paloalto
TECHDOCS

Administration d'Advanced Threat Prevention

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

May 18, 2023

Table of Contents

Prévention avancée des menaces

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

Les abonnements de prévention des intrusions par pare-feu de nouvelle génération de Palo Alto Networks® protègent et défendent votre réseau contre les menaces de base et les menaces persistantes avancées (APT) à l'aide de mécanismes de détection à plusieurs volets pour lutter contre toute la gamme du paysage des menaces. La solution de prévention des menaces de Palo Alto Networks se compose des abonnements suivants :

- **Advanced Threat Prevention** : le service cloud Advanced Threat Prevention utilise des modèles de deep learning et d'apprentissage automatique en ligne pour la détection en temps réel de menaces C2 évasives et jamais vues auparavant et d'exploits de vulnérabilités de type zero day. En tant que service cloud natif à très faible latence, cette solution extensible et évolutive à l'infini est toujours tenue à jour avec des améliorations de formation de modèle. Il prend également en charge le Deep Learning local, qui complète le composant Analyse cloud en ligne d'Advanced Threat Prevention en fournissant un mécanisme permettant d'effectuer une analyse rapide fondée sur le deep learning local des menaces de type zero day et d'autres menaces évasives. La licence Advanced Threat Prevention inclut tous les avantages inclus dans Threat Prevention.
- **Threat Prevention** : l'abonnement Prévention des menaces principal est basé sur des signatures générées à partir de données de trafic malveillantes collectées à partir de divers services Palo Alto Networks. Ces signatures sont utilisées par le pare-feu pour appliquer des stratégies de sécurité basées sur des menaces spécifiques, notamment : la commande et le contrôle (C2), divers types de logiciels malveillants connus et les exploits de vulnérabilité ; et combiné avec les technologies d'identification App-ID et User-ID sur le pare-feu, vous pouvez croiser les données contextuelles pour produire des stratégies affinées. Dans le cadre de vos stratégies d'atténuation des menaces, vous pouvez également identifier et bloquer les types de fichiers et les adresses IP connus ou à risque, dont plusieurs catégories prédéfinies sont disponibles, y compris des listes spécifiant des fournisseurs de services à toute épreuve et des adresses IP malveillantes connues. Dans les cas où des outils et des logiciels spécialisés sont utilisés, vous pouvez créer vos propres signatures de vulnérabilité pour personnaliser vos capacités de prévention des intrusions en fonction des besoins uniques de votre réseau.

Pour maximiser la prévention des menaces, Palo Alto Network vous recommande également les services d'abonnement suivants en plus de Advanced | Threat Prevention :

- **Sécurité DNS** : le service cloud de la Sécurité DNS est conçu pour protéger votre organisation contre les menaces DNS avancées. En appliquant l'apprentissage automatique avancé et l'analyse prédictive à un large éventail de sources de renseignements sur les menaces, DNS Security génère un ensemble de signatures DNS amélioré et fournit une analyse en temps réel des requêtes DNS pour défendre votre réseau contre les domaines malveillants nouvellement générés. DNS Security peut détecter diverses menaces C2, notamment le tunneling DNS, les attaques de reliaison DNS, les domaines créés à l'aide de la génération automatique, les hôtes de logiciels malveillants et bien d'autres. DNS Security requiert et fonctionne avec votre abonnement Advanced Threat Prevention ou Threat Prevention pour une couverture complète des menaces DNS.

Les abonnements de prévention des intrusions Palo Alto Networks fonctionnent ensemble pour fournir une solution complète qui intercepte et brise la chaîne à différentes étapes du processus d'attaque et fournit une visibilité pour prévenir les atteintes à la sécurité de votre infrastructure réseau.

Services de détection Advanced Threat Prevention

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

Advanced Threat Prevention est une solution de système de prévention des intrusions (IPS) capable de détecter et de bloquer les logiciels malveillants, les exploitations de vulnérabilité et la commande et le contrôle (C2) sur tous les ports et protocoles, à l'aide d'un système de prévention multicouche avec des composants fonctionnant sur le pare-feu et dans le cloud. Le cloud de Prévention des menaces exploite une multitude de services de détection utilisant les données de menace combinées des services Palo Alto Networks pour créer des signatures, chacun possédant des modèles identifiables spécifiques, et sont utilisés par le pare-feu pour appliquer des stratégies de sécurité lorsque des menaces et des comportements malveillants correspondants sont détectés. Ces signatures sont classées en fonction du type de menace et se voient attribuer des numéros d'identification uniques. Pour détecter les menaces qui correspondent à ces signatures, le pare-feu exploite des moteurs d'analyse qui inspectent et classent le trafic réseau présentant des caractéristiques anormales.

