers inconnus à WildFire pour identifier de nouvelles menaces et générer des signatures pour les bloquer :



La politique exemplaire garantit la détection et la prévention à plusieurs étapes du cycle des attaques.

Méthodologie exemplaire	Pourquoi est-ce important ?
Inspecter tout le trafic pour obtenir une visibilité	Parce que vous ne pouvez vous protéger contre les menaces que vous ne voyez pas, assurez-vous d'avoir, en tout temps, une visibilité complète de tout le trafic de tous les utilisateurs et de toutes les applications : • Déployez GlobalProtect de sorte à étendre la plateforme de sécurité de nouvelle génération aux utilisateurs et aux périphériques où qu'ils se trouvent. • Activez le décryptage afin que le pare-feu puisse inspecter le trafic crypté (chaque année, un nombre plus élevé de trafics web d'entreprise est crypté et de plus en plus de campagnes de logiciels malveillants utilisent le cryptage). • Activez User-ID afin de mapper le trafic des applications et les menaces associées aux utilisateurs/périphériques et de permettre à la politique de suivre les utilisateurs où qu'ils aillent. • Si la politique d'entreprise autorise les périphériques des utilisateurs à accéder au réseau (BYOD ou périphériques d'entreprise sans GlobalProtect ou d'autres applications de gestion de la sécurité), le contrôle d'accès aux périphériques non gérés sur l'API de sécurité SaaS permet aux utilisateurs d'accéder à vos applications SaaS dans le cloud à partir de périphériques personnels, peu importe leur emplacement, sans mettre vos données ou votre organisation à risque. Le trafic est redirigé via le pare-feu à des fins d'application de la politique et de prévention des menaces. Avec une visibilité totale, grâce aux technologies App-ID, Content-ID et User-ID natives, le pare-feu peut alors inspecter tout le trafic, y compris celui des applications, des menaces et du contenu, et l'associer à l'utilisateur, peu importe l'emplacement ou le type de périphérique, le port, le cryptage ou les techniques évasives utilisées. La première étape vers un contrôle informé des politiques est atteinte par l'obtention d'une visibilité complète sur les applications, les contenus et les utilisateurs de votre réseau.
Réduire la surface d'attaque	Après avoir pris connaissance du contexte des applications, du contenu et des utilisateurs sur votre réseau, créez des règles de sécurité basées sur les applications afin d'autoriser les applications professionnelles essentielles et de bloquer les applications à haut risque qui n'ont pas de légitimité professionnelle. Afin de réduire davantage votre surface d'attaque, associez les profils de blocage des fichiers et de URL Filtering à toutes les règles qui autorisent le trafic d'application d'empêcher les utilisateurs de consulter des sites web susceptibles d'être dangereux et de charger ou de télécharger des types de fichiers dangereux (consciemment ou à leur insu). Pour empêcher les pirates de mener à bien des attaques d'hameçonnage, configurez la prévention contre l'hameçonnage de données d'identification.

Méthodologie exemplaire	Pourquoi est-ce important ?
Empêchez les Menaces Connues	Associez des profils de sécurité à toutes les règles d'autorisation afin que le pare-feu puisse détecter et bloquer les exploitations de vulnérabilité des couches d'application et réseau, variantes de logiciels malveillants, les dépassements de capacité de la mémoire tampon, les attaques DoS et le balayage des ports, les variantes de logiciels malveillants connues (dont ceux dissimulés dans les fichiers compressés ou le trafic Web HTTP/ HTTPS compressé). Pour permettre l'inspection du trafic crypté, activez le décryptage SSL. En plus des règles de politique de sécurité basées sur les applications, créez des règles pour bloquer les adresses IP malveillantes connues en fonction des renseignements sur les menaces fournis par Palo Alto Networks et les sources tierces de confiance.
Détection des menaces inconnues	Transférez tous les fichiers inconnus vers WildFire à des fins d'analyse. WildFire identifie les logiciels malveillants inconnus ou ciblés (également appelés *advanced persistent threats*, *menaces persistantes avancées* ou *APT*) dissimulés dans des fichiers en observant directement et exécutant les fichiers inconnus dans un environnement virtuel basé sur le cloud ou sur l'appareil WildFire. Si WildFire détecte un logiciel malveillant, il développe automatiquement une signature et peut vous la transmettre en temps réel ou à un intervalle de temps de votre choix.

Pourquoi ai-je besoin d’une politique de sécurité des passerelles Internet exemplaire ?

Une politique de sécurité exemplaire vous permet d’activer les applications en toute sécurité en classifiant tout le trafic, sur tous les ports, à tout moment, y compris le trafic crypté. Déterminez l’utilisation commerciale de chaque application pour créer des règles de politique de sécurité visant à autoriser et à protéger les applications pertinentes. Une politique de sécurité exemplaire exploite les technologies de nouvelle génération (App-ID, Content-ID, User-ID et Device-ID (pour IoT Security, qui dépasse le cadre de ce livre)) sur la plateforme de sécurité d’entreprise Palo Alto Networks et :

- Identifie les applications, peu importe le port, le protocole, la tactique d’évasion ou le cryptage
- Identifie et contrôle les utilisateurs indépendamment de l’adresse IP, de l’emplacement ou de l’appareil.
- Protège contre les menaces connues et inconnues issues des applications.
- Offre une parfaite visibilité et un contrôle granulaire de l’accès aux applications et de leurs fonctionnalités.
- Suit les meilleures pratiques d’IoT Security si vous disposez d’un déploiement IoT.

Une politique de sécurité exemplaire se sert d’une approche en couche pour garantir que vous autorisez, en toute sécurité, les applications approuvées et que vous bloquez également les applications qui n’ont aucune utilité légitime. Pour atténuer le risque que des applications cessent de fonctionner lors du passage d’une mise en application basée sur les ports à une mise en application basée sur les applications, la base de règles exemplaire comprend des règles de politique de sécurité temporaires qui identifient les lacunes de la base de règles, détectent les activités alarmantes et les menaces potentielles, garantissent que les applications ne sont pas interrompues pendant la transition et vous permettent de surveiller l’utilisation des applications afin d’élaborer des règles appropriées. Certaines applications autorisées par une ancienne politique basée sur les ports peuvent être des applications que vous ne souhaitez pas autoriser ou que vous souhaitez limiter à un ensemble plus granulaire d’utilisateurs.

Une politique de sécurité exemplaire est plus facile à administrer et à poursuivre, car chaque règle répond à un objectif commercial spécifique et autorise l’accès à une application ou à un groupe d’applications pour un ou plusieurs groupes d’utilisateurs spécifiques. Les critères de correspondance entre l’application et l’utilisateur de chaque règle facilitent la compréhension du trafic imposé par la règle. Une base de règles de politique de sécurité exemplaire tire également profit des marquages et des objets pour en faciliter l’analyse et la synchronisation avec votre environnement en constante évolution.

Comment puis-je déployer une politique de sécurité des passerelles Internet exemplaire ?

L'objectif est d'élaborer une politique de sécurité exemplaire et basée sur les applications, qui s'aligne sur les objectifs de l'entreprise et les politiques d'utilisation acceptable, simplifie l'administration, réduit les risques d'erreur et applique les principes de Zero Trust à l'accès au réseau.

Comme pour toute technologie, la mise en œuvre complète se fait généralement de manière progressive. Planifiez soigneusement les phases de déploiement pour que la transition se fasse en douceur et que l'impact sur les utilisateurs finaux soit le plus faible possible. En général, le flux de travail pour la mise en œuvre d'une politique de sécurité des passerelles Internet exemplaire est le suivant :

- **Évaluez votre entreprise et identifiez ce que vous devez protéger** : la première étape du déploiement d'une architecture de sécurité consiste à évaluer votre entreprise. Identifiez vos actifs les plus précieux et les plus grandes menaces qui pèsent sur ces actifs. Par exemple, si vous êtes une entreprise technologique, votre propriété intellectuelle est votre ressource la plus précieuse. Dans ce cas, l'une des plus grandes menaces est le vol du code source.
- Segmentation de votre réseau via les interfaces et les zones : le trafic ne peut circuler d'une zone à l'autre que si une règle de sécurité l'autorise. Pour empêcher un pirate ayant accédé à votre réseau de se déplacer latéralement à travers le réseau, il convient de définir des zones granulaires et de n'autoriser l'accès qu'aux groupes d'utilisateurs spécifiques qui ont besoin d'accéder à une application ou à une ressource dans chaque zone. En segmentant votre réseau en zones granulaires, vous empêchez un pirate d'établir un canal de communication au sein de votre réseau (que ce soit par l'intermédiaire d'un logiciel malveillant ou d'applications légitimes), ce qui réduit la probabilité qu'une attaque réussisse.
- Identifiez votre liste de confiance pour les applications : avant de pouvoir créer une politique de sécurité des passerelles Internet exemplaire, créez un inventaire des applications que vous souhaitez autoriser sur votre réseau. Dressez une liste séparée des applications que vous administrez, que vous approuvez officiellement à des fins professionnelles et dont vous tolérez l'utilisation par vos employés. Après avoir identifié les applications que vous souhaitez autoriser, si vous migrez à partir d'une base de règles basée sur les ports, mappez les applications à vos règles basées sur les ports. Si aucune application n'est mappée à une règle basée sur les ports, il se peut que vous n'ayez pas besoin de cette règle.
- Création de groupes d'utilisateurs pour l'accès aux applications de confiance : une fois que vous avez déterminé les applications que vous prévoyez autoriser, établissez les groupes d'utilisateurs qui ont besoin d'accéder à chacune d'entre elles. Compromettre le système d'un utilisateur final est l'un des moyens les moins coûteux et les plus faciles pour un pirate d'accéder à votre réseau. Pour réduire considérablement votre surface d'attaque, n'autorisez l'accès aux applications qu'aux groupes d'utilisateurs ayant un besoin professionnel légitime.
- Décryptage du trafic pour une visibilité complète et pour l'inspection des menaces : vous ne pouvez pas protéger votre réseau contre les menaces que vous ne pouvez pas voir et inspecter. Le trafic crypté est un moyen courant pour les attaquants de diffuser des menaces. Par exemple, un pirate pourrait utiliser une application Web comme Gmail, qui utilise le cryptage TSL, pour envoyer, par courriel, une exploitation ou un fichier malveillant aux employés qui accèdent à cette application sur le réseau d'entreprise. Ou, un pirate, pourrait corrompre un site web qui utilise le cryptage TLS pour que les visiteurs y téléchargent silencieusement une exploitation ou un fichier malveillant.
- Création de profils de sécurité exemplaires pour la passerelle Internet : les applications légitimes fournissent du trafic de commande et de contrôle, des CVE, des téléchargements automatiques de contenus malveillants, des attaques d'hameçonnage et des APT. Pour vous protéger contre les menaces

connues et inconnues, associez des profils de sécurité stricts à toutes les règles de politique de sécurité qui autorisent le trafic.

- Définition de la politique de sécurité initiale des passerelles Internet : à l'aide de l'inventaire des groupes d'utilisateurs et d'applications que vous avez effectué, définissez une politique initiale qui autorise l'accès aux applications par utilisateur ou groupe d'utilisateurs. La base de règles de politique initiale comprend également des règles pour bloquer les adresses IP malveillantes connues ainsi que des règles temporaires pour empêcher d'autres applications, dont vous n'aviez peut-être pas connaissance, de s'interrompre et pour déceler les lacunes des politiques et les failles de sécurité de votre conception actuelle.
- Surveillance et peaufinage des règles de base de la politique : une fois que les règles temporaires sont en place, surveillez le trafic qui leur correspond afin de pouvoir affiner votre politique. Puisque les règles temporaires sont conçues pour découvrir le trafic imprévu sur le réseau, comme le trafic qui s'exécute sur des ports autres que ceux définis par défaut ou le trafic d'utilisateurs inconnus, vous devez évaluer le trafic qui correspond à ces règles et ajuster vos règles d'autorisation des applications en conséquence.
- Suppression des règles temporaires : à l'issue d'une période de surveillance de plusieurs mois, vous devriez voir de moins en moins de trafic atteindre les règles temporaires. Lorsque vous arrivez au point où le trafic n'atteint plus les règles temporaires, supprimez-les et achevez votre politique de sécurité des passerelles Internet exemplaire.
- Maintien de la base de règles : en raison de la nature dynamique des applications, vous devez continuellement surveiller votre liste des applications de confiance et adapter vos règles afin de tenir compte des nouvelles applications ainsi que de déterminer l'effet que les App-ID nouveaux ou modifiés ont sur votre politique. Étant donné que les règles d'une base de règles exemplaire cadrent avec vos objectifs professionnels et tirent parti des objets de la politique pour en simplifier l'administration, bien souvent l'ajout de soutien pour une nouvelle application autorisée ou un App-ID nouveau ou modifié est aussi simple que d'ajouter ou de retirer une application d'un groupe d'applications ou de modifier un filtre d'application.

Identifiez votre liste de confiance pour les applications

La liste des applications autorisées comprend les applications approuvées que vous fournissez et administrez pour les besoins de l'entreprise, de l'infrastructure et du travail des utilisateurs, ainsi que les applications tolérées que vous choisissez d'autoriser pour un usage personnel. Avant d'élaborer votre politique de sécurité pour la passerelle Internet, faites l'inventaire des applications que vous souhaitez autoriser.

- Mappage des applications aux objectifs d'entreprise pour obtenir une base de règles simplifiée
- Utilisez des règles temporaires pour affiner la liste de confiance
- Exemple de liste de confiance pour les applications

Mappage des applications aux objectifs d'entreprise pour obtenir une base de règles simplifiée

Tandis que vous dressez l'inventaire des applications présentes sur votre réseau, tenez compte de vos objectifs d'entreprise et des politiques d'utilisation acceptable et déterminez les applications qui leur correspondent. Cela vous permet de créer une base de règles axée sur les objectifs. Par exemple, un objectif commercial pourrait être d'autoriser les groupes des ventes et du soutien à accéder à la base de données de vos clients. Créez une règle d'autorisation des applications qui correspond à chaque objectif et regroupez toutes les applications qui cadrent avec l'objectif en une seule règle. Cette approche vous permet de créer une base de règles avec un nombre réduit de règles individuelles et chaque règle a un objectif clair.

Puisque les règles individuelles que vous créez correspondent à vos objectifs d'entreprise, vous pouvez utiliser les objets d'applications pour regrouper les applications de confiance en vue de simplifier davantage l'administration de la base de règles :

- Créer des groupes d'applications pour chaque ensemble d'applications autorisées : créez des groupes d'applications qui n'incluent explicitement que des ensembles d'applications approuvées. Les groupes d'applications simplifient l'administration de votre politique, car ils vous permettent d'ajouter et de supprimer des applications approuvées sans modifier les règles individuelles de la politique de sécurité. Généralement, si les applications qui sont mappées au même objectif ont les mêmes exigences en matière d'accès (par exemple, elles ont toutes une adresse de destination qui pointe vers Internet, elles autorisent toutes l'accès à n'importe quel utilisateur connu et vous voulez les activer uniquement sur leurs ports par défaut), vous les ajoutez au même groupe d'applications.

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

- Créer un filtre d'application pour autoriser chaque type d'application générale : outre les applications que vous approuvez officiellement, vous devez déterminer les applications supplémentaires auxquelles vous souhaitez autoriser les utilisateurs à accéder. Les filtres d'applications vous permettent d'autoriser, en toute sécurité, certaines catégories d'applications selon les marquages, la catégorie, la sous-catégorie, la technologie, le facteur de risque ou la caractéristique. Divisez les divers types d'applications selon l'utilisation professionnelle ou personnelle. Créez des filtres distincts pour chaque type d'applications afin de mieux comprendre chaque règle de politique.

Utilisez des règles temporaires pour affiner la liste de confiance

L'objectif final de la politique de sécurité basée sur les applications est d'autoriser explicitement le trafic des applications que vous souhaitez autoriser et de refuser implicitement le trafic que vous ne souhaitez pas. Toutefois, la base de règles initiale nécessite des règles temporaires, qui garantissent que vous disposez d'une visibilité complète sur toutes les applications de votre réseau afin que vous puissiez ajuster correctement la stratégie. La base de règles initiale a besoin des types de règles suivants :

- Des règles d'autorisation pour les applications que vous approuvez et déployez à des fins professionnelles.
- Des règles d'autorisation pour permettre l'accès, en toute sécurité, aux applications tolérées que vous souhaitez autoriser conformément à votre politique d'utilisation acceptable.
- Des règles de blocage qui bloquent les applications qui n'ont pas d'utilisation légitime. Ces règles empêchent le trafic malveillant d'entrer dans votre réseau, tandis que les règles temporaires détectent les applications que votre base de règles de politique ne prend pas encore en compte.
- Des règles d'autorisation temporaires qui vous procurent une visibilité de toutes les applications qui s'exécutent sur votre réseau afin que vous puissiez affiner votre base de règles.

Règles temporaires :

- Offrez une visibilité sur les applications dont vous ne soupçonniez pas l'existence sur votre réseau.
- Empêchez les applications légitimes que vous ne connaissiez pas d'être bloquées.
- Identifiez les utilisateurs inconnus, les applications inconnues et les applications exécutées sur des ports non standard (les pirates utilisent généralement des applications standard sur des ports non standard comme technique d'évasion pour les activités malveillantes).

Identifiez les applications légitimes qui s'exécutent sur des ports non standard (par exemple, des applications développées en interne) afin de pouvoir modifier les ports utilisés par l'application ou créer une application propre à l'entreprise à utiliser dans la stratégie.

Si vous avez des règles de politique de contrôle prioritaire sur l'application, créées pour définir des délais d'expiration de session personnalisés pour un ensemble de ports, convertissez ces politiques de contrôle prioritaire sur l'application 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. Migrez ensuite chaque règle vers une règle basée sur l'application. Les politiques de contrôle prioritaire sur l'application sont basées sur les ports et ne fournissent pas de visibilité aux applications sur le trafic. Vous ne savez donc pas quelles applications utilisent les ports, et vous ne pouvez pas 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.

Exemple de liste de confiance pour les applications

Vous n'avez pas à tenir compte de chaque application qui pourrait être utilisée sur votre réseau dans votre inventaire initial. Concentrez-vous plutôt sur les applications que vous souhaitez autoriser. Les règles temporaires interceptent d'autres applications susceptibles de se trouver sur votre réseau. Vous n'êtes donc pas inondé de plaintes liées à des applications défaillantes lors d'une transition vers une politique basée sur les applications. Le tableau suivant présente un exemple de liste d'autorisation des applications pour un déploiement de passerelles d'entreprise.

Type d’application	Recommandation en matière de sécurisation
Applications SaaS	Les fournisseurs de service des applications SaaS possèdent et gèrent le logiciel et l’infrastructure, mais vous conservez le contrôle total des données, et vous décidez notamment des personnes qui peuvent les créer, y accéder, les partager et les transférer. Pour contrôler les applications SaaS, utilisez SaaS Security (abonnement requis). Si vous utilisez la sécurité SaaS, utilisez la recommandation de politique SaaS pour contrôler les applications SaaS sur le pare-feu. Si vous ne disposez pas d’un abonnement SaaS Security, générez un rapport d’utilisation des applications SaaS pour vérifier si les applications SaaS en cours d’utilisation possèdent des caractéristiques d’hébergement non favorables, comme des fuites de données antérieures ou l’absence des certifications appropriées. Selon les besoins de l’entreprise et le risque que vous êtes prêt à assumer, utilisez ces informations pour : • Bloquer immédiatement les applications existantes dont les caractéristiques d’hébergement ne sont pas favorables. • Créer des politiques granulaires qui bloquent les applications comportant des caractéristiques d’hébergement non favorables afin de prévenir de futures violations. • Identifier les tendances du trafic réseau des principales applications qui présentent des caractéristiques d’hébergement non favorables, de sorte à ajuster la politique en conséquence. De nombreuses applications SaaS ont des versions d’entreprise et clientes (personnelles), mais une utilisation sans restriction augmente le risque que des données sensibles quittent votre réseau. L’insertion de l’en-tête HTTP vous permet de contrôler les versions d’applications SaaS que vous autorisez sur votre réseau. Par exemple, vous pouvez autoriser la version entreprise de Box ou Office 365 et bloquer les versions grand public. L’insertion de l’en-tête HTTP réduit la surface d’attaque en autorisant uniquement la version de chaque application SaaS que vous souhaitez approuver ou tolérer pour l’usage personnel de vos utilisateurs.
Applications autorisées	Il s’agit des applications que votre service des TI gère spécialement à des fins professionnelles au sein de votre organisation ou afin de fournir l’infrastructure nécessaire pour votre réseau et vos applications. Par exemple, dans un déploiement de passerelles Internet, ces applications se rangent dans les catégories suivantes : • **Applications d’infrastructure** : applications que vous devez autoriser pour permettre la mise en réseau et la sécurité, comme ping, NTP, SMTP et DNS. • **Applications autorisées par les TI** : applications que vous obtenez et gérez pour vos utilisateurs. Elles se répartissent en deux catégories : • **Applications sur site autorisées par les TI** : applications que vous installez et hébergez dans votre centre de données à des fins professionnelles. Lorsque vous disposez d’applications sur site autorisées par les TI, l’infrastructure et les données de l’application reposent sur de

Type d’application	Recommandation en matière de sécurisation
	l’équipement appartenant à l’entreprise. Il s’agit notamment de Microsoft Exchange et de ActiveSync ainsi que des outils d’authentification, comme Kerberos et LDAP. • **Applications SaaS approuvées par les TI** : applications SaaS que votre service des TI a approuvées à des fins d’affaires, par exemple, Salesforce, Box et GitHub. • **Applications administratives** : applications auxquelles seul un groupe donné d’utilisateurs administrateurs devrait avoir accès en vue de gérer les applications et d’aider les utilisateurs (par exemple, des applications d’accès à des bureaux à distance). 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.
Types d’applications tolérés	En plus des applications que vous approuvez officiellement, vous devez également permettre aux utilisateurs d’accéder en toute sécurité à d’autres types d’applications tolérées : • **Applications professionnelles générales** : par exemple, autorisez l’accès aux mises à jour logicielles pour les applications tolérées et aux services web, tels que WebEx, les services en ligne d’Adobe et Evernote. • **Applications personnelles** : par exemple, vous pourriez autoriser vos utilisateurs à naviguer sur le web ou à utiliser en toute sécurité la messagerie web, la messagerie instantanée ou des applications de mise en réseaux sociaux, dont des versions pour particuliers de certaines applications SaaS. Commencez par des filtres d’applications étendus pour comprendre quelles applications se trouvent sur votre réseau. Décidez du degré de risque que vous êtes prêt à prendre et réduisez la liste d’autorisation pour les applications. Par exemple, de nombreuses applications de messagerie pourraient être utilisées, chacune disposant d’un risque de perte de données, de transfert de fichiers malveillants, etc. La meilleure approche à adopter consiste à approuver une seule application de messagerie, puis à passer lentement d’une politique d’autorisation à une politique d’alerte, et après avoir suffisamment averti les utilisateurs, à une politique de blocage pour éliminer progressivement les autres applications de messagerie. Vous pourriez également choisir d’autoriser un petit groupe d’utilisateurs à continuer d’utiliser d’autres applications de messagerie, au besoin, afin d’accomplir leurs tâches auprès de partenaires.
Applications personnalisées propres à votre environnement	Créez des applications personnalisées pour les applications propriétaires ou les applications que vous exécutez sur des ports non standard. Cela vous permet d’autoriser l’application en tant qu’application autorisée (et appliquer le marquage Approuvé prédéfini) et la restreindre à son port par défaut. Autrement, vous devriez ouvrir des ports supplémentaires (dans le cas d’applications s’exécutant sur des ports non standard) ou autoriser le trafic

Type d’application	Recommandation en matière de sécurisation
	inconnu (dans le cas d’applications exclusives) ; aucune de ces options n’est recommandée dans une politique de sécurité exemplaire. 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. Migrez ensuite chaque règle vers une règle basée sur l’application. Les politiques de contrôle prioritaire sur l’application sont basées sur les ports et ne fournissent pas de visibilité aux applications sur le trafic. Vous ne savez donc pas quelles applications utilisent les ports, et vous ne pouvez pas 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.

Création de groupes d’utilisateurs pour l’accès aux applications de confiance

Autoriser en toute sécurité les applications, ce n’est pas seulement définir la liste des applications que vous souhaitez autoriser, mais également autoriser l’accès uniquement aux utilisateurs qui ont besoin de les utiliser dans le cadre de leurs fonctions. Par exemple, certaines applications, comme les applications SaaS qui autorisent l’accès aux services de Ressources humaines (tels que Workday ou Service Now) doivent être disponibles à tous les utilisateurs connus de votre réseau. Toutefois, pour les applications plus sensibles, réduisez votre surface d’attaque en n’autorisant l’accès qu’aux utilisateurs qui en ont besoin à des fins professionnelles. Par exemple, le personnel de soutien informatique peut légitimement avoir besoin d’accéder à des applications de bureau à distance, mais ce n’est pas le cas de la plupart des utilisateurs. En restreignant l’accès des utilisateurs aux applications, vous empêcherez la présence de failles de sécurité éventuelles qu’un pirate pourrait utiliser pour obtenir accès aux systèmes de votre réseau et les contrôler.

Pour autoriser l’accès basé sur l’utilisateur aux applications :

- Activez User-ID dans les zones à partir desquelles vos utilisateurs initient le trafic.
- Pour chaque règle d’autorisation des applications que vous définissez, identifiez les groupes d’utilisateurs qui, dans le cadre de leurs activités professionnelles, doivent utiliser les applications autorisées par la règle. Le mappage des règles d’autorisation de l’application aux objectifs de l’entreprise (ce qui inclut la prise en compte des utilisateurs ayant un besoin métier pour un type d’application particulier) entraîne un nombre réduit de règles à gérer par rapport au mappage des règles basées sur des ports à des utilisateurs.
- Si vous n’avez pas de groupes d’utilisateurs existants sur votre serveur Active Directory (AD), vous pouvez également créer des groupes LDAP personnalisés pour faire correspondre les groupes d’utilisateurs qui ont besoin d’accéder à une application particulière.
- Il suffit qu’un seul utilisateur final clique sur un lien d’hameçonnage et fournisse ses informations d’identification pour qu’un pirate puisse obtenir accès à votre réseau. Pour vous protéger contre cette technique d’attaque simple et efficace, configurez la prévention contre l’hameçonnage des informations d’identification de toutes les règles de politique de sécurité qui autorisent les utilisateurs à accéder à l’Internet. Configurez la détection des informations d’identification à l’aide de l’agent User-ID Windows pour vous assurer de pouvoir détecter les situations où des utilisateurs transmettent leurs informations d’identification d’entreprise à un site qui appartient à une catégorie non autorisée.

Décryptage du trafic pour une visibilité complète et pour l’inspection des menaces

Déchiffrez tout le trafic, à l’exception des catégories sensibles, qui incluent des catégories d’URL telles que les services financiers, la santé et la médecine, le gouvernement et d’autres trafics que vous ne déchiffrez pas pour des raisons commerciales, juridiques ou réglementaires. Utilisez des catégories d’URL, des catégories d’URL personnalisées et des listes dynamiques externes (EDL) pour spécifier le trafic que vous ne déchiffrez pas.

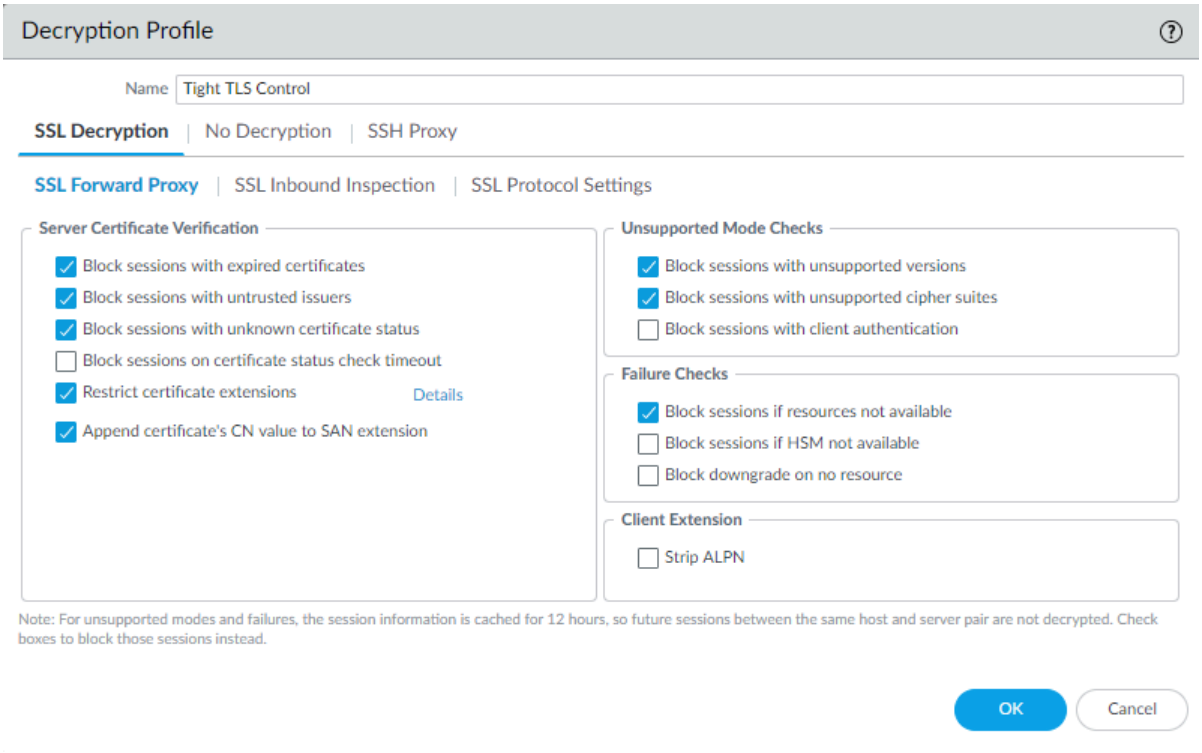
N’utilisez les exceptions de décryptage que lorsque cela est nécessaire. Soyez précis pour vous assurer de limiter les exceptions à des applications ou des utilisateurs spécifiques en fonction des besoins :

- Si le décryptage interrompt une application importante, créez une exception pour l’adresse IP, le domaine ou le nom commun précis qui se trouvent dans le certificat associé à l’application.
- Si vous devez exclure un utilisateur spécifique pour des motifs réglementaires, commerciaux ou juridiques, créez une exception qui ne s’applique qu’à cet utilisateur.

Pour garantir que les certificats présentés lors du décryptage sont valides, effectuez des vérifications CRL/OCSP.

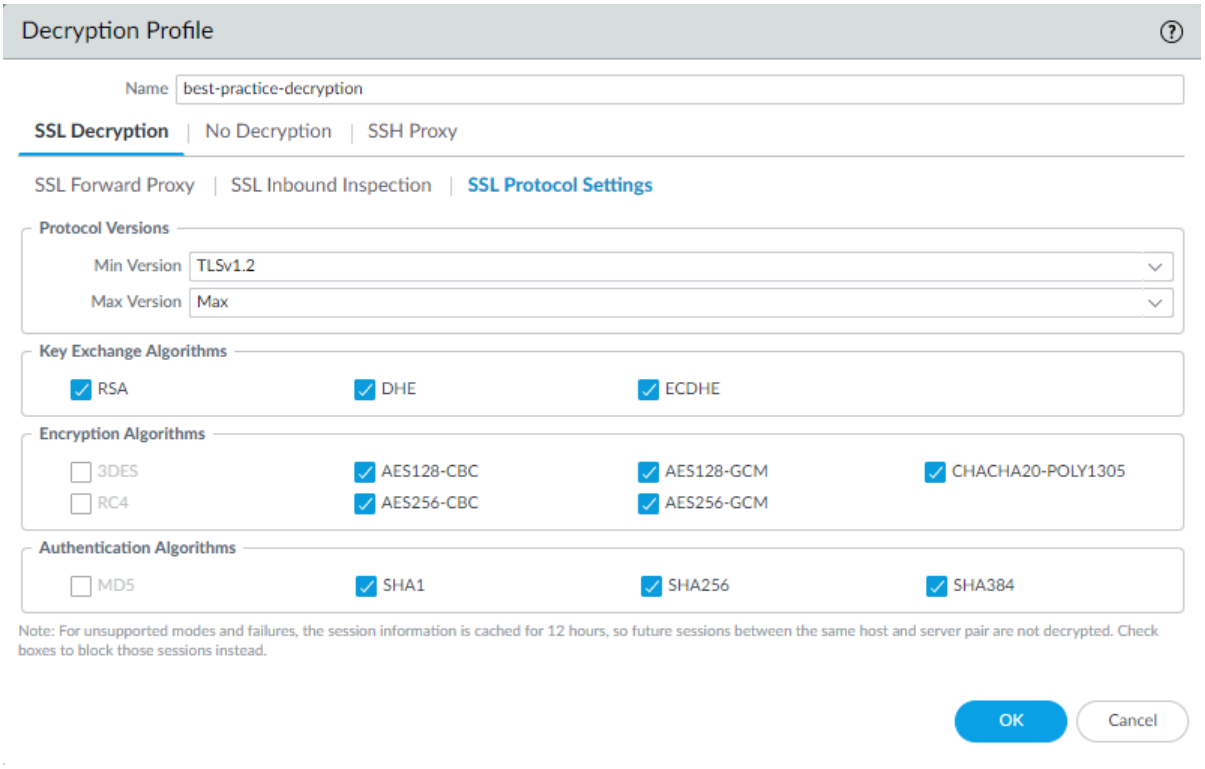
Ajoutez un profil de décryptage strict aux règles de politique de décryptage. Avant de configurer le proxy de transfert SSL, créez un profil de décryptage exemplaire (**Objects [Objets]** > **Decryption Profile [Profil de décryptage]**) pour l’associer à vos règles de politique de décryptage et suivez les meilleures pratiques de décryptage générales :

STEP 1 | Configurez les paramètres **SSL Decryption (Décryptage SSL)** > **SSL Forward Proxy (Proxy de transfert SSL)** pour interdire les exceptions lors de la négociation TLS et bloquer les sessions qui ne peuvent être déchiffrées :



Bloquer les sessions si les ressources ne sont pas disponibles empêche d'autoriser des connexions potentiellement dangereuses lorsque le pare-feu ne dispose pas des ressources nécessaires pour effectuer le décryptage, mais le blocage du trafic que vous ne pouvez pas décrypter pour cette raison risque d'affecter l'expérience de l'utilisateur.

STEP 2 | Configurez **SSL Decryption (Décryptage SSL)** > **SSL Protocol Settings (Paramètres du protocole SSL)** pour interdire l'utilisation de versions SSL/TLS vulnérables (TLSv1.0, TLSv1.1 et SSLv3) et pour éviter les algorithmes faibles (MD5, RC4 et 3DES) :

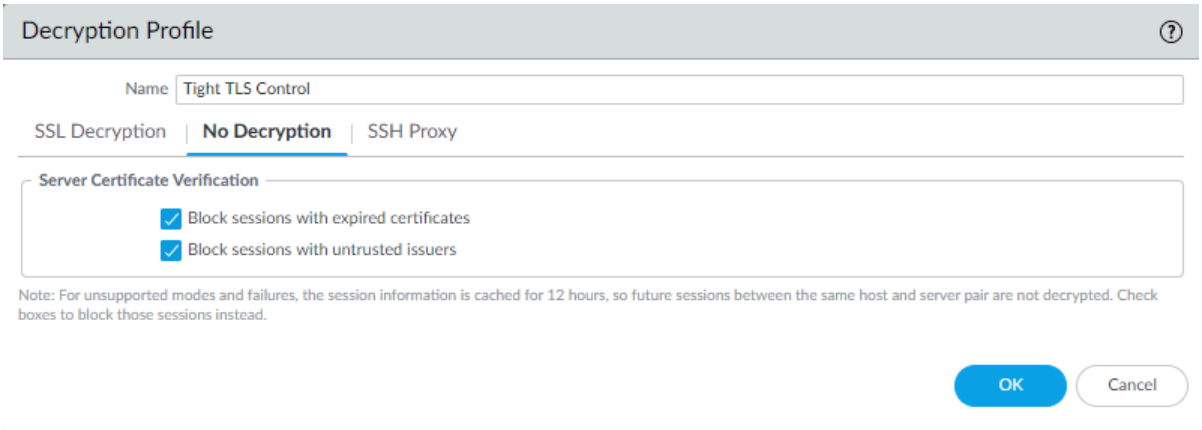


Utilisez TLSv1.3 (le protocole le plus sécurisé) dès que possible. De nombreuses applications mobiles utilisent l'épinglage de certificats qui empêche le décryptage et provoque l'interruption du trafic par le pare-feu. Pour ce trafic, utilisez TLSv1.2.

Revoyez les sites auxquels vous devez accéder pour des raisons d'affaires. Si l'un d'entre eux utilise TLSv1.1, créez une politique et un profil de décryptage distincts pour ces sites afin que seuls les sites dont vous avez besoin de manière professionnelle puissent utiliser le protocole moins sécurisé.

N'autorisez pas l'algorithme d'authentification SHA1 à moins d'y être obligé. Créez une règle et un profil de politique de décryptage distincts pour les sites qui utilisent SHA1 et auxquels vous devez accéder à des fins professionnelles.

STEP 3 | Pour le trafic que vous ne déchiffrez pas, configurez les paramètres **No Decryption (Aucun décryptage)** pour bloquer les sessions chiffrées vers des sites ayant des certificats expirés ou des émetteurs non approuvés :



Utilisez seulement un profil de non-décryptage pour TLSv1.2 et les versions antérieures. Ne créez pas un profil de non-décryptage au trafic TLSv1.3 que vous ne décryptez pas. TLSv1.3 crypte les informations de certificat qui n'ont pas été cryptées dans les versions précédentes afin que le pare-feu ne puisse pas bloquer les sessions basées sur les informations de certificat.

Transition en toute sécurité vers les profils de sécurité respectant les meilleures pratiques

Les profils de sécurité vous permettent d'inspecter le trafic du réseau à la recherche de menaces telles que les exploitations de vulnérabilité, les logiciels malveillants, la communication commande et contrôle (C2) et les menaces inconnues, et les empêchent de compromettre votre réseau à l'aide de divers types de signatures de menaces, machine learning et IA (certaines protections exigent un abonnement).

L'objectif final est d'atteindre un état respectant les meilleures pratiques pour tous vos profils de sécurité. Toutefois, pour garantir la disponibilité des applications essentielles à vos activités, il peut s'avérer impossible de mettre en œuvre dès le départ une configuration complète de profils de sécurité respectant les meilleures pratiques. Dans la plupart des cas, vous pouvez bloquer en toute sécurité certaines signatures, certains types de fichiers ou protocoles tout en alertant sur d'autres jusqu'à ce que vous obteniez les informations et la confiance nécessaires pour mener à bien la transition en toute sécurité vers les profils de sécurité respectant les meilleures pratiques sans affecter la disponibilité.

La mise en œuvre de profils de sécurité respectant les meilleures pratiques est la suivante :

1. Utilisez AIOps pour générer un rapport d'évaluation des meilleures pratiques (BPA) à la demande sur votre posture de sécurité. Examinez l'adoption des meilleures pratiques, identifiez les lacunes dans l'adoption et examinez la configuration du profil de sécurité.
2. Utilisez les étapes de transition en toute sécurité suivantes pour vous passer à l'état respectant les meilleures pratiques pour vos profils de sécurité.

Posez-vous les questions suivantes pour vous aider à déterminer la bonne approche pour activer les profils de sécurité pour un segment de réseau donné ou un ensemble de règles de politique de sécurité :

1. Des profils de sécurité sont-ils déjà activés pour les règles protégeant des applications ou des segments de réseau similaires ? Si la réponse est oui, vous pourrez peut-être dupliquer ces paramètres de profil, notamment les actions de blocage que vous considérez comme déjà assez sécurisées pour être activées.
2. Le segment de réseau que je protège est-il essentiel pour mes activités ? Si la réponse est oui et que vous n'avez pas de profils éprouvés activés dans des segments similaires, il est préférable d'envoyer d'abord une alerte, d'examiner le trafic à l'origine des alertes pour s'assurer que le profil ne bloque pas les applications critiques, puis de bloquer lorsque vous êtes satisfait.
3. Est-ce que je déploie des profils de sécurité pour contrer une menace immédiate ? Si la réponse est oui, vous souhaiterez peut-être bloquer l'action initiale au lieu d'envoyer une alerte.
4. Existe-t-il un processus de modification de pare-feu permettant d'enquêter et de remédier aux faux positifs en temps voulu ? Si la réponse est oui, vous pourrez peut-être bloquer l'action initiale au lieu d'envoyer une alerte.

La majorité des « faux positifs » sont des tentatives d'attaque contre une vulnérabilité qui n'existe pas sur votre réseau. L'attaque est réelle, mais le danger n'est pas dû au fait que la vulnérabilité n'est pas présente. L'attaque est donc souvent considérée comme un faux positif. Les signatures d'attaque par force brute peuvent également provoquer des faux positifs si le seuil d'attaque est défini trop bas.