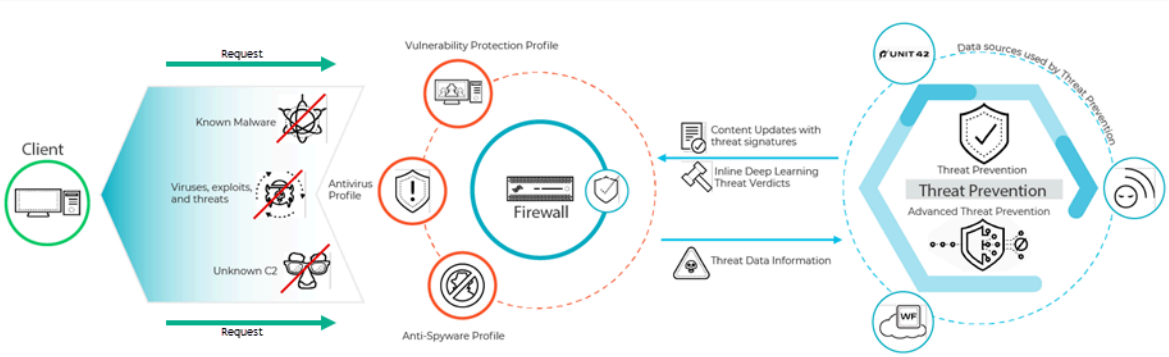
En plus du mécanisme de détection basé sur les signatures, la prévention avancée des menaces fournit un système de détection en ligne afin de prévenir les menaces C2 inconnues et évasives, y compris celles produites via le framework Empire, ainsi que les vulnérabilités d'injection de commandes et d'injection SQL. Le cloud Advanced Threat Prevention exploite des modèles de deep learning extensibles qui activent les capacités d'analyse en ligne sur le pare-feu, sur une base par requête, pour empêcher les menaces de type « zero-day » de pénétrer dans le réseau et pour distribuer des protections. Cela vous permet de prévenir les menaces inconnues à l'aide d'une inspection du trafic en temps réel avec des détecteurs en ligne. Les moteurs de détection basés sur le ML et le deep learning dans le cloud Advanced Threat Prevention analysent le trafic à la recherche de C2 inconnus et de vulnérabilités qui utilisent l'injection SQL et l'injection de commandes pour protéger contre les menaces de type « zero-day ». Pour fournir un contexte de menace et des détails de détection complets, des rapports sont générés et peuvent inclure les outils et techniques utilisés par l'attaquant, la portée et l'impact de la détection, ainsi que la classification de cyberattaque correspondante, telle que définie par le framework MITRE ATT&CK®.

MITRE ATT&CK® est une base de connaissances organisée et un modèle de comportement des cyberadversaires. Cette œuvre est reproduite et distribuée avec l'autorisation de The MITRE Corporation. The MITRE Corporation (MITRE) vous accorde par la présente une licence non exclusive et libre de droits pour utiliser ATT&CK® à des fins de recherche, de développement et commerciales. Toute copie que vous faites à ces fins est autorisée à condition que vous reproduisiez la désignation de droit d'auteur de MITRE et la présente licence dans la copie concernée.

En utilisant des moteurs de détection basés sur le cloud, vous pouvez accéder à un large éventail de mécanismes de détection qui sont mis à jour et déployés automatiquement sans que l'utilisateur n'ait à télécharger des packages de contenu ou à utiliser des analyseurs basés sur un pare-feu à processus intensif susceptibles de consommer des ressources. La logique du moteur de détection basée sur le cloud est surveillée et mise à jour en permanence à l'aide des ensembles de données de trafic C2 de WildFire, avec le soutien supplémentaire des chercheurs sur les menaces de Palo Alto Networks, qui fournissent une intervention humaine pour des améliorations de détection hautement précises. Les moteurs de deep learning d'Advanced Threat Prevention prennent en charge l'analyse des menaces basées sur C2 sur les applications HTTP, HTTP2, SSL, UDP inconnues et TCP inconnues. Des modèles d'analyse supplémentaires sont fournis via des mises à jour de contenu, cependant, les améliorations des modèles existants sont effectuées sous forme de mise à jour côté cloud, ne nécessitant aucune mise à jour du pare-feu.