Tenez compte de votre posture de sécurité actuelle ainsi que des instructions pour chaque type de profil de sécurité afin de décider du déploiement initial des profils, puis de passer aux instructions relatives aux meilleures pratiques.

Transition des profils de protection contre les vulnérabilités en toute sécurité vers les meilleures pratiques

La décision de bloquer ou d'envoyer une alerte lorsque vous appliquez pour la première fois des profils de protection contre les vulnérabilités au trafic dépend de votre posture de sécurité actuelle et des exigences de votre entreprise en matière de sécurité par rapport à la disponibilité. Les instructions ci-dessous permettent de déterminer s'il convient de commencer par des actions de blocage ou d'alerte lorsque vous démarrez la transition vers les profils de protection contre les vulnérabilités respectant les meilleures pratiques.

La prévention contre les vulnérabilités nécessite un abonnement Prévention avancée des menaces ou un abonnement Prévention des menaces hérité actif.

Pour identifier et prévenir les menaces, le pare-feu doit avoir une visibilité sur le trafic des applications. Décryptez *autant de trafic que le permettent les réglementations locales, les considérations commerciales, les considérations relatives à la protection de la vie privée et les capacités techniques. Si vous ne décryptez pas le trafic, le pare-feu ne peut pas analyser les en-têtes cryptés et les informations de la charge utile.*

En outre, suivez les meilleures pratiques de mise à jour du contenu des menaces *pour vous assurer que les signatures de votre profil de sécurité sont à jour.*

- **Applications critiques pour l'entreprise** : il est généralement préférable de définir l'**Action** initiale de la règle sur **alert (alerte)** pour garantir la disponibilité des applications. Toutefois, dans certaines situations, vous pouvez utiliser l'action **block (blocage)** dès le début. Par exemple, lorsque vous protégez déjà des applications similaires avec un profil de protection contre les vulnérabilités qui bloque les signatures de vulnérabilité et que vous êtes certain que ce profil répond à vos besoins

professionnels et à vos besoins en matière de sécurité, vous pouvez utiliser un profil similaire pour bloquer les vulnérabilités et protéger les applications similaires.

Les alertes vous permettent d'analyser les journaux des menaces et de créer des exceptions si nécessaire avant de commencer à bloquer le trafic. L'alerte et la surveillance avant de passer au blocage vous donnent confiance :

- *Le profil initial ne bloque pas les applications critiques lorsque vous le déployez.*
- *Vous créez les exceptions nécessaires lors du passage à l'état de blocage afin de maintenir la disponibilité de l'application.*

Limitez au minimum la durée pendant laquelle vous maintenez l'action d'alerte initiale afin de réduire le risque de faille de sécurité. Passez à l'état de blocage dès que vous êtes certain d'avoir identifié les exceptions que vous devez créer et configuré le profil en conséquence.

- **Signatures de sévérité élevée et critique** : les taux de faux positifs pour les signatures de sévérité élevée et critique sont généralement faibles et indiquent souvent une attaque contre une vulnérabilité qui n'existe pas sur votre réseau. Pour les applications qui ne sont pas essentielles à vos activités, telles que l'accès Internet, bloquez (**reset-both (réinitialiser les deux)**) dès le départ les signatures de sévérité élevée et critique.
- **Signatures de sévérité moyenne** : elles peuvent générer des faux positifs et nécessiter une surveillance initiale. Commencez par activer les alertes pour les signatures de sévérité moyenne et surveillez les journaux de menaces (**Monitor [Surveiller]** > **Logs [Journaux]** > **Threat [Menace]**) pour voir si vous devez bloquer les applications pour lesquelles vous recevez des alertes ou si vous devez les autoriser.
- Affinez les règles de profil qui alertent avant de passer au blocage, en particulier pour le trafic Internet et des centres de données. Passez au blocage dès que vous le pouvez.
- Définissez les signatures de la catégorie force brute sur alerte, puis passez au blocage dès que vous le pouvez. Les événements de force brute sont des événements agrégés qui se déclenchent lorsqu'une action a lieu plusieurs fois dans un court laps de temps. Par exemple, une tentative de connexion SSH est un événement informatif, mais 100 tentatives de connexion en 10 secondes déclenchent la signature force brute. Bien qu'il faille du temps pour ajuster le profil afin que le trafic réseau normal ne déclenche

pas de signature force brute, passez au blocage de ces signatures dès que cela est possible en toute sécurité, en fonction de votre niveau de confort.

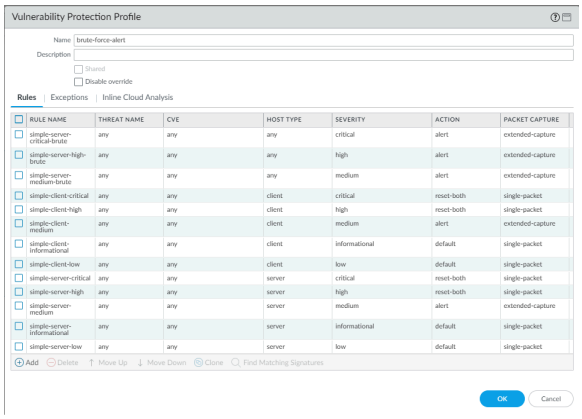


Figure 1: Profil de protection contre les vulnérabilités d'alerte force brute

- L'**Action** par défaut pour la plupart des signatures de sévérité faible et informative est **alert (alerte)** ou **allow (autoriser)**. Sauf s'il est nécessaire d'activer les alertes pour toutes les signatures de gravité faible et informative, configurez l'**Action** sur **default (par défaut)**.
- Si les ressources sont disponibles, activez la capture de paquets étendue pour les signatures de sévérité critique, élevée et moyenne sur lesquelles vous émettez des alertes. Activez la capture de paquets uniques pour les signatures bloquées et pour les signatures de sévérité faible et informative. L'activation de la capture de paquets vous permet d'enquêter de manière approfondie sur les événements si nécessaire. Lorsque vous passez aux profils respectant les meilleures pratiques, si des événements faibles et informatifs génèrent trop d'activités de capture de paquets (volume de trafic trop important) et que ces informations ne sont pas utiles, désactivez la capture de paquets pour les événements informatifs.

  *Les captures de paquets consomment des ressources du plan de gestion. Vérifiez les ressources système (par exemple, **Dashboard [Tableau de bord]** > **System Resources [Ressources système]**) pour comprendre leur utilisation avant et après la mise en œuvre de la capture de paquets afin de vous assurer que votre système dispose de ressources suffisantes pour effectuer toutes les captures de paquets.*
- Pour **Inline Cloud Analysis (Analyse cloud en ligne)**, utilisez les mêmes critères d'alerte et de blocage des applications professionnelles que ceux utilisés pour les règles de protection contre les vulnérabilités. Si vous disposez de contrôles existants, vous pouvez les répliquer pour bloquer le trafic. Pour les

nouveaux contrôles, alertez pendant au moins une semaine avant de passer au blocage. Passez au blocage dès que vous le pouvez.

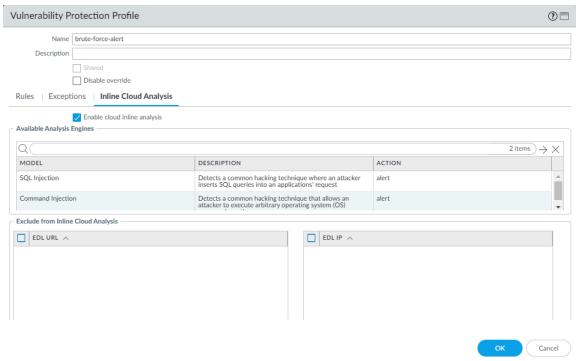


Figure 2: Profil de protection contre les vulnérabilités d'alerte Analyse cloud en ligne

Une fois les profils initiaux en place, surveillez les journaux de menaces pendant suffisamment de temps pour vous assurer de comprendre si des applications essentielles à vos activités provoquent des alertes ou des blocages. Créez des exceptions (ouvrez un billet d'assistance si nécessaire) dans chaque profil pour remédier aux faux positifs confirmés avant de passer aux profils de protection contre les vulnérabilités basés sur les meilleures pratiques. La rapidité de votre transition vers les profils de bonnes pratiques dépend de votre activité, de vos applications et de votre niveau de confort ; sachez que certaines applications ne sont utilisées qu'une fois par semaine, par mois, par trimestre ou par an pour des audits, des événements et des réunions périodiques, etc.

Transition des profils antispyware en toute sécurité vers les meilleures pratiques

Les instructions ci-dessous permettent de déterminer s'il convient de commencer par des actions de blocage ou d'alerte lorsque vous définissez les profils antispyware initiaux et commencez la transition vers les profils respectant les meilleures pratiques.

L'antispyware nécessite un abonnement Prévention avancée des menaces ou un abonnement Prévention des menaces hérité actif.

Pour identifier et prévenir les menaces, le pare-feu doit avoir une visibilité sur le trafic des applications. Décryptez autant de trafic que le permettent les réglementations locales, les considérations commerciales, les considérations relatives à la protection de la vie privée et les capacités techniques. Si vous ne décryptez pas le trafic, le pare-feu ne peut pas analyser les en-têtes cryptés et les informations de la charge utile.

En outre, suivez les meilleures pratiques de mise à jour du contenu des menaces pour vous assurer que les signatures de votre profil de sécurité sont à jour.

- **Applications essentielles à vos activités** : définissez l'action initiale sur Alerte pour garantir la disponibilité des applications. Toutefois, dans certaines situations, vous pouvez utiliser l'action de **blocage** dès le début. Par exemple, lorsque vous protégez déjà des applications avec un profil antispyware qui bloque les signatures critiques, élevées et/ou moyennes et que vous êtes certain que ce

profil répond à vos besoins professionnels et à vos besoins en matière de sécurité, vous pouvez utiliser un profil similaire pour bloquer les logiciels antispyware et protéger ces applications.

L'action d'alerte vous permet d'analyser les journaux de menaces et de créer des exceptions si nécessaire avant de passer à une action de blocage. L'alerte et la surveillance avant de passer au blocage vous donnent confiance :

- *Le profil ne bloque pas les applications critiques lorsque vous le déployez.*
- *Vous créez les exceptions nécessaires lors du passage à l'état de blocage afin de maintenir la disponibilité de l'application.*

Passez à l'état respectant les meilleures pratiques dès que vous êtes certain d'avoir identifié les exceptions que vous devez créer et configuré le profil en conséquence.

- **Signatures de sévérité élevée et critique** : les taux de faux positifs sont généralement faibles. Pour les applications qui ne sont pas essentielles à vos activités, bloquez dès le départ les signatures de sévérité élevée et critique.
- **Signatures de sévérité moyenne** : elles peuvent générer des faux positifs et nécessiter une surveillance initiale. Commencez par émettre des alertes sur les signatures de sévérité moyenne pour le trafic interne et par bloquer les signatures de sévérité moyenne pour le trafic orienté vers l'extérieur. Surveillez les journaux de menaces (**Monitor [Surveiller]** > **Logs [Journaux]** > **Threat (Menace)**) pour voir si vous devez bloquer les applications pour lesquelles vous recevez des alertes ou si vous devez les autoriser.
- **Signatures de gravité faible et informative** : l'action par défaut pour la plupart de ces signatures est alert (alerte) ou allow (autoriser). Sauf s'il est nécessaire d'activer les alertes pour toutes les signatures de gravité faible et informative, commencez par l'action par défaut.
- Activez la capture de paquets unique pour toutes les signatures de gravité pendant la transition si vous disposez des ressources nécessaires. L'activation de la capture de paquets vous permet d'enquêter de manière approfondie sur les événements si nécessaire. Lorsque vous passez aux profils respectant les meilleures pratiques, si des événements faibles et informatifs génèrent trop d'activités de capture de paquets (volume de trafic trop important) et que ces informations ne sont pas utiles, désactivez la capture de paquets pour ces sévérités.

  *Les captures de paquets consomment des ressources du plan de gestion. Vérifiez les ressources système (par exemple, **Dashboard [Tableau de bord]** > **System Resources [Ressources système]**) pour comprendre leur utilisation avant et après la mise en œuvre de la capture de paquets afin de vous assurer que votre système dispose de ressources suffisantes pour effectuer toutes les captures de paquets.*
- Si vous traitez les applications internes différemment des applications externes, vous aurez peut-être besoin d'un profil antispyware pour le trafic Internet et d'un profil antispyware différent pour le trafic interne.
- **DNS Policies (Politiques DNS)** :
  - Définissez **Policy Action (Action de politique)** pour les signatures DNS sur **Sinkhole** pour identifier les hôtes potentiellement compromis qui tentent d'accéder à des domaines suspects. DNS Sinkhole vous permet de suivre les hôtes et de les empêcher d'accéder à ces domaines. (L'activation immédiate de DNS Sinkhole est la meilleure pratique.) Définissez **Packet Capture (Capture de paquet)** sur **extended-capture (capture étendue)**.

- Mettez en entonnoir tous les types de domaines **DNS Security (Sécurité DNS)** et définissez **Packet capture (Capture de paquet)** comme indiqué dans la figure 1 (PAN-OS 10.0 et versions ultérieures).
- De plus, bloquez tous les types d'enregistrements DNS, car ils sont utilisés par les requêtes DNS cryptées. Cela empêche les clients de crypter leur message d'accueil pendant le processus de résolution DNS, ce qui bloque l'échange d'informations clés.

N'autorisez le trafic que vers les serveurs DNS approuvés. Utilisez le service de sécurité DNS pour empêcher les connexions à des serveurs DNS malveillants.

Sur les systèmes basés sur PAN-OS, définissez l'adresse DNS Sinkhole comme nom de domaine complet, par exemple, Sinkhole.paloaltonetworks.com, de sorte que si l'adresse IP change, le paramètre soit toujours valide. Pour Prisma Access, utilisez l'adresse IP entonnoir.

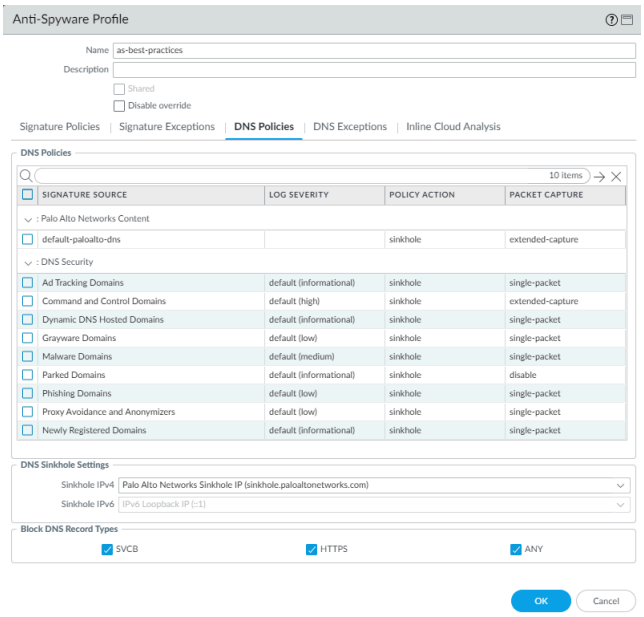


Figure 3: Politiques DNS du profil antispyware

- **Inline Cloud Analysis (Analyse cloud en ligne)** (nécessite un abonnement Prévention des menaces avancée et PAN-OS 10.2 ou version ultérieure) : sélectionnez **Enable cloud inline analysis (Activer l'analyse cloud en ligne)** pour tout le trafic sortant. Définissez l'**Action** sur **reset-both (réinitialiser les deux)** pour tous les modèles.

Les environnements isolés ne peuvent pas utiliser la prévention des menaces avancée, car il s'agit d'un service cloud qui nécessite une connexion cloud.

Une fois les profils initiaux en place, surveillez les journaux de menaces pendant suffisamment de temps pour vous assurer de comprendre si des applications essentielles à vos activités provoquent des alertes ou des blocages. Passez aux meilleures pratiques en matière de profils antispyware dès que vous vous sentez à l'aise. Créez des exceptions (ouvrez un billet d'assistance si nécessaire) dans chaque profil pour remédier aux faux positifs confirmés avant de mettre en œuvre des profils Antispyware complets respectant les meilleures pratiques.

Transition des profils antivirus en toute sécurité vers les meilleures pratiques

Les instructions suivantes permettent de déterminer s'il faut commencer par des actions de blocage ou d'alerte lorsque vous clonez le profil antivirus par défaut et que vous le modifiez pour définir les profils initiaux et commencer la transition vers les profils de meilleures pratiques.

L'antivirus nécessite un abonnement Prévention avancée des menaces ou un abonnement Prévention des menaces hérité actif.

Pour identifier et prévenir les menaces, le pare-feu doit avoir une visibilité sur le trafic des applications. Décryptez autant de trafic que le permettent les réglementations locales, les considérations commerciales, les considérations relatives à la protection de la vie privée et les capacités techniques. Si vous ne décryptez pas le trafic, le pare-feu ne peut pas analyser les en-têtes cryptés et les informations de la charge utile.

En outre, suivez les meilleures pratiques de mise à jour du contenu des menaces pour vous assurer que les signatures de votre profil de sécurité sont à jour.

- **Applications essentielles à vos activités** : définissez l'action initiale sur Alerte pour garantir la disponibilité des applications. Toutefois, dans certaines situations, vous pouvez bloquer les signatures Antivirus dès le début. Par exemple, lorsque vous protégez déjà des applications similaires avec un profil Antivirus et que vous êtes certain que ce profil répond à vos besoins professionnels et à vos besoins en matière de sécurité, vous pouvez utiliser un profil similaire pour protéger des applications similaires, car vous comprenez déjà ce que vous bloquez.

  *L'action d'alerte vous permet d'analyser les journaux de menaces (**Monitor [Surveiller]** > **Logs [Journaux]** > **Threat [Menace]**) et de créer des exceptions si nécessaire avant de passer à une action de blocage. L'alerte et la surveillance avant de passer au blocage vous donnent confiance :*

  - *Le profil ne bloque pas les applications critiques lorsque vous le déployez.*
  - *Vous créez les exceptions nécessaires lors du passage à l'état de blocage afin de maintenir la disponibilité de l'application.*

  Limitez au minimum la durée pendant laquelle vous maintenez l'action d'alerte initiale afin de réduire le risque de faille de sécurité. Passez à l'état respectant les meilleures pratiques dès que vous êtes certain d'avoir identifié les exceptions que vous devez créer et configuré le profil en conséquence.
- **Signatures de sévérité élevée et critique** : il est prudent de déployer les profils antivirus des meilleures pratiques pour bloquer immédiatement le trafic malveillant pour les applications qui ne sont pas critiques pour votre entreprise, car les taux de faux positifs sont rares, de sorte que les blocages inutiles se produisent rarement.

- Si vous traitez les applications internes différemment des applications externes, vous aurez peut-être besoin d'un profil antivirus pour le trafic Internet et d'un profil antivirus différent pour le trafic interne.
- Activez la recherche de signature en temps réel globalement sur le périphérique et dans le profil antivirus pour conserver les fichiers jusqu'à ce que le pare-feu reçoive la dernière signature antivirus en temps réel du cloud :
  - Activez globalement : **Device (Périphérique)** > **Setup (Configuration)** > **Content-ID** > **Content-ID Settings (Paramètres Content-ID)** > **Realtime Signature Lookup (Recherche de signature en temps réel)**, activez **Hold for WildFire Real Time Signature Look Up (Attente pour recherche de signature WildFire en temps réel)** et définissez **Action On Real Time Signature Timeout (Action après expiration de la signature en temps réel)** sur **reset-both (réinitialiser les deux)**. Vous devez activer la recherche de signature en temps réel à l'échelle mondiale pour l'activer dans les profils antivirus.
  - Activez dans le profil antivirus : **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Antivirus** et activez **Hold for WildFire Real Time Signature Look Up (Attente pour recherche de signature WildFire en temps réel)**.

  La conservation des fichiers pour garantir que WildFire obtient les dernières signatures antivirus vous protège contre les logiciels malveillants du jour zéro et les signatures antivirus obsolètes auxquelles vous pourriez être exposé si vous transférez des fichiers sans les conserver pour les dernières signatures.
- 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.

Une fois les profils initiaux en place, surveillez les journaux de menaces pendant suffisamment de temps pour vous assurer de comprendre si des applications essentielles à vos activités provoquent des alertes ou des blocages. Surveillez également les journaux des envois WildFire (**Monitor [Surveiller]** > **Logs [Journaux]** > **WildFire Submissions [Envois WildFire]**) pendant suffisamment de temps pour vous assurer de comprendre si des applications essentielles à vos activités provoquent des alertes ou des blocages en raison de l'action WildFire du profil Antivirus. Créez des exceptions (ouvrez un billet d'assistance si nécessaire) dans chaque profil pour remédier aux faux positifs confirmés avant de mettre en œuvre des profils antivirus complets respectant les meilleures pratiques. La rapidité de votre transition vers les profils de bonnes pratiques dépend de votre activité, de vos applications et de votre niveau de confort ; sachez que certaines applications ne sont utilisées qu'une fois par semaine, par mois, par trimestre ou par an pour des audits, des événements et des réunions périodiques, etc.

Transition des profils WildFire en toute sécurité vers les meilleures pratiques

Les instructions suivantes permettent de définir la configuration initiale des profils d'analyse WildFire.

Les pare-feu nouvelle génération Palo Alto Networks incluent le service WildFire de base et ne nécessitent pas d'abonnement WildFire avancé (ou WildFire hérité actif). Le service de base permet au pare-feu de transférer les fichiers PE pour analyse et récupère les signatures Advanced WildFire uniquement avec une mise à jour antivirus et/ou Threat Prevention toutes les 24-48 heures. Un abonnement Advanced WildFire (PAN-OS 10.0 ou version ultérieure) ou un abonnement WildFire hérité inclut beaucoup plus de fonctionnalités, telles que la réception de mises à jour en temps réel, la prise en charge de plus de types de fichiers et une API.

Pour identifier et prévenir les menaces, le pare-feu doit avoir une visibilité sur le trafic des applications. Décryptez *autant de trafic que le permettent les réglementations locales, les considérations commerciales, les considérations relatives à la protection de la vie privée et les capacités techniques. Si vous ne décryptez pas le trafic, le pare-feu ne peut pas analyser les en-têtes cryptés et les informations de la charge utile.*

La génération de signatures WildFire est extrêmement précise et les faux positifs sont rares. Le déploiement du profil d'analyse WildFire par défaut (qui est le profil basé sur les meilleures pratiques) n'a pas d'impact sur le trafic réseau. (Cependant, 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.)

Une fois les profils initiaux en place, surveillez les journaux des envois WildFire (**Monitor [Surveiller]** > **Logs [Journaux]** > **WildFire Submissions [Envois WildFire]**) pendant suffisamment de temps pour vous assurer de comprendre si des applications essentielles à vos activités provoquent des alertes ou des blocages en raison de l'action WildFire du profil Antivirus. Créez des exceptions (ouvrez un billet d'assistance si nécessaire) dans le profil Antivirus si nécessaire pour remédier aux faux positifs confirmés.

Transition des profils de filtrage des URL en toute sécurité vers les meilleures pratiques

Suivez les instructions ci-dessous pour déterminer s'il convient de commencer par des actions de blocage ou d'alerte lorsque vous définissez les profils de filtrage des URL initiaux et commencez la transition vers les profils respectant les meilleures pratiques. Appliquez des fichiers de URL Filtering au trafic Internet (n'appliquez aucun profil de URL Filtering au trafic interne).

Vous devez activer le décryptage *pour profiter du filtrage des URL, car vous devez décrypter le trafic pour révéler l'URL exacte afin que le pare-feu puisse prendre la mesure appropriée. Au minimum, décryptez le trafic à risque élevé et moyen.*

Le filtrage des URL avancé *nécessite un abonnement.*

- Les catégories d'URL prédéfinies sont précises. Par conséquent, il est prudent de mettre en œuvre des profils de filtrage des URL avec des actions de catégorie configurées conformément à la politique de votre entreprise pour autoriser ou refuser l'accès à différents types de sites web.
- Bloquez dès le départ **Site Access (Accès au site)** et **User Credential Submission (Envoi des informations d'identification de l'utilisateur)** pour les catégories d'URL connues comme malveillantes, notamment les logiciels malveillants, la commande et le contrôle, la violation des droits d'auteur, l'extrémisme, l'hameçonnage, les ransomwares, les DNS dynamiques, le piratage (mais faire des exceptions pour les testeurs PEN internes), et le contournement de proxy et anonymiseurs.
- Pour les catégories d'URL unknown (inconnues) (les sites PAN-DB n'ont pas encore été identifiés), parked (parquées) (souvent utilisées pour l'hameçonnage des informations d'identification), grayware (logiciel indésirable) (malveillants ou douteux) et newly-registered-domains (domaines nouvellement enregistrés) (souvent utilisés pour des activités malveillantes), alerter au départ pour pouvoir surveiller les journaux de filtrage des URL (**Monitor [Surveiller]** > **Logs [Journaux]** > **URL Filtering [Filtrage des URL]**) si des sites web légitimes déclenchent des alertes avant de passer à la meilleure pratique de blocage de ces catégories.

- Définissez toutes les autres catégories d'URL sur **alert (alerte)** afin de générer des journaux pour le trafic. Le pare-feu ne journalise pas le trafic lorsque l'accès est défini sur **allow (autoriser)**. Surveillez les journaux de filtrage des URL pour voir si vous souhaitez bloquer d'autres catégories.

  Vous pouvez combiner les catégories de risque élevé, moyen et faible avec d'autres catégories pour déterminer le trafic à autoriser, à bloquer et à décrypter. Par exemple, vous pouvez bloquer l'accès à tous les sites web qui présentent un risque élevé et qui proposent des services financiers. Si votre pare-feu doit économiser des ressources, vous pouvez décrypter tout le trafic à haut risque et à risque moyen pour certaines catégories et ne pas décrypter le trafic à faible risque pour ces mêmes catégories.

Une fois les profils initiaux en place, surveillez les journaux de filtrage des URL pendant suffisamment de temps pour vous assurer que les sites essentiels à vos activités seront bloqués si vous passez d'une alerte à un blocage et aux Profils de filtrage des URL respectant les meilleures pratiques. Si vous pensez qu'une URL donnée n'est pas classée correctement, effectuez la Demande de recatégorisation d'URL pour que l'URL soit placée dans la bonne catégorie. La rapidité de votre transition vers les profils basés sur les meilleures pratiques dépend de votre activité, de vos applications et de votre niveau de confort.

Transition des profils de blocage de fichiers en toute sécurité vers les meilleures pratiques

Les instructions ci-dessous permettent de déterminer s'il convient de commencer par des actions de blocage ou d'alerte lorsque vous définissez les profils de blocage de fichiers initiaux et commencez la transition vers les profils respectant les meilleures pratiques. Alertez au lieu de permettre aux types de fichiers de générer des journaux et d'avoir une visibilité sur le trafic.

- Les profils de blocage des fichiers basés sur les meilleures pratiques sont souvent différents selon les types d'applications et peuvent être différents pour le trafic entrant, sortant et interne. Par exemple :
  - Si des applications internes dépendent des transferts de types de fichiers et que le profil de blocage de fichiers respectant les meilleures pratiques recommande le blocage, autorisez ces types de fichiers pour ces applications internes ; les fichiers .dll en sont un bon exemple. N'autorisez ces types de transferts de fichiers que pour les applications internes nécessaires et non pour toutes les applications.
  - Pour le trafic basé sur Internet, adoptez une approche plus restrictive afin d'empêcher les pirates de diffuser des fichiers malveillants et de réduire la surface d'attaque.
  - Pour le trafic des centres de données, adoptez une approche plus restrictive (à l'exception des applications internes dépendant des types de transfert de fichiers que vous bloqueriez sinon) pour réduire la surface d'attaque et protéger vos atouts les plus précieux.
  - Lorsque vous prévoyez des exceptions, suivez le principe au moindre privilège et n'appliquez les exceptions qu'aux applications et aux utilisateurs qui ont besoin d'accéder au type de fichier à des fins professionnelles.
- **Applications critiques pour l'entreprise** : commencez par l'action d'alerte pour tous les types de fichiers et passez dès que possible aux profils de blocage de fichiers basés sur les meilleures pratiques. Si vous avez déjà mis en place des contrôles de blocage, reproduisez-les et continuez à bloquer le trafic que vous savez déjà vouloir bloquer.

- Pour les applications qui ne sont pas critiques pour l'entreprise, commencez la transition vers un profil de blocage de fichiers basé sur les meilleures pratiques :
  - **Trafic entrant et sortant** : définissez l'**Action** sur **block (blocage)** pour les fichiers 7z, bat, chm, class, cpl, dll, dlp, hta, jar, ocx, pif, scr, torrent, vbe et wsf. Définissez l'**Action** sur **alert (alerte)** pour tous les autres fichiers.
  - **Trafic interne** : bloquez les fichiers 7z, bat, chm, class, cpl, dlp, hta, jar, ocx, pif, scr, torrent, vbe et wsf (identique au profil entrant/sortant, sauf qu'il alerte sur les fichiers .dll au lieu de les bloquer). Activez les alertes pour tous les autres fichiers.
  - Bloquez tous les types de fichiers suivants pour les utilisateurs qui n'en ont pas besoin à des fins professionnelles : cab, exe, flash, msi, Multi-Level-Encoding, PE, rar, tar, encrypted-rar et encrypted-zip.

Si nécessaire, créez des exceptions pour les groupes informatiques et les autres personnes qui ont besoin d'un accès professionnel légitime à l'un de ces types de fichiers. Si vous bloquez déjà d'autres types de fichiers, continuez à les bloquer.

Passez à un profil de blocage de fichiers basé sur les meilleures pratiques aussi rapidement que vous êtes à l'aise pour le faire.

Affinez les règles de profil qui alertent et passez au blocage dès que vous le pouvez, en particulier pour le trafic en direction de l'Internet et des centres de données. Surveillez les journaux de filtrage des données (**Monitor [Surveiller]** > **Logs [Journaux]** > **Data Filtering [Filtrage des données]**) pour comprendre l'utilisation des types de fichiers avant de configurer les actions de blocage pour des types de fichiers spécifiques. Au fur et à mesure que vous apprenez quels types de fichiers sont nécessaires à vos applications critiques et à vos applications internes personnalisées, vous pouvez adopter une configuration de blocage de fichiers basée sur les meilleures pratiques, en la modifiant si nécessaire pour répondre aux besoins de votre entreprise.

Création des meilleures pratiques de profils de sécurité pour la passerelle Internet

La plupart des logiciels malveillants se glissent sur le réseau au moyen d'applications ou de services légitimes. Pour activer les applications en toute sécurité, vous devez analyser tout le trafic autorisé à la recherche de menaces. Associez les profils de sécurité à toutes les règles de politique de sécurité qui autorisent le trafic afin de pouvoir détecter les menaces (connues et inconnues) présentes dans le trafic de votre réseau. Les recommandations de bonnes pratiques suivantes se concentrent sur la sécurité la plus stricte. Associez un profil de filtrage des URL à toutes les règles qui autorisent le trafic Internet et associez les autres profils à toutes les règles d'autorisation.

Plus de 90 % du trafic web est crypté. Activez le décryptage pour gagner en visibilité sur le trafic, utilisez les profils de sécurité pour inspecter la charge utile et prévenir les événements malveillants.

Pensez à ajouter vos profils de sécurité basés sur les meilleures pratiques à un groupe de profils de sécurité par défaut. *Lorsque vous nommez un groupe de profils de sécurité* ***`default (par défaut)`****, le pare-feu l'associe automatiquement à chaque nouvelle règle de politique de sécurité que vous créez et garantit que le pare-feu inspecte le trafic à la recherche d'activités malveillantes.*

Pensez également à créer des groupes de profils de sécurité spécialement conçus pour différents types de trafic. Les groupes de profils de sécurité facilitent l'application de tous les profils nécessaires aux règles de politique de sécurité et garantissent qu'aucun profil critique n'est oublié.

- Profil de blocage des fichiers exemplaire pour la passerelle Internet
- Politique antivirus exemplaire pour la passerelle Internet
- Profil de protection contre les vulnérabilités exemplaires pour la passerelle Internet
- Profil antispyware exemplaire pour la passerelle Internet
- Profil de URL Filtering exemplaire pour la passerelle Internet
- Profil d'analyse WildFire exemplaire pour la passerelle Internet

Profil de blocage des fichiers exemplaire pour la passerelle Internet

Utilisez le profil **strict file blocking (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 types de fichiers, vous réduisez la surface d'attaque. Le profil strict prédéfini bloque des fichiers batch, des DLL, 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 de la procédure Transition des profils de blocage de fichiers en toute sécurité vers les meilleures pratiques *pour vous aider à déterminer si vous devez créer des exceptions dans différentes zones du réseau. Passez en revue les journaux de filtrage des données (**Monitor [Surveiller]** > **Logs [Journaux]** > **Data Filtering [Filtrage des données]**) pour identifier les types de fichiers et discuter avec les parties prenantes des types de fichiers dont leurs applications ont besoin. En vous fondant sur ces renseignements, clonez le profil strict et modifiez-le, selon vos besoins, pour autoriser uniquement les autres types de fichiers requis pour supporter ces applications essentielles. Vous pouvez également utiliser le paramètre **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

Vous pouvez également avoir besoin de quelques protocoles souvent utilisés à des fins malveillantes pour des activités telles que les mises à jour Windows. Le profil **strict file blocking (blocage des fichiers strict)** bloque les fichiers .exe., .dll, .pe et .cab. Pour faire des exceptions afin d'autoriser les protocoles pour une activité spécifique telle que les mises à jour Windows :

1. Créez une règle de politique de sécurité spécifique qui autorise uniquement les utilisateurs et applications métier requis qui utilisent les protocoles que vous souhaitez bloquer pour le reste du trafic.
2. Clonez votre profil de blocage des fichiers strict, modifiez-le pour autoriser les protocoles requis, puis associez-le à la règle.
3. Placez la règle au-dessus d'une règle de politique de sécurité avec un profil de blocage des fichiers qui bloque les protocoles pour tout autre trafic.

Cette méthode vous permet d'utiliser des types de fichiers potentiellement malveillants de manière sûre, ce qui active les applications métier tout en bloquant le trafic malveillant. Affinez les profils et la base de règles pour autoriser toutes les exceptions requises.

Pourquoi ai-je besoin de ce profil ?

Les pirates peuvent diffuser des fichiers malveillants de plusieurs manières :

- Pièces jointes ou liens dans un e-mail professionnel ou personnel.
- Liens ou messages instantanés dans les médias sociaux et autres sources.
- Kits d'exploitation.
- Applications de partage de fichiers (telles que FTP, Google Drive ou Dropbox).
- Clés USB.
-

L'association d'un profil de blocage des fichiers strict empêche ces types d'attaques et réduit votre surface d'attaque.

Si vous choisissez de ne pas bloquer l'ensemble des fichiers PE, envoyez tous les fichiers inconnus à WildFire pour qu'ils soient analysés. Définissez l'Action sur **Continue (Continuer)** pour empêcher qu'un téléchargement automatique ne se produise lorsqu'un utilisateur final télécharge du contenu qui installe, à son insu, des fichiers malveillants, tels que des applets Java ou des exécutables. Des téléchargements automatiques peuvent se produire lorsque des utilisateurs se rendent sur des sites web, consultent leurs e-mails ou cliquent sur des fenêtres contextuelles visant à les tromper. Informez vos utilisateurs qu'ils pourraient faire l'objet d'un téléchargement malveillant s'ils sont invités à poursuivre un transfert de fichier qui a été lancé à leur insu. De plus, utilisez le blocage des fichiers avec le filtrage des URL pour limiter les catégories dans lesquelles les utilisateurs peuvent transférer des fichiers afin de réduire la surface d'attaque si vous devez autoriser les types de fichiers susceptibles de contenir des menaces.

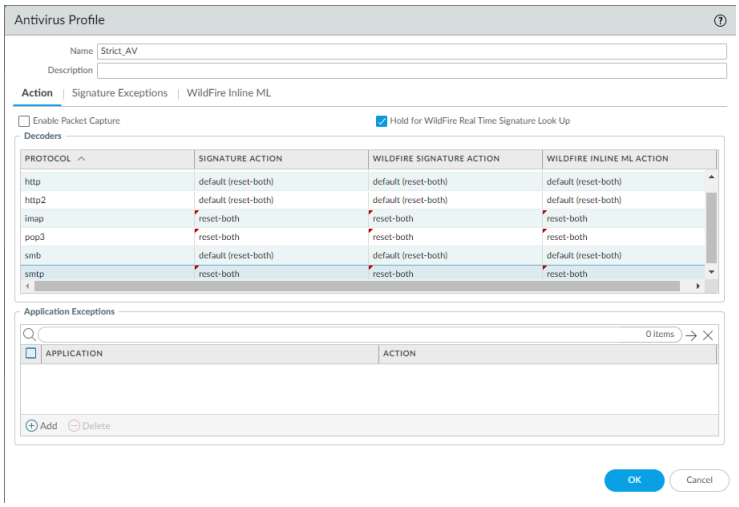
Politique antivirus exemplaire pour la passerelle Internet

Pour assurer la disponibilité des applications essentielles à vos activités, suivez les conseils de la procédure Transition des profils antivirus en toute sécurité vers les meilleures pratiques lorsque vous passez de votre état actuel au profil respectant les meilleures pratiques. L'objectif est de passer au profil comme indiqué ici et de l'associer à toutes les règles de politique de sécurité qui autorisent le trafic. Le profil d'antivirus possède des décodeurs de protocole lui permettant de détecter des virus et des logiciels malveillants et de les empêcher d'être transférés à travers sept protocoles : FTP, HTTP, HTTP2, IMAP, POP3, SMB et SMTP.

Définissez les actions WildFire Signature et WildFire Inline ML pour les sept protocoles (le profil antivirus applique également des actions basées sur les signatures WildFire) et si vous ne l'avez pas déjà fait, activez la recherche de signature en temps réel comme indiqué dans Transition des profils antivirus en toute sécurité vers les meilleures pratiques.

Configurez le profil antivirus cloné pour rétablir le client et le serveur des sept décodeurs de protocole et les actions WildFire, puis associez le profil aux règles d'autorisation de la politique de sécurité.

Si vous traitez les applications internes différemment des applications externes, vous aurez peut-être besoin d'un profil antivirus pour le trafic Internet et d'un profil antivirus différent pour le trafic interne.



Activez la recherche de signature en temps réel globalement et dans le profil antivirus pour conserver les fichiers jusqu'à ce que le pare-feu reçoive la dernière signature antivirus en temps réel du cloud :

- Activez globalement : **Device (Périphérique)** > **Setup (Configuration)** > **Content-ID** > **Content-ID Settings (Paramètres Content-ID)** > **Realtime Signature Lookup (Recherche de signature en temps réel)**, activez **Hold for WildFire Real Time Signature Look Up (Attente pour recherche de signature WildFire en temps réel)** et définissez **Action on Real Time Signature Timeout (Action après expiration de la signature en temps réel)** sur **Reset Both (Réinitialiser les deux)**. Vous devez activer la recherche de signature en temps réel à l'échelle mondiale pour l'activer dans les profils antivirus.
- Activez **Hold for WildFire Real Time Signature Lookup (Attente pour recherche de signature WildFire en temps réel)** dans le profil antivirus. La conservation des fichiers pour garantir que WildFire obtient les dernières signatures antivirus vous protège contre les logiciels malveillants du jour zéro et les signatures antivirus obsolètes auxquelles vous pourriez être exposé si vous transférez des fichiers sans les conserver pour les dernières signatures.

Pourquoi ai-je besoin de ce profil ?

En associant des profils antivirus à toutes les règles de sécurité, vous pouvez bloquer des fichiers malveillants inconnus (logiciel malveillant, ransomware et virus) à leur entrée dans votre réseau. Les utilisateurs reçoivent des fichiers malveillants de diverses façons, dont les plus fréquentes sont les suivantes : des pièces jointes malveillantes dans des e-mails, des liens vers des fichiers malveillants ou une attaque silencieuse facilitée par des kits d'attaque qui exploitent une vulnérabilité avant de télécharger des charges malveillantes directement au périphérique de l'utilisateur final.

Profil de protection contre les vulnérabilités exemplaires pour la passerelle Internet

Associez un profil de protection contre les vulnérabilités pour autoriser tout le trafic en vue d'assurer la protection contre le dépassement de capacité de la mémoire tampon, l'exécution non autorisée de code et d'autres tentatives d'exploitation des vulnérabilités côté client et côté serveur. Pour assurer la disponibilité des applications essentielles à vos activités, suivez les conseils de la procédure Transition des profils de protection contre les vulnérabilités en toute sécurité vers les meilleures pratiques lorsque vous passez de votre état actuel au profil respectant les meilleures pratiques. Clonez le profil de protection contre les vulnérabilités strict prédéfini et modifiez-le pour créer le profil de bonnes pratiques :

- Définissez l'**Action** dans les trois règles de force brute sur **reset-both (réinitialiser les deux)** et **Packet Capture (Capture de paquet)** sur **single-packet (un seul paquet)** pour bloquer les événements d'attaque par force brute au lieu d'envoyer des alertes lorsqu'ils se produisent.
- Regroupez les événements de gravité critique, élevée et moyenne pour les serveurs et les clients en une seule règle. Définissez l'**Action** sur **reset-both (réinitialiser les deux)** et définissez **Packet Capture (Capture de paquet)** sur **single-packet (un seul paquet)**. Cela simplifie le profil et fonctionne, car le profil utilise la même action et les mêmes paramètres de capture de paquets pour ces gravités.