Advanced Threat Prevention prend également en charge le Deep Learning local, qui fournit un mécanisme permettant d'effectuer une analyse rapide et locale basée sur le deep learning des menaces de type « zero-day » et d'autres menaces évasives. Il s'agit d'une fonctionnalité complémentaire du composant d'analyse cloud en ligne d'Advanced Threat Prevention. Le trafic malveillant connu correspondant à l'ensemble de signatures publié par Palo Alto Networks est supprimé (ou une autre action définie par l'utilisateur lui est appliquée). Toutefois, certains trafics qui correspondent aux critères de contenu suspect sont redirigés pour être analysés à l'aide du module de détection Deep Learning Analysis. Si une analyse plus approfondie est nécessaire, le trafic est envoyé au cloud Advanced Threat Prevention pour une analyse supplémentaire, ainsi que pour les vérifications requises des faux positifs et des faux négatifs. Le module de détection de Deep Learning est basé sur les modules de détection éprouvés fonctionnant dans le cloud Advanced Threat Prevention et, en tant que tel, dispose des mêmes capacités de détection avancées des menaces et « zero-day ». Cependant, il présente également l'avantage supplémentaire de traiter un volume de trafic beaucoup plus élevé, sans le décalage associé aux requêtes cloud. Cela vous permet d'inspecter davantage de trafic et de recevoir des verdicts dans un délai plus court. Cela est particulièrement utile lorsque vous êtes confronté à des conditions de réseau difficiles.

Palo Alto Networks propose également l'abonnement Prévention des menaces qui n'inclut pas les fonctionnalités de la licence Advanced Threat Prevention basée sur le cloud.



Les signatures de menace utilisées par le pare-feu sont généralement classées en trois types : antivirus, antispyware, vulnérabilité et sont utilisées par les profils de sécurité correspondants pour appliquer des politiques définies par l'utilisateur.

Les services de sécurité fournis par Palo Alto Networks dans le cloud génèrent également des signatures WildFire et DNS C2 pour leurs services respectifs, ainsi que des signatures au format de fichier, qui peuvent désigner des types de fichiers au lieu de signatures de menace; par exemple, en tant qu'exceptions de signature.

- Les signatures antivirus détectent divers types de logiciels malveillants et de virus, notamment les vers, les chevaux de Troie et les téléchargements de logiciels espions.
- Les signatures antispyware détectent les logiciels espions C2 sur les hôtes compromis lorsqu'ils tentent de téléphoner à la maison ou de se diriger vers un serveur C2 externe.
- Les signatures de vulnérabilité détectent les vulnérabilités du système d'exploitation.

Les signatures ont un niveau de gravité par défaut avec une action par défaut associée ; par exemple, dans le cas d'une menace hautement malveillante, l'action par défaut est Réinitialiser les deux. Ce paramètre est basé sur les recommandations de sécurité de Palo Alto Networks.

Dans les déploiements où des applications internes spécialisées sont présentes ou dans les cas où des flux de renseignements tiers utilisent des règles Snort et Suricata open source, des signatures personnalisées peuvent être créées pour une protection spécialement conçue.

Les pare-feu reçoivent des mises à jour de signature sous la forme de deux packages de mise à jour : le contenu antivirus quotidien et les mises à jour hebdomadaires du contenu des applications et des menaces. Les mises à jour du contenu antivirus incluent respectivement des signatures antivirus et des signatures DNS (C2) utilisées par les profils de sécurité antivirus et antispyware. Les mises à jour du contenu pour les applications et les menaces incluent des signatures de vulnérabilité et antispyware, utilisées respectivement par les profils de sécurité de vulnérabilité et antispyware. Les packages de mise à jour incluent également du contenu supplémentaire exploité par d'autres services et sous-fonctions. Pour plus d'informations, reportez-vous à la sectionMises à jour de contenu dynamique.