  *Pour les profils qui contrôlent le trafic interne (est-ouest), le blocage des événements de gravité moyenne peut avoir un impact sur les applications métier. Si le blocage affecte les applications métier, créez une règle distincte dans le profil pour les événements de gravité moyenne avec l'**Action** définie sur **alert (alerte)**. Appliquez le profil uniquement au trafic interne.*
- Pour simplifier le profil, consolidez les événements de faible gravité pour les serveurs et les clients en une seule règle. Définissez l'**Action** sur **default (par défaut)** et définissez **Packet Capture (Capture de paquet)** sur **single-packet (un seul paquet)**.

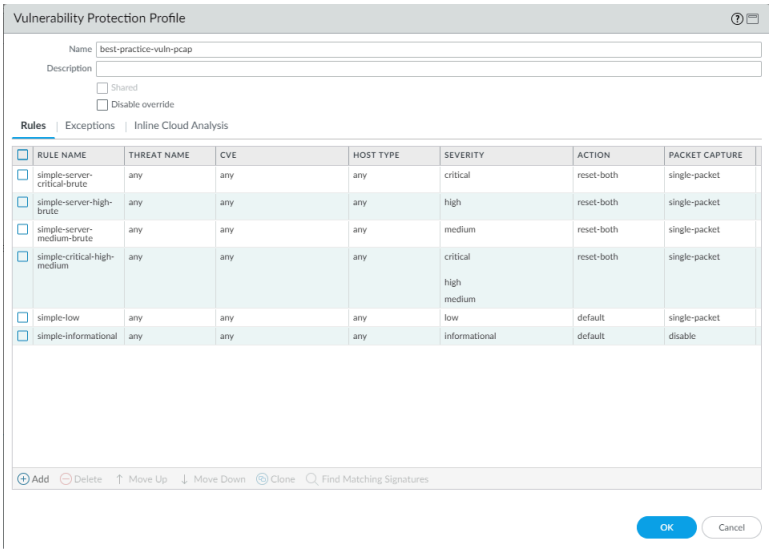
- Consolidez les événements d'information pour les serveurs et les clients en une seule règle. Définissez l'**Action** sur **default (par défaut)** et définissez **Packet Capture (Capture de paquet)** sur **disable (désactiver)**.

  Les PCAP pour les événements d'information génèrent un volume de trafic relativement élevé qui n'est généralement pas utile par rapport aux captures de menaces potentielles.
- Appliquez une PCAP étendue au lieu d'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 et 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 une 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.

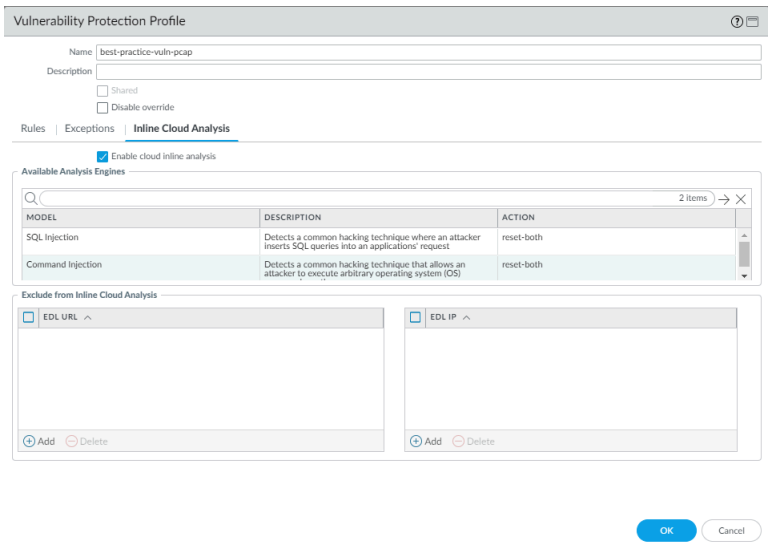
*Si vous souhaitez plus de granularité pour affiner le profil, créez des règles distinctes avec les paramètres **Action** et **Packet Capture (Capture de paquet)** décrits. Par exemple, créez une règle pour les niveaux de gravité critique, élevé et moyen pour les serveurs et une autre règle similaire pour les clients, ou créez des règles distinctes pour chaque niveau de gravité pour les clients et les serveurs afin d'atteindre le niveau de granularité et de contrôle souhaité.*

*Les captures de paquets consomment des ressources du plan de gestion. Vérifiez les ressources système (par exemple, **Dashboard [Tableau de bord]** > **System Resources [Ressources système]**) pour comprendre leur utilisation avant et après la mise en œuvre de la capture de paquets afin de vous assurer que votre système dispose de ressources suffisantes pour effectuer les captures de paquets souhaitées.*

Activez packet capture (capture de paquet, PCAP) pour chaque règle afin de pouvoir localiser la source des attaques potentielles. 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.



Pour **Inline Cloud Analysis (Analyse cloud en ligne)**, définissez l'**Action** sur **reset-both (réinitialiser les deux)** pour bloquer les techniques de piratage courantes.



Pourquoi ai-je besoin de ce profil ?

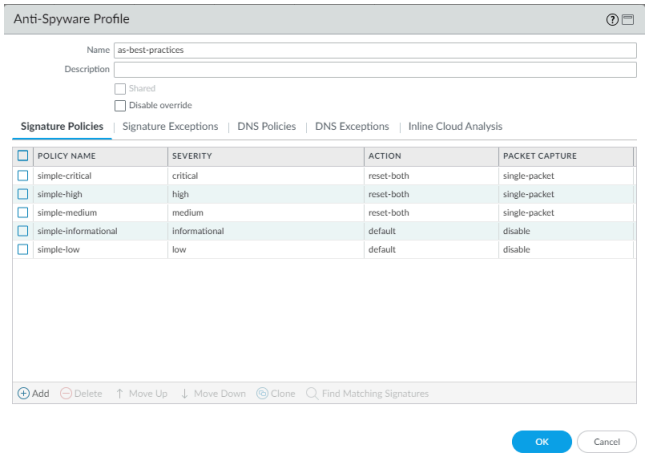
Sans protection stricte contre les vulnérabilités, les pirates peuvent profiter des vulnérabilités côté client et côté serveur pour compromettre les utilisateurs finaux. Par exemple, un pirate pourrait tirer profit d'une vulnérabilité pour installer un code malveillant sur les systèmes client ou utiliser un kit d'attaque pour transmettre automatiquement des charges malveillantes aux utilisateurs finaux. Les profils de protection contre les vulnérabilités empêchent un pirate d'utiliser les vulnérabilités des hôtes internes pour accéder librement à l'ensemble de votre réseau.

Profil antispyware exemplaire pour la passerelle Internet

Associez un profil antispyware à tout le trafic autorisé afin de détecter le trafic de commande et de contrôle (C2) provenant d'un code malveillant s'exécutant sur un serveur ou un point de terminaison et d'empêcher les systèmes infectés d'établir une connexion sortante à partir de votre réseau. Clonez le profil Anti-Spyware strict prédéfini et modifiez-le. Pour garantir la disponibilité des applications critiques pour l'entreprise, transférez les profils antispyware en toute sécurité vers les meilleures pratiques. Modifiez le profil pour autoriser la mise en entonnoir DNS et la capture de paquets (PCAP) pour vous aider à détecter le terminal qui a tenté de résoudre le domaine malveillant. Conservez l'**Action** par défaut pour réinitialiser la connexion lorsque le pare-feu détecte une menace de gravité moyenne, élevée ou critique, et activez un PCAP unique pour ces menaces.

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

Si vous traitez les applications internes différemment des applications externes, vous aurez peut-être besoin d'un profil antispyware pour le trafic Internet et d'un profil antispyware différent pour le trafic interne.



N’activez pas de PCAP à titre informatif, car cela génère un volume relativement élevé pour ce trafic et cela n’est pas particulièrement utile, comparé à des PCAP pour menaces potentielles. Appliquez une PCAP étendue au lieu d’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 et 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 une 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.

*Les captures de paquets consomment des ressources du plan de gestion. Vérifiez les ressources système (par exemple, **Dashboard [Tableau de bord]** > **System Resources [Ressources système]**) pour comprendre leur utilisation avant et après la mise en œuvre de la capture de paquets afin de vous assurer que votre système dispose de ressources suffisantes pour effectuer toutes les captures de paquets souhaitées.*

Configurez les politiques de DNS pour protéger votre réseau des requêtes DNS et des domaines malveillants. Pour une sécurité optimale, utilisez le service de sécurité DNS pour sécuriser votre trafic DNS. Sinon, utilisez des ensembles de signatures DNS téléchargeables et disponibles localement (fournis avec les mises à jour antivirus et WildFire).

L’utilisation du trafic malveillant Sinkhole au lieu du blocage 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. Pour les catégories de domaines qui représentent une menace plus importante, configurez un niveau de gravité des journaux et/ou des paramètres de capture de paquets plus élevés pour vous aider à déterminer si l’attaque a réussi, identifier les méthodes d’attaque et fournir un meilleur contexte global.

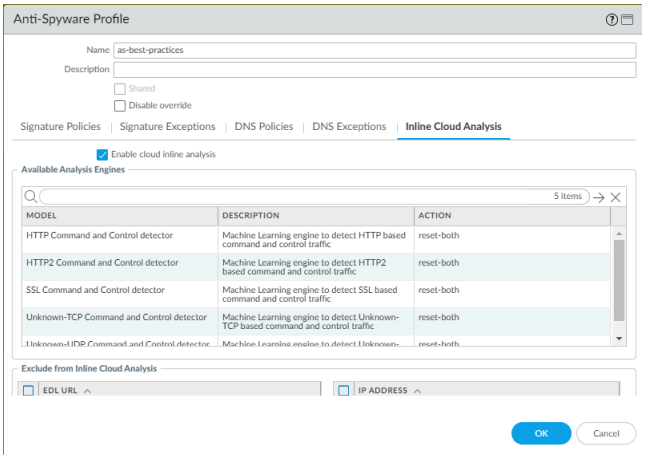
Configurez le DNS par défaut de Palo Alto Networks et les catégories de sources de signature DNS individuelles (PAN-OS 10.0 et versions ultérieures) :

Signature DNS source	Gravité des journaux	Action de politique	Capture de paquets
Contenu Palo Alto Networks			

Signature DNS source	Gravité des journaux	Action de politique	Capture de paquets
default-paloalto-dns	par défaut	sinkhole	extended-capture
Sécurité DNS			
Domaines de commande et contrôle	élevé (par défaut)	sinkhole	extended-capture
Domaines DNS dynamiques hébergés	informatif (par défaut)	sinkhole	un seul paquet
Domains de logiciels indésirables	faible (par défaut)	sinkhole	un seul paquet
Domaines de logiciels malveillants	moyen (par défaut)	sinkhole	un seul paquet
Domaines parqués	informatif (par défaut)	sinkhole	désactiver (par défaut)
Domaines de hameçonnage	faible (par défaut)	sinkhole	un seul paquet
Contournement de proxy et anonymiseurs	faible (par défaut)	sinkhole	un seul paquet
Domaines nouvellement enregistrés	informatif (par défaut)	sinkhole	un seul paquet
Domaines de suivi des publicités	informatif (par défaut)	sinkhole	un seul paquet

Pour **Inline Cloud Analysis (Analyse cloud en ligne)** (nécessite un abonnement Prévention des menaces avancée), sélectionnez **Enable cloud inline analysis (Activer l'analyse cloud en ligne)** pour tout le trafic sortant. Définissez l'**Action** sur **reset-both (réinitialiser les deux)** pour tous les modèles.

Les environnements isolés ne peuvent pas utiliser la prévention des menaces avancée, car il s'agit d'un service cloud qui nécessite une connexion cloud.



Profil de URL Filtering exemplaire pour la passerelle Internet

Utilisez le filtrage des URL avancé pour empêcher l'accès à du contenu web qui présente un risque élevé d'activité douteuse. Joignez un profil de filtrage des URL à toutes les règles qui autorisent l'accès à des applications web afin de vous protéger contre des URL qui ont déjà hébergé des logiciels malveillants, potentiellement malveillants, un risque de responsabilité et du contenu d'exploitation selon Palo Alto Networks.

Vous devez activer le décryptage pour profiter du filtrage des URL, car vous devez décrypter le trafic pour révéler l'URL exacte afin que le pare-feu puisse prendre la mesure appropriée. Au minimum, décryptez le trafic à risque élevé et moyen.

Pour garantir la disponibilité des applications critiques pour l'entreprise, Transition des profils de filtrage des URL en toute sécurité vers les meilleures pratiques. Un profil de filtrage des URL basé sur les meilleures pratiques définit toutes les catégories d'URL dangereuses connues et les soumissions d'informations d'identification à bloquer. Le but est de bloquer les catégories suivantes :

- Définissez toutes les actions pour les catégories d'URL malveillantes afin de bloquer à la fois l'accès au site et la soumission des informations d'identification de l'utilisateur. Faites des exceptions appropriées pour les tests PEN, la recherche sur les menaces et la sécurité des informations, si nécessaire :
  - **command-and-control (commande et contrôle)** : URL et domaines que les logiciels malveillants ou les systèmes compromis utilisent pour communiquer avec le serveur distant d'un pirate.
  - **grayware (logiciel indésirable)** : ces sites ne répondent pas à la définition d'un virus et ne constituent pas une menace directe pour la sécurité, mais ils incitent les utilisateurs à accorder un accès à distance ou à effectuer d'autres actions non autorisées. Les sites de logiciels indésirables incluent les escroqueries, les activités illégales, les activités criminelles, les logiciels publicitaires et autres applications indésirables et non sollicitées, y compris le « typosquattage » de domaines.
  - **malware (logiciel malveillant)** : sites connus pour héberger des logiciels malveillants ou qui sont utilisés pour des activités de commande et de contrôle.
  - **phishing (hameçonnage)** : sites connus pour héberger des pages visant à obtenir des informations d'identification et personnelles par hameçonnage, y compris des escroqueries au support technique et des scarewares.
  - **ransomware** : sites connus pour distribuer des ransomwares.

- **scanning-activity (activité d’analyse)** : sites qui recherchent les vulnérabilités existantes ou mènent des attaques ciblées.

- Certaines catégories d’URL présentent un fort potentiel malveillant, mais ne le sont pas nécessairement. Définissez toutes les actions pour ces catégories d’URL afin de bloquer à la fois l’accès au site et la

soumission des informations d'identification de l'utilisateur. Faites des exceptions appropriées pour les tests PEN, la recherche sur les menaces et la sécurité des informations, si nécessaire :

- **dynamic-dns (DNS dynamique)** : systèmes dont les adresses IP sont dynamiquement attribuées et qui sont souvent utilisés pour transmettre des charges utiles malveillantes ou des logiciels malveillants de commande et de contrôle.

  Si vous avez un objectif commercial pour un domaine DNS dynamique, assurez-vous de mettre d'autoriser ces URL dans votre profil de URL Filtering.

- **hacking (piratage)** : sites liés à l'accès ou à l'utilisation illégale ou douteuse d'équipements et de logiciels. Comprend les sites qui facilitent le contournement des systèmes de licences et de droits numériques.

  Faites des exceptions à cette catégorie pour les utilisateurs appropriés des tests PEN et de la recherche sur les menaces.

- **insufficient-content (contenu insuffisant)** : sites web et services qui présentent des pages de test, n'ont pas de contenu, fournissent un accès API non destiné à l'affichage de l'utilisateur final ou nécessitent une authentification sans afficher aucun autre contenu.
- **newly-registered-domains (domaines nouvellement enregistrés)** : domaines que les algorithmes de génération de domaines génèrent souvent ou que des acteurs malveillants génèrent pour des activités malveillantes.
- **not-resolved (non résolu)** : si le cloud PAN-DB est inaccessible et que l'URL ne se trouve pas dans le cache de filtrage des URL du pare-feu, le pare-feu ne peut pas résoudre et identifier la catégorie d'URL.

  *Pour une sécurité maximale, activez **Hold client request for category lookup (Garder en mémoire la demande du client pour la recherche de catégorie)** afin de donner au pare-feu plus de temps pour résoudre la catégorie d'URL. Cela prolonge le temps dont dispose le pare-feu pour interroger le type de catégorie à partir du cloud et entraîne une meilleure sécurité, mais peut augmenter la latence.*

- **parked (parqué)** : domaines qui seront souvent utilisés à des fins d'hameçonnage d'informations d'identification ou de vol d'informations personnelles.
- **proxy-avoidance-and-anonymizers (contournement des proxys et anonymiseurs)** : URL et services qui sont souvent utilisés pour contourner des produits de filtrage de contenu.
- **unknown (inconnu)** : sites qui n'ont pas encore été identifiés par Palo Alto Networks (PAN-DB).

  Les mises à jour en temps réel de PAN-DB détectent les sites inconnus après la première tentative d'accès à un site inconnu, de sorte que le pare-feu identifie rapidement les URL inconnues et les traite ensuite en fonction de la catégorie d'URL réelle du site.

  Si la disponibilité est importante pour votre entreprise et que vous devez autoriser le trafic depuis des sites inconnus, appliquez au trafic les profils de sécurité les plus stricts et enquêtez sur toutes les alertes du trafic.

- Définissez l'action pour l'accès au site et la soumission des informations d'identification de l'utilisateur afin de bloquer les catégories d'URL suivantes en fonction des exigences légales ou commerciales et

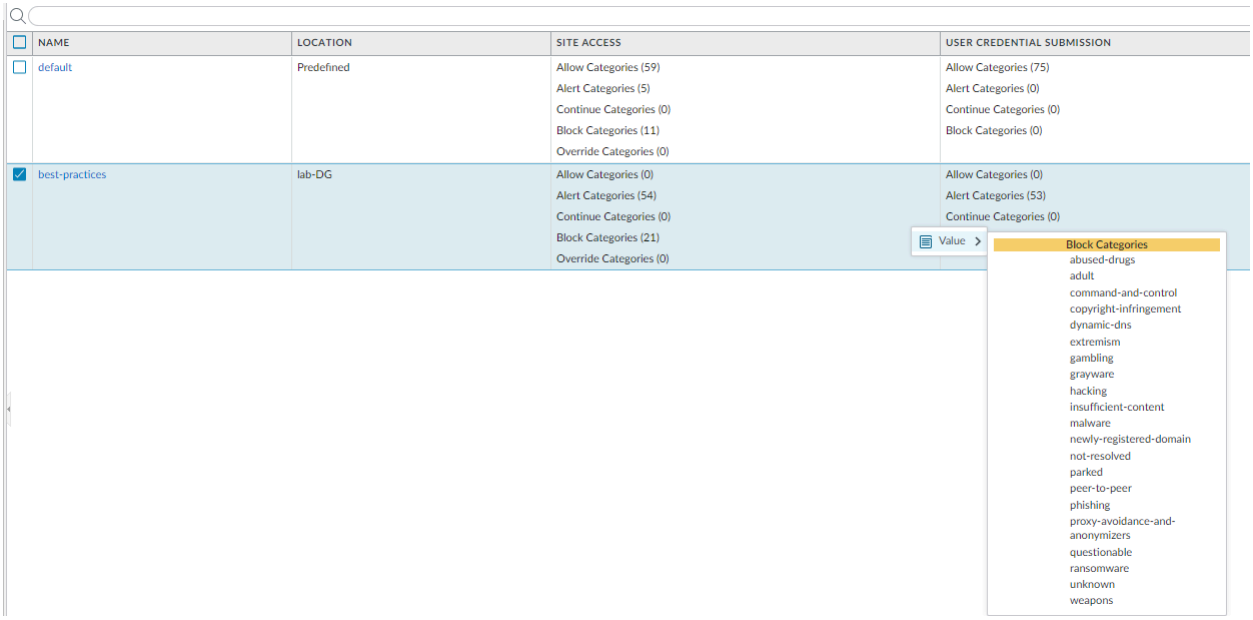
du risque de responsabilité potentiel. Si vous ne bloquez pas ces sites, activez les alertes à leur sujet et appliquez des profils de sécurité stricts au trafic.

- **abused-drugs (usage illicite des drogues)** : sites qui promeuvent l'abus de drogues illégales et légales.
- **adult (adulte)** : tous les sites présentant du contenu pour adultes de toute nature, y compris des jeux et des bandes dessinées ainsi que du matériel, des médias, des œuvres d'art, des forums et des services sexuellement explicites.
- **copyright-infringement (violation des droits d'auteur)** : domaines ayant un contenu illégal qui présente un risque de responsabilité.
- **extremism (extrémisme)** : sites web faisant la promotion du terrorisme, du racisme, de l'exploitation des enfants, etc.
- **gambling (jeux d'argent)** : sites de loterie et de jeux d'argent.
- **peer-to-peer** : partage peer-to-peer de torrents, de programmes de téléchargement, de fichiers multimédias ou d'autres applications logicielles. (N'inclut pas les sites de partagiciel ou de logiciels gratuits.)
- **questionable (douteux)** : sites faisant la promotion d'un humour de mauvais goût et de contenus offensants ciblant des groupes spécifiques.
- **weapons (armes)** : vente, critique, descriptions ou instructions concernant les armes et leur utilisation.

Réfléchissez également à la manière dont vous souhaitez gérer les catégories d'URL de cryptomonnaie et d'alcool et de tabac. Activez les alertes à leur sujet et appliquez des profils de sécurité stricts au trafic ou bloquez-les, en fonction des besoins de votre entreprise.

- Bloquez l'envoi des informations d'identification de l'utilisateur pour la catégorie à haut risque. (Ne bloquez pas l'accès au site pour la catégorie à haut risque.)

En plus de bloquer les catégories connues comme malveillantes, activez les alertes pour toutes les autres catégories afin d'avoir une visibilité sur tous les sites que vos utilisateurs consultent. Si vous devez introduire progressivement une politique de blocage, définissez des catégories pour continuer et procédez à la création d'une page de réponse personnalisée pour informer vos utilisateurs de vos politiques d'utilisation acceptable et les prévenir qu'ils consultent un site qui pourrait présenter une menace. Cela vous ouvre la voie pour que vous puissiez bloquer les catégories à l'issue d'une période de surveillance.



Désactivez l'option **Log Container Page Only (Consigner la page de conteneur uniquement)** dans le profil, qui est activée par défaut. Si vous consignez uniquement les pages du conteneur, vous perdez la visibilité sur les applications fonctionnelles telles que la publication, le chargement, le téléchargement, etc. Désactivez l'option **Log Container Page Only (Consigner la page de conteneur uniquement)** pour voir le journal complet pour pouvoir voir la véritable application fonctionnelle.

Si votre environnement est une école qui reçoit un financement fédéral, activez l'option **Safe Search Enforcement (Mise en œuvre de la recherche sécurisée)** (exigence légale).

Si vous exécutez PAN-OS 9.0.4 ou une version ultérieure, activez l'option permettant de conserver les requêtes client (entrez **`config`**, puis **`set deviceconfig setting ctd hold-client-request yes`**) pour garantir que le pare-feu gère les requêtes web des utilisateurs de la manière la plus sécurisée possible. Par défaut, le pare-feu autorise les requêtes pendant qu'il recherche une catégorie d'URL non mise en cache dans PAN-DB puis applique la politique adaptée lorsque le serveur répond. Suspendez les requêtes pendant cette recherche pour maximiser la sécurité (cela peut augmenter la latence, mais constitue l'option la plus sécurisée). Pour plus de détails, reportez-vous à la section Configuration du URL Filtering.

Que faire si je n'arrive pas à bloquer toutes les catégories recommandées ?

Si les utilisateurs ont besoin d'accéder à des sites appartenant à des catégories bloquées à des fins professionnelles, créez une liste d'autorisations uniquement pour les sites spécifiques dans une règle qui autorise uniquement les utilisateurs et applications nécessaires, si vous estimez que le risque est justifié. Tenez compte des lois et réglementations locales qui régissent les types de sites que vous pouvez bloquer, ne pas bloquer et que vous devez bloquer. Pour les catégories à risque pour lesquelles vous décidez d'autoriser l'accès, configurez une protection contre l'hameçonnage des informations d'identification pour garantir que les utilisateurs ne soumettent pas leurs informations d'identification d'entreprise à un site susceptible d'héberger une attaque d'hameçonnage.

Si vous autorisez le trafic vers des catégories d'URL malveillantes et potentiellement malveillantes ou vers des sites web qui posent des problèmes potentiels de responsabilité, les risques incluent :

- Catégories d’URL malveillantes :
  - **Command-and-control (Commande et contrôle)** : Les URL et les domaines de commande et contrôle utilisés par les logiciels malveillants et autres systèmes compromis pour communiquer discrètement avec le serveur à distance d’un pirate afin de recevoir des commandes malveillantes ou d'exfiltrer des données.
  - **grayware (logiciel indésirable)** : sites web et services qui ne correspondent pas à la définition d’un virus, mais qui sont malveillants ou douteux et qui peuvent compromettre la performance du périphérique et causer des risques d’atteinte à la sécurité. Avant la version de contenu 8206, le pare-feu plaçait les logiciels indésirables dans la catégorie des URL malveillantes ou douteuses. Si vous n’êtes pas certain de devoir bloquer les logiciels indésirables, commencez par placer des alertes à l’égard des logiciels indésirables et enquêter sur les alertes, puis décider si vous devez bloquer les logiciels indésirables ou continuer à recevoir des alertes à leur égard.
  - **malware (logiciel malveillant)** : sites qui sont reconnus pour héberger des logiciels malveillants ou qui sont utilisés pour du trafic de commande et de contrôle (C2) et susceptibles de contenir des kits d’attaque.
  - **phishing (hameçonnage)** : sites qui sont reconnus pour héberger des pages de phishing pour obtenir les informations de connexion ou pour tenter d'obtenir les identifiants personnels par hameçonnage.
  - **ransomware** : sites connus pour distribuer des ransomwares.
  - **scanning-activity (activité d’analyse)** : sites qui recherchent les vulnérabilités existantes ou mènent des attaques ciblées.
- Catégories d’URL potentiellement malveillantes :
  - **dynamic-DNS (DNS dynamique)** : noms d’hôtes et de domaines de systèmes dont les adresses IP sont dynamiquement attribuées et qui sont souvent utilisés pour transmettre des charges utiles malveillantes ou du trafic C2. De plus, les domaines DNS dynamiques ne passent pas par le même processus de contrôle que les domaines qui sont enregistrés par une société spécialisée dans l’enregistrement de noms de domaine qui est digne de confiance ; ils sont donc moins fiable.
  - **hacking (piratage)** : sites liés à l’accès ou à l’utilisation illégale ou douteuse d’équipements et de logiciels. Comprend les sites qui facilitent le contournement des systèmes de licences et de droits numériques.

    Faites des exceptions à cette catégorie pour les utilisateurs appropriés des tests PEN et de la recherche sur les menaces.
  - **insufficient-content (contenu insuffisant)** : sites web et services qui présentent des pages de test, n’ont pas de contenu, fournissent un accès API non destiné à l’affichage de l’utilisateur final ou nécessitent une authentification sans afficher aucun autre contenu.
  - **newly-registered-domain (domaine nouvellement enregistré)** : les domaines nouvellement enregistrés sont souvent générées volontairement ou par les algorithmes de génération de domaines et utilisés pour mener des activités malveillantes.

- **not-resolved (non résolu)** : si le cloud PAN-DB est inaccessible et que l'URL ne se trouve pas dans le cache de filtrage des URL du pare-feu, le pare-feu ne peut pas résoudre et identifier la catégorie d'URL.

  *Pour une sécurité maximale, activez **Hold client request for category lookup (Garder en mémoire la demande du client pour la recherche de catégorie)** afin de donner au pare-feu plus de temps pour résoudre la catégorie d'URL. Cela prolonge le temps dont dispose le pare-feu pour interroger le type de catégorie à partir du cloud et entraîne une meilleure sécurité, mais peut augmenter la latence.*

- **parked (en parking)** : domaines enregistrés par des personnes ; on découvre souvent plus tard qu'ils ont servi à usurper des informations de connexion . Ces domaines peuvent ressembler à des domaines légitimes, par exemple, pal0alto0netw0rks.com ; ils servent toutefois à usurper des informations de connexion ou des informations personnelles. Il peut également s'agir de domaines pour lesquels une personne a acheté les droits dans l'espoir qu'ils aient un jour de la valeur, par exemple panw.net.
- **proxy-avoidance-and-anonymizers (contournement des proxys et anonymiseurs)** : URL et services qui sont souvent utilisés pour contourner des produits de filtrage de contenu.
- **Unknown (inconnu)** : sites qui n'ont pas encore été identifiés par PAN-DB. Si la disponibilité est importante pour votre entreprise et que vous devez autoriser le trafic, demandez qu'une alerte soit envoyée en présence de sites inconnus, appliquez au trafic les profils de sécurité recommandés et enquêtez sur les alertes.

  Les mises à jour en temps réel de PAN-DB prennent connaissance des sites inconnus après la première tentative d'accès à ces derniers. Les URL inconnues sont donc identifiés rapidement et deviennent des URL connues que le pare-feu peut gérer en fonction de la véritable catégorie d'URL.

- Catégories d'URL présentant un risque de responsabilité potentiel :
  - **abused-drugs (usage illicite des drogues)** : sites web qui font la promotion de l'abus de drogues légales et illégales, de la vente et de l'utilisation d'accessoires liés à la drogue, ainsi que de la fabrication ou de la vente de drogues.
  - **adult (adulte)** : sites web qui pourraient ne pas être appropriés sur le lieu de travail.
  - **Copyright-infringement (infraction au droit d'auteur)** : domaines dont le contenu est illégal, par exemple du contenu qui permet le téléchargement illégal de logiciels ou d'autres propriétés intellectuelles, ce qui présente un risque de responsabilité eventuel. Cette catégorie a été ajoutée pour assurer le respect des lois en matière de protection des enfants au sein de l'industrie de l'éducation ainsi que des lois des pays qui exigent que les fournisseurs Internet empêchent les utilisateurs de partager du matériel protégé par des droits d'auteur via leur service.
  - **Extremism (extrémisme)** : les sites Web faisant la promotion du terrorisme, du racisme, du fascisme ou d'autres points de vue extrémistes discriminant des gens ou des groupes d'origines ethniques différentes, d'autres religions ou d'autres croyances. Cette catégorie a été ajoutée pour assurer le respect des lois en matière de protection des enfants au sein de l'industrie de l'éducation. Dans certaines régions, les lois et règlements peuvent interdire l'accès aux sites extrémistes, et l'autorisation de l'accès peut présenter un risque de responsabilité.
  - **gambling (jeux d'argent)** : sites web de loterie ou de jeux d'argent qui facilitent l'échange d'argent réel et/ou virtuel. Également des sites web proposant des didacticiels, des conseils ou d'autres informations sur les jeux d'argent, y compris les cotes de paris et les pools.

- **peer-to-peer** : sites web auxquels les clients accèdent ou qui souhaitent partager des torrents, des programmes de téléchargement, des fichiers multimédias ou d'autres applications logicielles, principalement pour se protéger contre les capacités de téléchargement bitTorrent. N'inclut pas les sites de partagiciel ou de logiciels gratuits.
- **questionable (douteux)** : sites web contenant du contenu potentiellement offensant ciblant des groupes ou des individus spécifiques, des activités criminelles, des activités illégales et des programmes d'enrichissement rapide.
- **weapons (armes)** : sites web qui vendent, examinent, décrivent ou fournissent des instructions sur les armes et leur utilisation qui pourraient ne pas être appropriées sur le lieu de travail.

Le profil de filtrage des URL par défaut bloque les catégories d'URL malware (logiciel malveillant), phishing (hameçonnage), et command-and-control (commande et contrôle), mais pas le reste des catégories qu'il est recommandé de bloquer. Le profil de filtrage des URL par défaut bloque également les catégories D'URL relatives à la toxicomanie, aux sites destinés aux adultes, aux jeux et aux armes ainsi que celles qui sont discutables. Le décision de bloquer ces catégories dépend de vos exigences d'affaires. Par exemple, une université ne limitera probablement pas l'accès des étudiants à la plupart de ces sites, car la disponibilité est importante, mais une entreprise qui accorde la priorité à la sécurité peut tous les bloquer.

Exemples de URL Filtering

Le filtrage des URL fonctionne avec les fonctionnalités de blocage de fichiers, décryptage, listes dynamiques externes (EDL), journalisation et d'autres fonctionnalités de sécurité pour créer des règles granulaires pouvant aller au-delà du simple blocage ou de la simple autorisation de catégories entières d'URL. Utilisez les étapes de transition en toute sécurité du filtrage des URL pour évaluer quels sites vous souhaitez autoriser et quels sites vous souhaitez bloquer pour mettre en œuvre des politiques qui répondent aux exigences de votre entreprise. Par exemple :

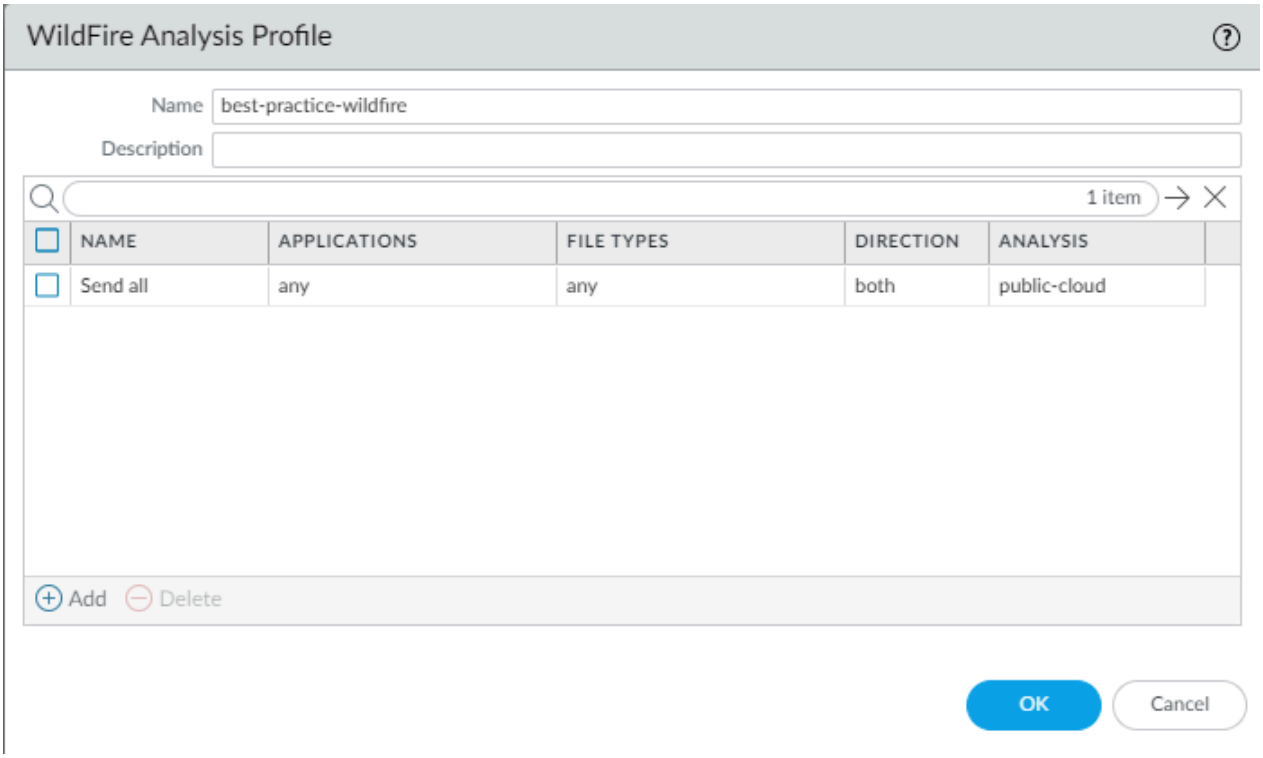
- Utilisez des catégories d'URL basées sur le risque (risque élevé, risque moyen et risque faible) en combinaison avec d'autres catégories d'URL pour cibler le décryptage ou le blocage du trafic. Par exemple, vous pouvez :
  - Bloquer le trafic vers les sites web à haut risque dans la catégorie des services financiers.
  - Décrypter tout le trafic web à haut et à moyen risque.
  - Décrypter le trafic à risque élevé et moyen vers des catégories d'URL spécifiques si le pare-feu ne dispose pas de ressources suffisantes pour décrypter tout le trafic que vous souhaitez décrypter.
- Consigner tous les agents d'utilisateurs et référents, toutes les URL et tous les téléchargements de fichiers pour les domaines de catégories à risque élevé et moyen afin d'accroître la visibilité.
- Autoriser l'accès à des catégories telles que sites personnels et blogues lors de l'application d'un profil de blocage de fichiers au trafic afin d'empêcher le téléchargement de contenu à risque tel que .exe, .scr et d'autres fichiers potentiellement malveillants.
- Utilisez l'EDL prédéfinie **Palo Alto Networks - Bulletproof IP addresses (Palo Alto Networks - Adresses IP bulletproof)** pour empêcher l'accès aux sites hébergés chez des ISP bulletproof, en particulier si vous autorisez l'accès à des sites financiers à haut ou à risque moyen.
- Utiliser des combinaisons de catégories d'URL pour simplifier la politique.

Profil d’analyse WildFire exemplaire pour la passerelle Internet

Transférez des fichiers vers WildFire pour analyse afin de protéger votre réseau contre les menaces inconnues. Sans cette protection, les pirates peuvent s’infiltrer dans votre réseau et exploiter les vulnérabilités des applications que vos employés utilisent quotidiennement. Étant donné que WildFire vous protège contre les menaces inconnues, il est votre meilleure protection contre les menaces persistantes avancées (APT).

Paramétrez les mises à jour de contenu pour un appareil WildFire pour qu’elles soient téléchargées et installées de manière automatique en temps réel, vous assurant ainsi le support le plus actualisé.

Le profil d’analyse WildFire Analysis exemplaire envoie tous les fichiers dans les deux directions (chargement et téléchargement) vers WildFire à des fins d’analyse. Plus particulièrement, assurez-vous d’envoyer tous les fichiers PE (si vous ne les bloquez pas conformément aux recommandations en matière de blocage de fichiers), Adobe Flash et Reader (PDF, SWF), Microsoft Office (PowerPoint, Excel, Word, RTF), Java (Java, .CLASS) et Android (.APK).



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, (sinon, 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.*

Définition de la politique de sécurité initiale des passerelles Internet

L’objectif d’une politique de sécurité des passerelles Internet basée sur les meilleures pratiques est l’application positive des applications autorisées. Cependant, il faut du temps pour identifier les applications exactes qui fonctionnent sur votre réseau, les applications critiques pour votre entreprise et les personnes qui ont besoin d’accéder à chaque application. Pour créer une politique de sécurité basée sur des règles d’autorisation des applications, commencez par une base de règles qui autorise librement les applications que vous approuvez officiellement pour les utilisateurs, et tolère les applications professionnelles générales et les applications personnelles (si elles sont appropriées pour votre entreprise).

La politique initiale comprend des règles qui bloquent explicitement les adresses IP et les applications malveillantes connues, ainsi que des règles d’autorisation temporaire qui permettent d’affiner votre politique et de préserver la disponibilité des applications pendant la période de transition vers une politique de meilleures pratiques.

Pour appliquer la politique de sécurité uniformément à plusieurs endroits, vous pouvez réutiliser des modèles ou des piles de modèles pour que les mêmes politiques s’appliquent à chaque pare-feu de la passerelle Internet de chaque emplacement. Les modèles utilisent des variables afin d’appliquer des valeurs spécifiques aux périphériques, telles que des adresses IP, des 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.

Les rubriques suivantes décrivent comment créer la base de règles initiale, expliquent pourquoi chaque règle est nécessaire et mettent en lumière les risques liés à l’ignorance des recommandations en matière de bonnes pratiques :

- Étape 1 : Création de règles basées sur des sources de confiance de prévention des menaces
- Étape 2 : Création des règles d’autorisation pour les applications
- Étape 3 : Création des règles relatives au blocage d’applications
- Étape 4 : Création des règles de mise au point temporaires
- Étape 5 : Activez la journalisation du trafic qui ne correspond à aucune règle

Étape 1 : Création de règles basées sur des sources de confiance de prévention des menaces

Bloquez le trafic provenant d’hôtes identifiés par Palo Alto Networks et des tiers de confiance comme malveillants. Une licence Prévention avancée des menaces (ou une licence Prévention des menaces héritée active) comprend des listes dynamiques externes (EDL) intégrées contenant des adresses IP malveillantes connues. Utilisez les EDL dans la politique pour bloquer le trafic malveillant. Palo Alto Networks compile et met à jour dynamiquement les listes sur la base des dernières informations sur les menaces. Les pare-feu reçoivent et implémentent les mises à jour dynamiques sans nécessiter de redémarrage.

STEP 1 | Bloquez le trafic en direction de et en provenance d'adresses IP identifiées par Palo Alto Networks comme malveillantes.