Catégories de signatures de menace

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

Il existe trois types de signatures de menaces Palo Alto Networks, chacune conçue pour détecter différents types de menaces lors de l'analyse du trafic réseau :

- Signatures antivirus: détectez les virus et les logiciels malveillants détectés dans les exécutables et les types de fichiers.
- Signatures anti-spyware : détecte les activités de commande-et-contrôle (C2), dans le cadre desquelles un logiciel espion installé sur un client infecté collecte des données sans le consentement de l'utilisateur et/ou entre en communication avec un pirate à distance.
- Signatures de vulnérabilité : détecte les failles du système qu'un pirate pourrait autrement tenter d'exploiter.

La gravité d'une signature indique le risque de l'événement détecté, et l'action par défaut d'une signature (par exemple, bloquer ou transmettre une alerte) correspond à la façon dont Palo Alto Networks vous recommande d'appliquer le trafic correspondant.

Vous devez Paramétrage des profils Antivirus, Antispyware et Protection contre les vulnérabilités pour définir l'action à entreprendre lors de la détection d'une menace, et vous pouvez facilement utiliser les profils de sécurité par défaut pour commencer à bloquer les menaces en fonction des recommandations de Palo Alto Networks. Pour chaque type de signature, de catégorie et même de signature spécifique, vous pouvez continuer à modifier ou à créer de nouveaux profils pour appliquer plus efficacement les menaces éventuelles.

Le tableau suivant répertorie toutes les catégories de signatures possibles par type (antivirus, logiciels espions et vulnérabilités) et inclut la mise à jour du contenu (applications et menaces, antivirus ou WildFire) fournissant les signatures de chaque catégorie. Vous pouvez aussi aller sur les réseaux Palo Alto Coffre de Menaces à En savoir plus sur les signatures de menaces.

Catégorie de menaces	Mises à jour de contenu fournissant ces signatures	Description
Signatures antivirus		

Catégorie de menaces	Mises à jour de contenu fournissant ces signatures	Description
apk	Antivirus WildFire	Fichiers malveillants d'application Android (APK).
MacOSX	Antivirus WildFire	Fichiers MacOSX malveillants, notamment : • Fichiers d'image disque Apple (DMG). • Les fichiers objet Mach (Mach-O) sont des exécutables, des bibliothèques et du code objet. • Packages d'installation de logiciels Apple (PKG)
flash	Antivirus WildFire ou WildFire privé	Applets Adobe Flash et contenu Flash intégré à des pages Web.
jar	Antivirus WildFire	Applets Java (types de fichiers JAR/Class).
ms-office	Antivirus WildFire ou WildFire privé	Fichiers Microsoft Office, y compris les documents (DOC, DOCX, RTF), les cahiers de travail (XLS, XLSX) et les présentations PowerPoint (PPT, PPTX). Cela inclut également les documents Office Open XML (OOXML) 2007+.
pdf	Antivirus WildFire ou WildFire privé	Fichiers Portable Document Format (PDF).
pe	Antivirus WildFire ou WildFire privé	Les fichiers exécutables portatifs (PE) peuvent s'exécuter automatiquement sur un système Windows de Microsoft et ne devraient être autorisés que lorsqu'ils sont autorisés. Ces types de fichiers comprennent ce qui suit : • Code d'objet. • Polices (FON). • Fichiers système (SYS). • Fichiers lecteur (DRV). • Éléments du panneau de configuration Windows (CPL). • DLL (bibliothèque à liaisons dynamiques)