Pourquoi ai-je besoin de ces règles ?	Points clés de la règle
❑ Cette règle vous protège des adresses IP dont Palo Alto Networks a prouvé qu'elles ne servaient pratiquement qu'à distribuer des logiciels malveillants, entreprendre une activité de commande et contrôle, et déclencher des attaques.	• Une règle bloque le trafic sortant vers des adresses IP identifiées comme malveillantes, tandis qu'une autre règle bloque le trafic entrant depuis ces adresses. • Établissez la liste dynamique externe **Palo Alto Networks - Known malicious IP addresses (Palo Alto Networks - Adresses IP identifiées comme malveillantes)** comme adresse de destination pour la règle de trafic sortant, et comme adresse source pour la règle de trafic entrant. • Refusez tout trafic correspondant à ces règles. • Activez la journalisation du trafic correspondant à ces règles, pour pouvoir enquêter sur les menaces éventuelles qui existent sur votre réseau. • Étant donné que ces règles interrompent le trafic malveillant, elles protègent le trafic provenant de tout utilisateur s'exécutant sur n'importe quel port.

		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Drop Outbound Malicious IP	universal	any	any	any	any	any	Palo Alto Networks - Known malicio...	any	any	any	Deny	none	
Drop Inbound Malicious IP	universal	any	Palo Alto Networks - Known malic...	any	any	any	any	any	any	any	Deny	none	

STEP 2 | Bloquez le trafic en provenance et à destination des fournisseurs d'hébergement Bulletproof.

Pourquoi ai-je besoin de ces règles ?	Points clés de la règle
❑ Cette règle vous protège contre les adresses IP dont Palo Alto Networks a démontré l'appartenance à des fournisseurs d'hébergement Bulletproof. Les fournisseurs d'hébergement Bulletproof n'ont pas ou peu de restrictions sur le contenu et ne consignent pas les événements. Les sites Bulletproof sont ainsi idéaux pour lancer des attaques de commande et contrôle (C2) et des activités illégales, car tout est permis et rien n'est suivi.	• Une règle bloque le trafic sortant vers des adresses IP des fournisseurs d'hébergement Bulletproof, tandis qu'une autre règle bloque le trafic entrant depuis ces adresses. • Définissez la liste dynamique externe **Palo Alto Networks - Bulletproof IP addresses** (Palo Alto Networks - Adresses IP Bulletproof) comme Destination address (Adresse de destination) pour la règle de trafic sortant et comme Source address (Adresse source) pour la règle de trafic entrant. • Refusez tout trafic correspondant à ces règles.

Pourquoi ai-je besoin de ces règles ?	Points clés de la règle
	• Activez la journalisation du trafic correspondant à ces règles, pour pouvoir enquêter sur les menaces éventuelles qui existent sur votre réseau. • Étant donné que ces règles interrompent le trafic malveillant, elles protègent le trafic provenant de tout utilisateur s'exécutant sur n'importe quel port.

		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Drop Outbound Bulletproof IP	universal	any	any	any	any	any	Palo Alto Networks - Bulletproof IP ...	any	any	any	Deny	none	
Drop Inbound Bulletproof IP	universal	any	Palo Alto Networks - Bulletproof I...	any	any	any	any	any	any	any	Deny	none	

STEP 3 | Bloquez et consignez le trafic en provenance de et à destination d'adresses IP à haut risque identifiées par des avis de confiance relatifs aux menaces.

Pourquoi ai-je besoin de ces règles ?	Points clés de la règle
Même si Palo Alto Networks n'a pas de preuve directe de la malveillance d'une adresse IP figurant dans le flux d'adresses IP à haut risque, des avis de confiance relatifs aux menaces les ont associées à des comportements malveillants. ❑ Bloquez et consignez le trafic comme indiqué dans cet exemple. ❑ Si vous devez autoriser une adresse IP à haut risque pour des raisons professionnelles, créez une règle de politique de sécurité avec des profils de sécurité stricts qui n'autorise que cette adresse IP et placez-la devant la règle de blocage des adresses IP à haut risque dans la base de règles. Surveillez de près et enregistrez toutes les adresses IP à haut risque que vous choisissez d'autoriser.	• Une règle consigne le trafic sortant bloqué vers des adresses IP à haut risque, et une autre règle consigne le trafic entrant bloqué depuis ces adresses. • Établissez la liste dynamique externe **Palo Alto Networks - High risk IP addresses (Palo Alto Networks - Adresses IP à haut risque)** comme adresse de destination pour la règle de trafic sortant, et comme adresse source pour la règle de trafic entrant. • Si vous autorisez le trafic, appliquez les meilleures pratiques relatives aux profils de sécurité. • Étant donné que ces règles interrompent le trafic malveillant, elles protègent le trafic provenant de tout utilisateur s'exécutant sur n'importe quel port, pour n'importe quelle application.

		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Block Outbound High Risk IPs	universal	any	any	any	any	any	Palo Alto Networks - High risk IP addresses	any	any	any	Deny	none	
Block Inbound High Risk IPs	universal	any	Palo Alto Networks - Known malicious IP addresses	any	any	any	any	any	any	any	Deny	none	

STEP 4 | De même, créez deux règles qui bloquent et consignent le trafic vers et depuis les nœuds de sortie Tor, qui sont souvent (mais pas toujours) associés à des activités malveillantes, en particulier dans les

environnements d'entreprise, à l'aide de la liste dynamique externe **Palo Alto Networks Tor Exit IP Addresses (Palo Alto Networks - Adresses IP de sortie Tor)**.

Étape 2 : Création des règles d'autorisation pour les applications

Identifiez votre liste de confiance pour les applications avant de créer des règles d'autorisation pour les applications. Créez des règles d'autorisation basées sur des applications et non sur des ports. À l'exception de certaines applications d'infrastructure qui requièrent l'accès de l'utilisateur avant que le pare-feu ne puisse l'identifier, n'autorisez l'accès qu'aux utilisateurs connus. Procédez à la création de groupes d'utilisateurs pour l'accès aux applications autorisées afin de restreindre l'accès aux utilisateurs ou aux groupes particuliers qui doivent accéder à chaque application dans le cadre de leurs activités.

Pour convertir les règles basées sur les ports en règles basées sur les applications ou pour migrer d'un pare-feu basé sur les ports, suivez les conseils des meilleures pratiques pour une migration vers une politique basée sur les applications*, qui s'appuient sur* l'optimiseur de politique*. L'optimiseur de politique vous aide à analyser les règles basées sur les ports et vous indique les applications exactes qui correspondent à ces règles. Il vous aide également à trouver les règles inutilisées, les règles avec des applications inutilisées (règles surdimensionnées) et les règles existantes basées sur les ports.*

Placez les règles spécifiques au-dessus des règles générales dans la base de règles de la politique de sécurité. Sinon, une règle générale pourrait occulter une règle spécifique. (L'occultation consiste à placer une règle générale qui inclut les mêmes critères de correspondance qu'une règle plus spécifique plus haut dans la base de règles que la règle spécifique, de sorte que le trafic destiné à correspondre à la règle spécifique correspond plutôt à la règle générale.)

La première partie de la base de règles comprend les règles d'autorisation applicables aux applications que vous avez identifiées dans la liste d'autorisation des applications, notamment :

- Les applications approuvées que vous obtenez et gérez à des fins professionnelles et d'infrastructure.
- Les applications commerciales générales dont les utilisateurs peuvent avoir besoin pour accomplir leur travail.
- Les applications tolérées que vous choisissez d'autoriser pour un usage personnel.

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.*

Associez des profils de sécurité aux meilleures pratiques afin d'analyser tout le trafic autorisé pour détecter les menaces connues et inconnues. Si vous n'avez pas créé ces profils, vous devez alors créer des profils de sécurité exemplaires pour la passerelle Internet. Parce que vous ne pouvez pas inspecter ce que vous ne voyez pas, configurez le pare-feu pour qu'il procède au Décryptage du trafic pour une visibilité complète et pour l'inspection des menaces.

STEP 1 | Autorisez l’accès à vos serveurs DNS d’entreprise.

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

Pourquoi ai-je besoin de cette règle ?	Points clés de la règle
❑ L’accès DNS offre des services d’infrastructure réseau et est généralement exploité par les pirates. ❑ N’autorisez l’accès que sur votre serveur DNS interne pour réduire votre surface d’attaque.	• Étant donné que cette règle est très précise, placez-la près de la base de règles. • Créez un objet d’adresse à utiliser pour l’adresse de destination afin de garantir que les utilisateurs n’accèdent qu’au serveur DNS de votre centre de données. • Puisque les utilisateurs ont besoin d’accéder à ces services avant de se connecter, autorisez l’accès à tous les utilisateurs.

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
IT DNS Services	Best Practice	universal	Users	any	any	any	IT Infrastructure	DNS Servers	any	dns	application-default	Allow		

STEP 2 | Autorisez l’accès aux autres ressources de l’infrastructure informatique requises.

Pourquoi ai-je besoin de cette règle ?	Points clés de la règle
❑ Autorisez les applications qui sont à la base de votre infrastructure réseau et de vos fonctions de gestion, telles que NTP, OCSP, STUN et ping. ❑ Bien que le trafic DNS qui est autorisé à la règle précédente soit limité à l’adresse de destination du centre de données, ces applications pourraient ne pas se trouver dans votre centre de données et, par conséquent, exiger une règle distincte.	• Parce que ces applications s’exécutent sur le port par défaut, autorisez l’accès à tous les utilisateurs (les utilisateurs pourraient ne pas encore être connectés et connus en raison du moment dont ils ont besoin de ces services). De plus, comme elles possèdent une adresse de destination définie sur **any (indifférent)**, ajoutez-les à un groupe d’applications et créez une règle pour autoriser l’accès à l’ensemble de ces applications.

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Required Infrastructure	Best Practice	universal	Users	any	any	any	Internet	any	any	Required Infrastructure	application-default	Allow		

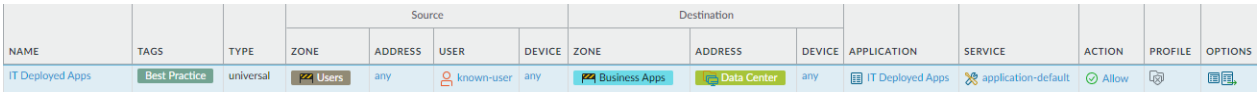
STEP 3 | Autorisez l’accès aux applications SaaS approuvées par les TI.

Pourquoi ai-je besoin de cette règle ?	Points clés de la règle
❑ Avec les applications SaaS, les données propriétaires résident dans le cloud. Cette règle garantit que seuls les utilisateurs connus ont	• Créez un groupe d’applications pour contrôler toutes les applications SaaS approuvées.

Pourquoi ai-je besoin de cette règle ?	Points clés de la règle
accès à ces applications (et aux données sous-jacentes). ❑ Analysez le trafic SaaS autorisé à la recherche de menaces.	• Les applications SaaS devraient toujours s'exécuter sur le port par défaut de l'application. • Restreindre l'accès aux utilisateurs connus. Reportez-vous à la section Création de groupes d'utilisateurs pour l'accès aux applications autorisées.

STEP 4 | Autorisez l'accès aux applications sur site obtenues par les TI.

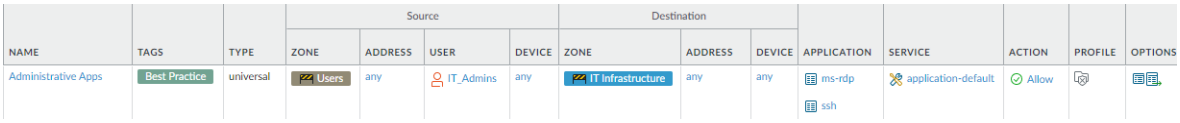
Pourquoi ai-je besoin de cette règle ?	Points clés de la règle
❑ Les attaques utilisent souvent des applications critiques du centre de données, telles que FTP, pendant la phase d'exfiltration ou exploitent les vulnérabilités de l'application pour se déplacer latéralement. ❑ De nombreuses applications de centre de données utilisent plusieurs ports. Il suffit de définir le Service sur **application-default (par défaut de l'application)** pour autoriser les applications en toute sécurité sur leurs ports standard. N'autorisez pas d'applications sur des ports non standard, puisque cela est souvent signe de comportement évasif.	• Créez un groupe d'applications pour regrouper toutes les applications de centres de données. • Créez un groupe d'adresses pour les adresses des serveurs de vos centres de données. • Restreindre l'accès aux utilisateurs connus. Reportez-vous à la section Création de groupes d'utilisateurs pour l'accès aux applications autorisées.



STEP 5 | Autorisez l'accès aux applications dont ont besoin vos utilisateurs administratifs.

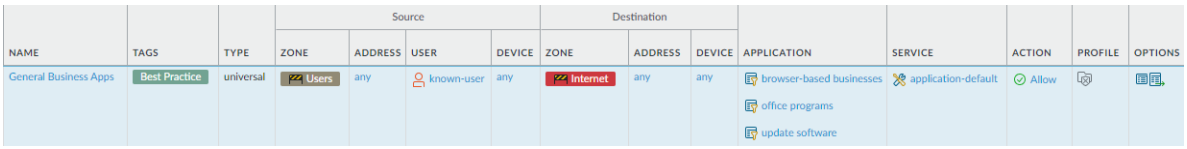
Pourquoi ai-je besoin de cette règle ?	Points clés de la règle
❑ Pour réduire votre surface d'attaque, procédez à la Création de groupes d'utilisateurs pour l'accès aux applications inconnues. ❑ Étant donné que les administrateurs ont souvent besoin d'accéder aux données sensibles du compte et d'accéder à distance aux autres systèmes (par exemple RDP), vous pouvez réduire votre surface d'attaque en	• Cette règle restreint l'accès aux utilisateurs qui figurent dans le groupe IT_admins. • Créez une application personnalisée pour chaque application interne ou pour chaque application qui s'exécute sur des ports non standard afin de les mettre en œuvre sur les ports par défaut plutôt que d'ouvrir des ports supplémentaires sur votre réseau.

Pourquoi ai-je besoin de cette règle ?	Points clés de la règle
n’autorisant l’accès qu’aux administrateurs qui en ont besoin dans le cadre de leurs activités.	• Si vous avez des groupes d’utilisateurs différents pour des applications différentes, créez des règles distinctes pour un contrôle granulaire.



STEP 6 | Autorisez l’accès aux applications commerciales générales.

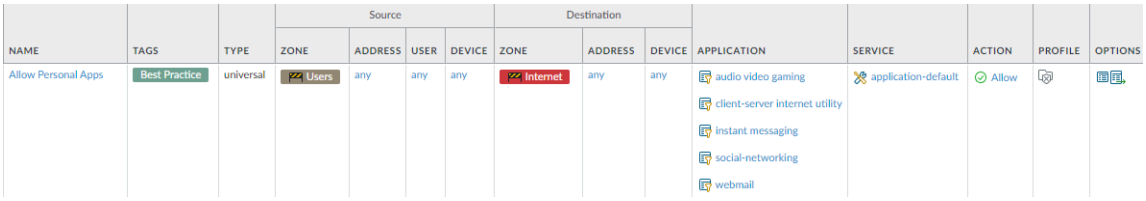
Pourquoi ai-je besoin de cette règle ?	Points clés de la règle
❑ Outre les applications que vous approuvez et administrez pour les utilisateurs, ces derniers ont souvent besoin d’accéder à d’autres applications professionnelles, telles que Zoom, les services en ligne d’Adobe ou G Suite. ❑ Cette règle vous permet d’autoriser en toute sécurité la navigation web tout en recherchant les menaces. Reportez-vous à la section Création de profils de sécurité exemplaires pour la passerelle Internet.	• Limitez l’accès aux seuls utilisateurs connus. Reportez-vous à la section Création de groupes d’utilisateurs pour l’accès aux applications autorisées. • Pour la visibilité, créez un filtre d’application pour chaque type d’applications que vous souhaitez autoriser. • Associez des profils de sécurité aux meilleures pratiques afin d’éviter les menaces connues et inconnues dans tout le trafic.



STEP 7 | (Facultatif) Autorisez l’accès aux applications personnelles.

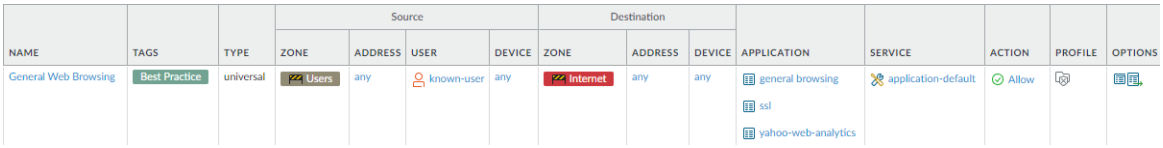
Pourquoi ai-je besoin de cette règle ?	Points clés de la règle
❑ À l’heure où la démarcation entre les périphériques professionnels et personnels s’estompe, il est essentiel de vous assurer que les applications auxquelles vos utilisateurs accèdent sont sécurisées et libres de toute menace. ❑ Utilisez des filtres d’applications pour sécuriser l’accès aux applications personnelles lorsque vous créez cette base de règles initiale. Une fois que vous avez évalué les applications qui sont utilisées, servez-vous de	• Limitez l’accès aux seuls utilisateurs connus. Reportez-vous à la section Création de groupes d’utilisateurs pour l’accès aux applications autorisées. • Pour la visibilité, créez un filtre d’application distinct pour chaque type d’applications que vous souhaitez autoriser. • Associez des profils de sécurité aux meilleures pratiques afin d’éviter les menaces connues et inconnues dans tout le trafic.

Pourquoi ai-je besoin de cette règle ?	Points clés de la règle
ces renseignements pour décider de retirer le filtre et d'autoriser un plus petit sous-réseau d'applications personnelles qui respectent vos politiques d'utilisation acceptable.	



STEP 8 | Autorisez la navigation Web générale.

Pourquoi ai-je besoin de cette règle ?	Points clés de la règle
❑ La règle précédente autorisait l'accès aux applications personnelles (dont un bon nombre sont basées sur le navigateur). Cette règle permet une navigation web générale. ❑ La navigation Web générale comporte plus de risques que les autres types de trafic d'applications. Afin de sécuriser la navigation web, procédez à la création de profils de sécurité exemplaires et associez-les à cette règle. ❑ Étant donné que les menaces se cachent souvent dans le trafic chiffré, procédez au décryptage du trafic pour une visibilité complète et pour l'inspection des menaces pour sécuriser la navigation web.	• Utilisez les mêmes profils de sécurité que les autres règles et renforcez le profil de filtrage des URL autant que possible. • Pour empêcher les périphériques ayant des logiciels malveillants ou les périphériques intégrés d'atteindre l'Internet, n'autorisez que les utilisateurs connus. • Utilisez des filtres d'applications pour permettre l'accès aux types généraux d'applications. • Autorisez explicitement SSL en tant qu'application pour autoriser les utilisateurs à consulter les sites HTTPS qui sont exclus du décryptage. • Définissez le Service sur **application-default (par défaut de l'application)**.



Étape 3 : Création des règles relatives au blocage d'applications

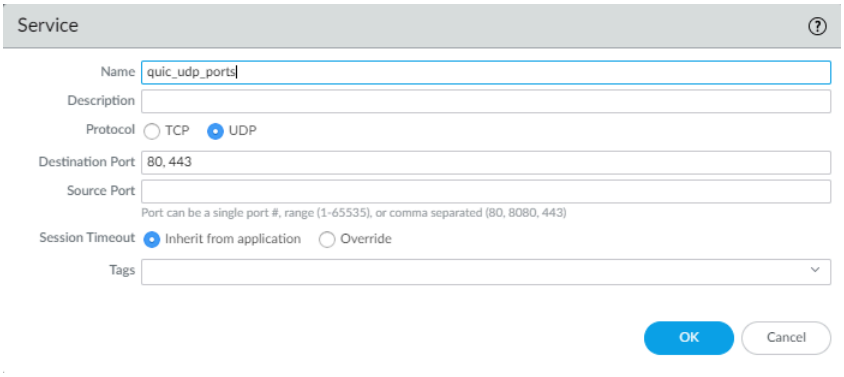
Les règles de blocage des applications vous protègent des applications évasives et couramment exploitées pendant que vous développez et affinez votre règle de politique de sécurité. Des règles de mise au point temporaires permettent de déceler les lacunes de la politique et d'identifier les attaques possibles. Étant donné qu'elles saisissent le trafic d'applications dont vous ignoriez l'existence sur votre réseau, elles autorisent un trafic qui pourrait présenter des risques pour la sécurité. Les règles de blocage suivantes

bloquent explicitement les applications et protocoles potentiellement malveillants que les pirates utilisent couramment, tels que les applications DNS et SMTP publiques, les tunnels cryptés, l'accès à distance et les applications de partage de fichiers non approuvées.