Catégorie de menaces	Mises à jour de contenu fournissant ces signatures	Description
		• OCX (bibliothèques des contrôles personnalisés OLE ou des contrôles ActiveX). • Fichiers d'économiseur d'écran Windows (SCR). • Fichiers EFI (Extensible Firmware Interface), qui s'exécutent entre un système d'exploitation et un microprogramme afin de faciliter les mises à jour de périphériques et les opérations de démarrage. • Fichiers d'informations sur le programme (PIF).
Linux	Antivirus WildFire	Fichiers Executable and Linkable Format (format exécutable et liable ; ELF).
archive	Antivirus WildFire	Fichiers d'archive Roshal Archive (RAR) et 7-Zip (7z).
Signature de logiciels espions		
adware	Applications et menaces	Détecte les programmes qui affichent des publicités potentiellement indésirables. Certains logiciels publicitaires modifient les navigateurs pour mettre en évidence et créer des liens hypertextes à partir des mots-clés les plus recherchés sur les pages Web. Ces liens redirigent les utilisateurs vers des sites Web publicitaires. Les logiciels publicitaires peuvent également récupérer des mises à jour à partir d'un serveur C2 (commande-et-contrôle) et les installer dans un navigateur ou sur un système client. Les protections nouvellement lancées dans cette catégorie sont rares.
autogen	Antivirus	Ces signatures basées sur la charge détectent le trafic de commande et de contrôle (C2) et sont générées automatiquement. Il est important de souligner que les signatures de l'autogène peuvent détecter le trafic C2 même lorsque l'hôte C2 est inconnu ou change rapidement.
backdoor	Applications et menaces	Détecte un programme qui permet à un pirate d'obtenir un accès distant non autorisé à un système.

Catégorie de menaces	Mises à jour de contenu fournissant ces signatures	Description
Réseau de robots (Botnet)	Applications et menaces	Indique une activité de botnet. Un botnet est un réseau d'ordinateurs infectés par des logiciels malveillants (« bots ») qui sont contrôlés par un pirate. Le pirate peut ordonner, de manière centralisée, à chaque ordinateur d'un réseau de botnets d'effectuer simultanément une action coordonnée (par exemple, le lancement d'une attaque par déni de service).
browser-hijack	Applications et menaces	Détecte la présence d'un plugin ou d'un logiciel qui modifie les paramètres du navigateur. Un pirate de navigateur peut prendre en charge la recherche automatique ou suivre l'activité Web des utilisateurs et envoyer cette information à un serveur C2. Les protections nouvellement lancées dans cette catégorie sont rares.
cryptominer	Applications et menaces	(Parfois connu sous le nom de cryptojacking ou de mineurs) Détecte la tentative de téléchargement ou le trafic réseau généré par des programmes malveillants conçus pour utiliser des ressources informatiques afin de miner des cryptomonnaies à l'insu de l'utilisateur. Les binaires Cryptominer sont souvent livrés par un téléchargeur de script shell qui tente de déterminer l'architecture du système et de tuer d'autres processus de mineurs sur le système. Certains mineurs s'exécutent dans le cadre d'autres processus, tels qu'un navigateur web rendant une page web malveillante.
data-theft	Applications et menaces	Détecte un système qui envoie des informations à un serveur C2 connu. Les protections nouvellement lancées dans cette catégorie sont rares.
dns	Antivirus	Détecte les requêtes DNS visant la connexion à des domaines malveillants. Les signatures DNS et DNS-Wildfire détectent les mêmes domaines malveillants. Cependant, les signatures DNS sont incluses dans la mise à jour quotidienne du contenu antivirus et les signatures dns-wildfire sont incluses dans les mises à jour WildFire qui fournissent des protections toutes les 5 minutes.