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

Pourquoi ai-je besoin de cette règle ?	Points clés de la règle
❑ Chrome et certains autres navigateurs établissent des sessions en utilisant QUIC au lieu de TLS. QUIC utilise un cryptage propriétaire que le pare-feu ne peut pas décrypter, de sorte qu'un trafic crypté potentiellement dangereux peut pénétrer dans le réseau. ❑ 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 un service (**Objects [Objets]** > **Services**) qui spécifie les ports UDP 80 et 443. • La première règle bloque QUIC sur ses ports de service UDP (80 et 443) et utilise le service que vous avez créé pour spécifier ces ports. • La deuxième règle bloque l'application QUIC.

Le service spécifie les ports UDP à bloquer pour QUIC.



La première règle spécifie le service que vous avez configuré pour QUIC et la seconde règle bloque l'application 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 les applications qui n'ont pas d'utilisation légitime.

Pourquoi ai-je besoin de cette règle ?	Points clés de la règle
❑ Bloquez les applications potentiellement malveillantes telles que les tunnels cryptés, les applications de partage de fichiers peer-to-peer et les applications de partage de fichiers sur le	• Utilisez l'action **Drop (Abandonner)** pour abandonner silencieusement le trafic sans envoyer de signal au client ou au serveur. • Activez la journalisation du trafic correspondant à cette règle pour pouvoir

Pourquoi ai-je besoin de cette règle ?	Points clés de la règle
web qui n'ont pas été approuvées par le service informatique. ❑ Étant donné que les règles de mise au point temporaires peuvent autoriser un trafic malveillant ainsi qu'un trafic légitime qui ne correspond pas aux règles de votre politique, elles peuvent autoriser un trafic risqué ou malveillant. Cette règle bloque le trafic qui n'a aucune légitimité et qu'un pirate ou un utilisateur négligent pourrait utiliser.	enquêter sur la mauvaise utilisation des applications et sur les menaces éventuelles qui existent sur votre réseau. • Étant donné que cette règle a pour but de capter le trafic malveillant, elle est mise en correspondance avec le trafic provenant de tout utilisateur s'exécutant sur n'importe quel port.

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Block Bad Apps	Best Practice	universal	Users	any	any	any	Internet	any	any	encrypted tunnels file sharing remote access	any	Drop	none	

STEP 3 | Bloquez les applications SMTP et DNS publiques.

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

Pourquoi ai-je besoin de cette règle ?	Points clés de la règle
❑ Bloquez les applications DNS/SMTP publiques pour éviter la tunnelisation DNS, le trafic de contrôle et de commande et les applications d'administration à distance.	• Utilisez l'action **Reset both client and server (Réinitialiser le client et le serveur)** pour envoyer un message de réinitialisation TCP aux périphériques côté client et côté serveur. • Activez la journalisation du trafic correspondant à cette règle afin que vous puissiez enquêter sur les menaces éventuelles.

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Block Public DNS and SMTP	Best Practice	universal	Users	any	any	any	Internet	any	any	dns smtp	any	Reset Both	none	

Étape 4 : Création des règles de mise au point temporaires

Les règles de mise au point temporaires vous aident à surveiller la base de règles exemplaire initiale à la recherche de lacunes et avertissent de tout comportement alarmant.

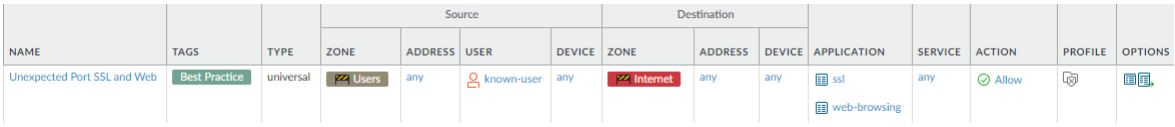
Par exemple, les règles temporaires identifient le trafic provenant d'utilisateurs inconnus ou d'applications exécutées sur des ports inattendus. Surveillez le trafic qui correspond aux règles temporaires afin d'obtenir une compréhension complète de toutes les applications utilisées sur votre réseau (et d'assurer la disponibilité des applications pendant la transition vers une base de règles de meilleures pratiques). Utilisez

ces informations pour affiner votre liste de confiance, soit en y ajoutant de nouvelles règles d'autorisation pour des applications dont vous ignoriez l'existence, soit en restreignant vos règles d'autorisation et en remplaçant les filtres d'applications par des groupes d'applications ou des applications spécifiques. Lorsque le trafic ne correspond plus à ces règles, vous pouvez supprimer les règles temporaires.

Pour s'assurer que le trafic ciblé atteint la règle pertinente, tout en évitant que le mauvais trafic soit autorisé sur votre réseau, certaines règles de mise au point temporaires doivent précéder les règles qui bloquent les mauvaises applications, et certaines doivent les suivre.

STEP 1 | Autorisez la navigation Web et SSL sur des ports non standard pour les utilisateurs connus afin de déterminer si des applications légitimes s'exécutent sur des ports non standard.

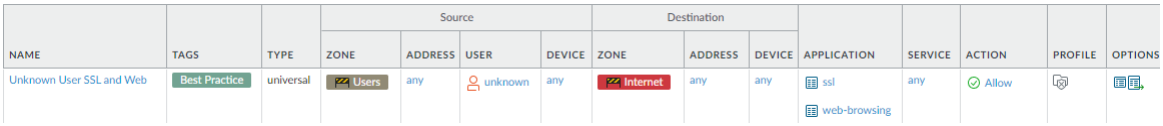
Pourquoi ai-je besoin de cette règle ?	Points clés de la règle
❑ Cette règle vous aide à déterminer si votre politique comporte des lacunes qui font en sorte que des utilisateurs n'arrivent pas à accéder à des applications légitimes parce qu'elles s'exécutent sur des ports non standard. ❑ Surveillez tout le trafic qui correspond à cette règle. Pour le trafic légitime, ajoutez les applications appropriées aux règles d'autorisation appropriées. Créez une application propre à l'entreprise le cas échéant.	• Contrairement aux règles d'autoriser des applications de confiance qui autorisent les applications sur le port par défaut, cette règle autorise la navigation web et le trafic SSL sur n'importe quel port, afin que vous puissiez déceler les lacunes de votre liste de confiance. • Étant donné que cette règle vise à déceler les lacunes des politiques, limitez-la aux utilisateurs connus de votre réseau. • Autorisez explicitement SSL en tant qu'application si vous voulez que les utilisateurs soient en mesure de consulter les sites HTTPS qui ne sont pas déchiffrés (comme des sites web relatifs aux services financiers ou à la santé). • Associez des profils de sécurité basés sur les meilleures pratiques pour rechercher les menaces. • Ajoutez cette règle au-dessus des règles de blocage des applications ; autrement, aucun trafic n'atteindra cette règle.



STEP 2 | Autorisez la navigation Web et le trafic SSL sur les ports non standard de la part d'utilisateurs connus pour mettre en évidence tous les utilisateurs inconnus, peu importe le port.

Pourquoi ai-je besoin de cette règle ?	Points clés de la règle
❑ Cette règle vous aide à déterminer si votre protection User-ID comporte des lacunes.	• Bien que la majorité des règles relatives aux applications de confiance s'appliquent

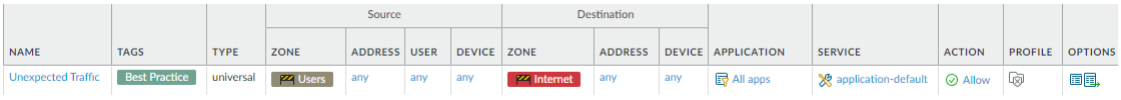
Pourquoi ai-je besoin de cette règle ?	Points clés de la règle
❑ Cette règle vous aide à identifier les périphériques infectés ou intégrés qui tentent d'accéder à l'Internet. ❑ Il importe de bloquer l'utilisation des ports non standard, même pour le trafic de navigation web, puisqu'il s'agit d'une technique d'évasion.	aux utilisateurs connus ou à des groupes d'utilisateurs donnés, cette règle permet de mettre explicitement en correspondance le trafic provenant des utilisateurs **inconnus**. • Cette règle doit être placée devant les règles de blocage des applications ; autrement, le trafic ne l'atteindra jamais. • Associez des profils de sécurité basés sur les meilleures pratiques pour rechercher les menaces.



			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unknown User SSL and Web	Best Practice	universal	Users	any	unknown	any	Internet	any	any	ssl web-browsing	any	Allow		

STEP 3 | Autorisez toutes les applications qui sont sur le port par défaut de l'application à identifier les applications inattendues.

Pourquoi ai-je besoin de cette règle ?	Points clés de la règle
❑ Cette règle vous procure une visibilité quant aux applications dont vous ignoriez la présence sur votre réseau, afin de vous permettre d'affiner votre liste d'applications de confiance. ❑ Surveillez tout le trafic correspondant à cette règle pour déterminer s'il pourrait présenter une menace ou si vous devez modifier vos règles d'autorisation pour autoriser l'accès à plus d'applications.	• Étant donné que cette règle permet toutes les applications, vous devez l'ajouter à la suite des règles de blocage d'applications afin d'éviter que de mauvaises applications s'exécutent sur votre réseau. • Si vous utilisez PAN-OS 7.0.x ou une version antérieure, pour bien identifier les applications inattendues, créez un filtre d'application qui comprend toutes les applications, plutôt que de définir la règle sur **any (indifférent)** pour autoriser n'importe quelle application.

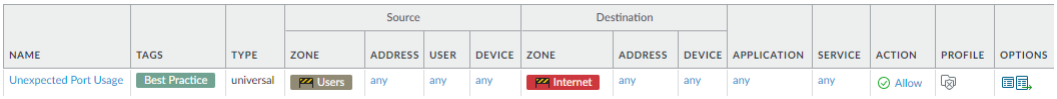


			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected Traffic	Best Practice	universal	Users	any	any	any	Internet	any	any	All apps	application-default	Allow		

STEP 4 | Autorisez n'importe quelle application, peu importe le port, pour identifier les applications qui s'exécutent sur des ports non standard.

Pourquoi ai-je besoin de cette règle ?	Points clés de la règle
❑ Cette règle permet d'identifier les applications légitimes et connues s'exécutant sur des ports inconnus.	• Étant donné qu'il s'agit d'une règle très générale qui autorise toute application de tout utilisateur sur n'importe quel port, placez-la à la toute fin de la base de règles.

Pourquoi ai-je besoin de cette règle ?	Points clés de la règle
❑ Cette règle permet d'identifier les applications inconnues pour lesquelles vous devez créer une application propre à l'entreprise à ajouter à votre règle d'autorisation des applications. ❑ Le trafic qui correspond à cette règle est exploitable. Recherchez la source du trafic et assurez-vous que vous n'autorisez pas le trafic unknown tcp, udp ou non-syn-tcp.	• Activez la journalisation du trafic correspondant à cette règle afin de pouvoir enquêter sur la mauvaise utilisation des applications et sur les menaces éventuelles ou d'identifier des applications légitimes qui nécessitent la création d'une application personnalisée.



Étape 5 : Activer la journalisation du trafic qui ne correspond à aucune règle

Le trafic de la passerelle Internet qui ne correspond pas aux règles que vous avez définies est mis en correspondance avec la règle d'interzone par défaut prédéfinie au bas de la base de règles et est bloqué. Pour une visibilité du trafic qui ne correspond pas aux règles que vous avez créées, activez la journalisation de la règle d'interzone par défaut :

STEP 1 | Sélectionnez la ligne de la règle d'interzone par défaut dans la base de règles, puis sélectionnez **Override (Remplacer)** pour modifier 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 | À 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 correspond à cette règle :

1. Sélectionnez **Monitor (Surveiller)** > **Manage Custom Reports (Gérer les rapports personnalisés)**.
2. **Add (Ajoutez)** un rapport et donnez-lui un **Name (Nom)** descriptif.
3. Définissez la **Database (Base de données)** sur **Traffic Summary (Récapitulatifs du trafic)**.
4. Sélectionner la **Scheduled (Planifié)** case à cocher.
5. Ajoutez **Rule (Règle)**, **Application**, **Bytes (Octets)** et **Sessions** à la liste des colonnes sélectionnées.
6. Définissez les champs **Time Frame (Délai d'exécution)**, **Sort By (Trier par)** et **Group By (Regrouper par)** selon vos besoins.
7. Définissez la requête pour faire correspondre le trafic la règle d'interzone par défaut :

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

STEP 5 | **Commit (Validez)** les modifications que vous avez apportées à la base de règles.

Surveillance et peaufinage des règles de base de la politique

Créer une politique de sécurité exemplaire est un processus itératif. Après avoir défini la politique initiale de sécurité de la passerelle Internet, surveillez le trafic correspondant aux règles temporaires qui identifient les lacunes de la politique et les comportements alarmants, et adaptez votre politique en conséquence. La surveillance du trafic correspondant à ces règles vous permet d'apporter les ajustements nécessaires aux règles permanentes et de vous assurer que tout le trafic correspond à vos règles d'autorisation des applications ou d'évaluer si vous devez autoriser les applications qui ne correspondent à aucune règle.

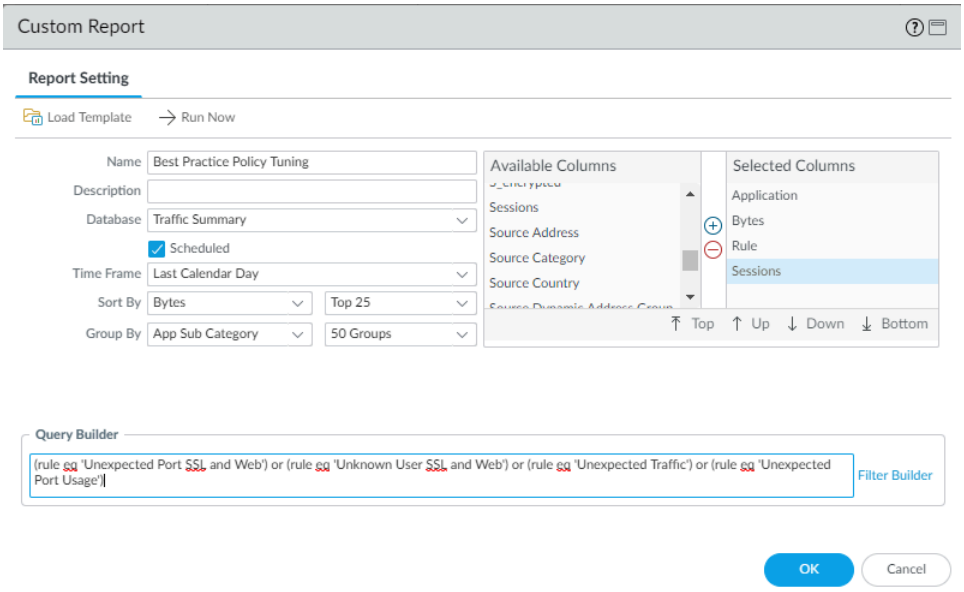
Au fur et à mesure de l'ajustement de votre base de règles, de moins en moins de trafic que vous souhaitez autoriser devrait apparaître en fonction des règles temporaires. Lorsque le trafic que vous souhaitez autoriser ne correspond plus à ces règles, vos règles d'autorisation à application positive sont terminées et vous pouvez supprimer les règles temporaires (la règle de refus d'interzone par défaut refuse automatiquement le trafic qu'aucune règle n'autorise explicitement).

Étant donné que les versions mensuelles du contenu ajoutent de nouveaux App-ID, examinez l'impact des changements d'App-ID sur votre politique de sécurité.

STEP 1 | Créez des rapports personnalisés pour surveiller le trafic correspondant aux règles qui identifient les lacunes de la politique.

1. Sélectionnez **Monitor (Surveiller)** > **Manage Custom Reports (Gérer les rapports personnalisés)**.
2. Sélectionnez **Add (Ajouter)** pour ajouter un rapport et, dans le champ **Name (Nom)**, donnez-lui un nom descriptif qui indique la lacune de la politique que vous étudiez.
3. Définissez la **Database (Base de données)** sur **Traffic Summary (Récapitulatifs du trafic)**.
4. Sélectionnez **Scheduled (Planifié)**.
5. Ajoutez **Rule (Règle)**, **Application**, **Bytes (Octets)** et **Sessions** à la liste des colonnes sélectionnées.
6. Définissez les champs **Time Frame (Délai d'exécution)**, **Sort By (Trier par)** et **Group By (Regrouper par)** selon vos besoins.
7. Définissez la requête pour faire correspondre le trafic aux règles qui détectent les lacunes de la politique et les comportements alarmants. 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. Les exemples de requêtes suivants utilisent les noms de règles définis dans l'exemple de politique :
   - `(rule eq 'Unexpected Port SSL and Web')`
   - `(rule eq 'Unknown User SSL and Web')`
   - `(rule eq 'Unexpected Traffic')`

- `(rule eq 'Unexpected Port Usage')`



STEP 2 | Consultez régulièrement le rapport pour comprendre pourquoi le trafic correspond à chacune des règles de mise au point. Mettez à jour les règles pour inclure les applications et les utilisateurs légitimes ou utilisez les informations contenues dans le rapport pour évaluer le risque de l'application et mettre en œuvre des réformes politiques.

Suppression des règles temporaires

Après plusieurs mois de surveillance de votre politique de sécurité exemplaire en matière de passerelle Internet et d'ajustement de la base de règles, vous devriez constater que le trafic que vous souhaitez autoriser est moins important et correspond aux règles temporaires. Lorsque le trafic que vous souhaitez autoriser ne correspond plus à ces règles, vous avez réalisé votre objectif qui consistait à passer à une base de règles de politique de sécurité complètement basée sur des applications. Vous pouvez maintenant supprimer les règles temporaires, y compris les règles de blocage des applications qui n'ont pas de cas d'utilisation légitime et des applications DNS et SMTP publiques, car la règle de refus d'interzone par défaut bloque automatiquement ce trafic puisqu'il ne correspond à aucune règle d'autorisation explicite. (Conservez les règles du protocole QUIC.)

STEP 1 | Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.

STEP 2 | Sélectionnez la règle et cliquez sur **Delete (Supprimer)**.

Vous pouvez également **Disable (Désactiver)** les règles pendant un certain temps avant de les supprimer. Vous pourrez sélectionner **Enable (Activer)** plus tard pour les réactiver si les journaux du trafic montrent que le trafic que vous souhaitez autoriser correspond à la règle de refus d'interzone par défaut.

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

Maintien de la base de règles

Les entreprises et les applications évoluent, de sorte que la base de règles de votre politique de sécurité doit également évoluer. Lorsque vos applications approuvées changent, modifiez les règles existantes en fonction des cas d'utilisation de l'application, dans la mesure du possible, au lieu d'ajouter de nouvelles règles. Souvent, la modification est aussi simple que l'ajout d'une nouvelle application à un groupe d'applications ou la suppression d'une application obsolète d'un groupe d'applications.

Sur Panorama ou sur un pare-feu autonome, utilisez le nombre 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. Poursuivez en vérifiant les widgets* ***ACC*** *>* ***Threat Activity*** *>* ***Applications Using Non Standard Ports*** *et les widgets* ***ACC*** *>* ***Threat Activity*** *>* ***Rules Allowing Apps On Non Standard Ports*** *pour voir si le trafic sur les ports non standard a causé le nombre de correspondances inattendu.*

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.

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 entre eux, pour identifier les écarts par rapport à leur comportement normal.*

Configurez le téléchargement automatique des mises à jour du contenu de Palo Alto Networks et planifiez l'installation sur les pare-feu dès que possible. Les mises à jour du contenu de menace et des applications ont lieu chaque fois que les signatures des profils de sécurité doivent être mises à jour. Les mises à jour de contenu envoyées le troisième mardi de chaque mois contiennent également des App-ID nouveaux et modifiés (mises à jour d'applications ; dans de rares cas, une mise à jour d'application peut être retardée d'un ou deux jours). Évaluez l'impact des nouveaux App-ID et des App-ID modifiés sur votre base de règles de sécurité dans un environnement de non-production et modifiez les règles si nécessaire.

Suivez les meilleures pratiques en matière de mise à jour de contenu, installez les mises à jour dès que possible pour protéger votre passerelle Internet et configurez la fonction Transfert des journaux pour toutes les mises à jour du contenu.

STEP 1 | Avant d'installer une nouvelle mise à jour de contenu, revoyez les nouvelles App-ID 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-ID sélectionnées si certaines App-ID exigent plus de tests, et installer le reste des nouvelles App-ID et les App-ID modifiées. Terminez les essais et les révisions de politique nécessaires avant que la prochaine version de contenu mensuelle contenant les nouveaux App-ID n'arrive (troisième mardi de chaque mois) pour éviter les chevauchements.

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 ou supprimer de nouvelles applications approuvées à vos règles d'autorisation des applications.