Catégorie de menaces	Mises à jour de contenu fournissant ces signatures	Description
dns-security	Antivirus	Détecte les requêtes DNS visant la connexion à des domaines malveillants. dns-security comprend les signatures dns et dns-wildire, en plus des signatures uniques générées par le service de sécurité DNS.
dns-wildfire	WildFire ou WildFire privé	Détecte les requêtes DNS visant la connexion à des domaines malveillants. Les signatures DNS et DNS-Wildfire détectent les mêmes domaines malveillants. Cependant, les signatures DNS sont incluses dans la mise à jour quotidienne du contenu antivirus et les signatures dns-wildfire sont incluses dans les mises à jour WildFire qui fournissent des protections toutes les 5 minutes.
téléchargeur	Applications et menaces	(Aussi connu sous le nom de droppers, stagers ou loaders) Détecte les programmes qui utilisent une connexion Internet pour se connecter à un serveur distant afin de télécharger et d'exécuter des logiciels malveillants sur le système compromis. Le cas d'utilisation le plus courant est celui d'un téléchargeur déployé comme point culminant de la *première étape* d'une cyber-attaque, où l'exécution de la charge utile récupérée par le téléchargeur est considérée comme la *deuxième étape*. Les scripts shell (Bash, PowerShell, etc.), les chevaux de Troie et les documents de leurre malveillants (également appelés maldocs) tels que les fichiers PDF et Word sont des types de téléchargeurs courants.
fraude	Applications et menaces	(y compris le détournement de formulaires, le hameçonnage et les escroqueries) Détecte l'accès à des sites web compromis dont il a été déterminé qu'ils ont été injectés avec du code JavaScript malveillant pour recueillir des informations sensibles sur les utilisateurs. (par exemple, nom, adresse, e-mail, numéro de carte de crédit, CVV, date d'expiration) à partir des formulaires de paiement qui sont saisis sur les pages de paiement des sites de commerce électronique.
outil de piratage	Applications et menaces	Détecte le trafic généré par des outils logiciels qui sont utilisés par des acteurs malveillants pour effectuer une reconnaissance, attaquer ou accéder

Catégorie de menaces	Mises à jour de contenu fournissant ces signatures	Description
		à des systèmes vulnérables, exfiltrer des données, ou créer un canal de commande et de contrôle pour contrôler subrepticement un système informatique sans autorisation. Ces programmes sont fortement associés aux logiciels malveillants et aux cyber-attaques. Les outils de piratage peuvent être déployés de manière bénigne lorsqu'ils sont utilisés dans les opérations de l'Équipe rouge et bleue, les tests de pénétration et la R&D. L'utilisation ou la possession de ces outils peut être illégale dans certains pays, quelle que soit l'intention.
Keylogger	Applications et menaces	Détecte les programmes qui permettent aux pirates de suivre secrètement l'activité des utilisateurs en enregistrant les touches de clavier et en enregistrant des captures d'écran. Les enregistreurs de frappe utilisent diverses méthodes C2 pour envoyer périodiquement des journaux et des rapports à une adresse électronique prédéfinie ou à un serveur C2. Par la surveillance des enregistreurs de frappe, un pirate pourrait récupérer des informations d'identification qui lui permettraient d'accéder au réseau.
networm	Applications et menaces	Détecte un programme qui se réplique et se propage automatiquement d'un système à l'autre. Les « net-worms » peuvent utiliser des ressources partagées ou exploiter les défaillances de sécurité pour accéder aux systèmes cibles.
Hameçonnage	Applications et menaces	Détecte une situation où un utilisateur tente de se connecter à une page d'hameçonnage (probablement après avoir reçu un email contenant un lien vers le site malveillant). Un site Web d'hameçonnage incite les utilisateurs à soumettre des informations d'identification qu'un pirate peut voler pour accéder au réseau.

Catégorie de menaces	Mises à jour de contenu fournissant ces signatures	Description
		En plus de bloquer l'accès aux pages de destination des kits d'hameçonnage, activez l'authentification multifacteur et empêchez l'hameçonnage des informations d'identification pour empêcher les attaques d'hameçonnage à toutes les étapes.
post-exploitation	Applications et menaces	Détecte des activités qui indiquent la phase post-exploitation d'une attaque, dans le cadre de laquelle un pirate tente d'évaluer la valeur d'un système compromis. Cela peut inclure l'évaluation de la sensibilité des données stockées sur le système et de l'utilité du système pour compromettre davantage le réseau.
webshell	Applications et menaces	Détecte les shells web et le trafic des shells web, y compris la détection des implants et l'interaction de commande et de contrôle. Les shells web doivent d'abord être implantés par un acteur malveillant sur l'hôte compromis, le plus souvent en ciblant un serveur ou un cadre web. La communication ultérieure avec le fichier shell web permet souvent à un acteur malveillant de prendre pied dans le système, d'effectuer le dénombrement des services et du réseau, l'exfiltration des données et l'exécution du code à distance dans le contexte de l'utilisateur du serveur web. Les types de shells web les plus courants sont les scripts PHP, .NET et les scripts de balisage Perl. Les attaquants peuvent également utiliser des serveurs web infectés par un shell (les serveurs web peuvent être à la fois orientés vers Internet ou des systèmes internes) pour cibler d'autres systèmes internes.
spyware	Applications et menaces	Détecte la communication C2 sortante. Ces signatures sont générées automatiquement ou créées manuellement par les chercheurs de Palo Alto Networks.

Catégorie de menaces	Mises à jour de contenu fournissant ces signatures	Description
		Les signatures de spyware et d'autogen détectent toutes les deux la communication C2 sortante ; cependant, les signatures autogènes sont basées sur la charge utile et peuvent détecter de manière unique les communications C2 avec des hôtes C2 inconnues ou qui changent rapidement.
Signatures de vulnérabilités		
brute force	Applications et menaces	Une signature de force brute détecte plusieurs occurrences d'une condition au cours d'une période donnée. Bien que l'activité isolée puisse être bénigne, la signature de force brute indique que la fréquence et le taux auxquels l'activité s'est produite sont suspects. Par exemple, un échec de connexion FTP unique n'indique pas une activité malveillante. Cependant, de nombreux échecs de connexion FTP sur une courte période de temps indiquent la probabilité qu'un pirate tente de combiner des mots de passe pour accéder à un serveur FTP. Vous pouvez régler l'action et les conditions de déclenchement pour les signatures de force brute.
code execution	Applications et menaces	Détecte une vulnérabilité d'exécution de code qu'un pirate peut exploiter pour exécuter du code sur un système disposant des privilèges de l'utilisateur connecté.
Occultation de code	Applications et menaces	Détecte le code qui a été transformé pour dissimuler certaines données tout en conservant sa fonction. Le code occulté est difficile ou impossible à lire, il est donc difficile de savoir quelles commandes le code est en train d'exécuter ou avec quels programmes il est conçu pour interagir. Le plus souvent, des acteurs malveillants dissimulent du code pour dissimuler des logiciels malveillants. Plus rarement, les développeurs légitimes peuvent dissimuler du code pour protéger la confidentialité ou la propriété intellectuelle ou pour améliorer l'expérience utilisateur. Par exemple, certains types de dissimulation (tels que la minification) réduisent la taille du fichier, ce qui diminue les temps de

Catégorie de menaces	Mises à jour de contenu fournissant ces signatures	Description
		chargement sur le site Web et l'utilisation de la bande passante.
dos	Applications et menaces	Détecte une attaque par déni de service, dans le cadre de laquelle un pirate tente de rendre indisponible un système ciblé en interrompant temporairement le système et les applications et services dépendants. Pour effectuer une attaque par déni de service, un pirate peut inonder un système cible de trafic ou envoyer des informations qui entraînent son échec. Les attaques par déni de service privent les utilisateurs légitimes (tels que les employés, les membres et les titulaires de compte) du service ou de la ressource auquel ils souhaitent accéder.
exploit-kit	Applications et menaces	Détecte une page de renvoi d'un kit d'attaques. Les pages de renvoi d'un kit d'attaques contiennent souvent plusieurs exploits qui ciblent une ou plusieurs vulnérabilités et expositions (CVE) communes, pour plusieurs navigateurs et plugins. Étant donné que les CVE ciblés changent rapidement, les signatures des kits d'attaques se déclenchent en fonction de la page de renvoi du kit d'attaques et non des CVE. Lorsqu'un utilisateur visite un site Web avec un kit d'attaques, ce dernier cherche les CVE ciblés et tente de fournir en mode silencieux une charge malveillante à l'ordinateur de la victime.
info-leak	Applications et menaces	Détecte une vulnérabilité logicielle qu'un pirate pourrait exploiter pour dérober des informations sensibles ou propriétaires. Souvent, une fuite d'informations peut se produire, car les contrôles complets n'existent pas pour protéger les données et les pirates peuvent exploiter les fuites d'informations en envoyant des requêtes spécialement construites.
identifiants non sécurisés	Applications et menaces	Détecte l'utilisation de mots de passe faibles, compromis et par défaut du fabricant pour les logiciels, les appareils réseau et les dispositifs IdO.
Dépassement de capacité	Applications et menaces	Détecte une vulnérabilité de débordement dans le cadre de laquelle un pirate pourrait exploiter le manque de contrôles adéquats des requêtes. Une attaque réussie pourrait entraîner l'exécution de code à distance avec

Catégorie de menaces	Mises à jour de contenu fournissant ces signatures	Description
		les privilèges de l'application, du serveur ou du système d'exploitation.
phishing	Applications et menaces	Détecte une situation où un utilisateur tente de se connecter à une page d'hameçonnage (probablement après avoir reçu un email contenant un lien vers le site malveillant). Un site Web d'hameçonnage incite les utilisateurs à soumettre des informations d'identification qu'un pirate peut voler pour accéder au réseau. *En plus de bloquer l'accès aux pages de destination des kits d'hameçonnage, activez l'authentification multifacteur et empêchez l'hameçonnage des informations d'identification pour empêcher les attaques d'hameçonnage à toutes les étapes.*
protocol-anomaly	Applications et menaces	Détecte les anomalies de protocole, lorsque le comportement d'un protocole s'écarte de l'utilisation standard et conforme. Par exemple, un paquet malformé, une application mal conçue ou une application qui s'exécute sur un port non standard sont des exemples d'anomalies de protocole et pourraient servir de techniques d'évasion. Il est recommandé de bloquer les anomalies de protocole, peu importe leur niveau de gravité.
sql-injection	Applications et menaces	Détecte une technique de piratage courante dans le cadre de laquelle un pirate insère des requêtes SQL dans les requêtes d'une application, afin de lire ou de modifier une base de données. Ce type de technique est souvent utilisé sur des sites Web qui ne suppriment pas complètement les données saisies par l'utilisateur.

Meilleures pratiques pour sécuriser votre réseau contre les fuites au niveau des couches 4 et 7

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

Pour surveiller et protéger votre réseau contre la plupart des attaques des couches 4 et 7, voici quelques recommandations à suivre.

- ❑ Mettez à niveau vers la dernière version logicielle et de contenu PAN-OS pour vous assurer de disposer des dernières mises à jour de sécurité. Reportez-vous à la section Installer les mises à jour de contenu et logicielles
- ❑ Activez la sécurité DNS (nécessite une licence d'abonnement Prévention des menaces et Sécurité DNS) pour mettre en entonnoir les requêtes DNS malveillantes. Palo Alto Networks recommande d'utiliser les paramètres de configuration suivants de la catégorie Sécurité DNS dans votre profil antispyware :

SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
: Palo Alto Networks Content			
default-paloalto-dns		sinkhole	extended-capture
: DNS Security			
Command and Control Domains	default (high)	sinkhole	extended-capture
Dynamic DNS Hosted Domains	default (informational)	sinkhole	disable
Grayware Domains	default (low)	sinkhole	disable
Malware Domains	default (medium)	sinkhole	disable
Parked Domains	default (informational)	sinkhole	disable
Phishing Domains	default (low)	sinkhole	disable
Proxy Avoidance and Anonymizers	default (low)	sinkhole	disable
Newly Registered Domains	default (informational)	sinkhole	disable

  - Pour les paramètres de gravité du journal, utilisez les paramètres par défaut :
  - Pour l'action de politique, régler toutes les sources de signature sur **entonnoir**.
  - Pour la capteur de paquet, réglez Command (Commande) et Control Domains (Domaines de contrôle) sur **capture étendue**. Laissez toutes les autres catégories aux réglages par défaut.

  Pour plus d'informations sur les paramètres antispyware connexes, voir Meilleures pratiques du profil antispyware pour la passerelle Internet.
- ❑ Si vous disposez d'un abonnement Advanced Threat Prevention actif, activez l'analyse cloud en ligne et le Deep Learning local, le cas échéant, pour bloquer en temps réel les menaces avancées de C2 et de logiciels espions. L'action par défaut pour chaque moteur d'analyse est **l'alerte**, qui génère un journal des menaces lorsqu'une menace correspondante est détectée ; toutefois, Palo Alto Networks recommande de définir toutes les actions du modèle d'analyse

sur **Réinitialiser les deux**. Cela supprime les paquets correspondants et envoie un RST au client et au serveur, rompant la connexion, ainsi que la génération d'une entrée de journal des menaces.

- Configurez le pare-feu pour qu'il agisse en tant que proxy DNS et activez les signatures d'évasion :

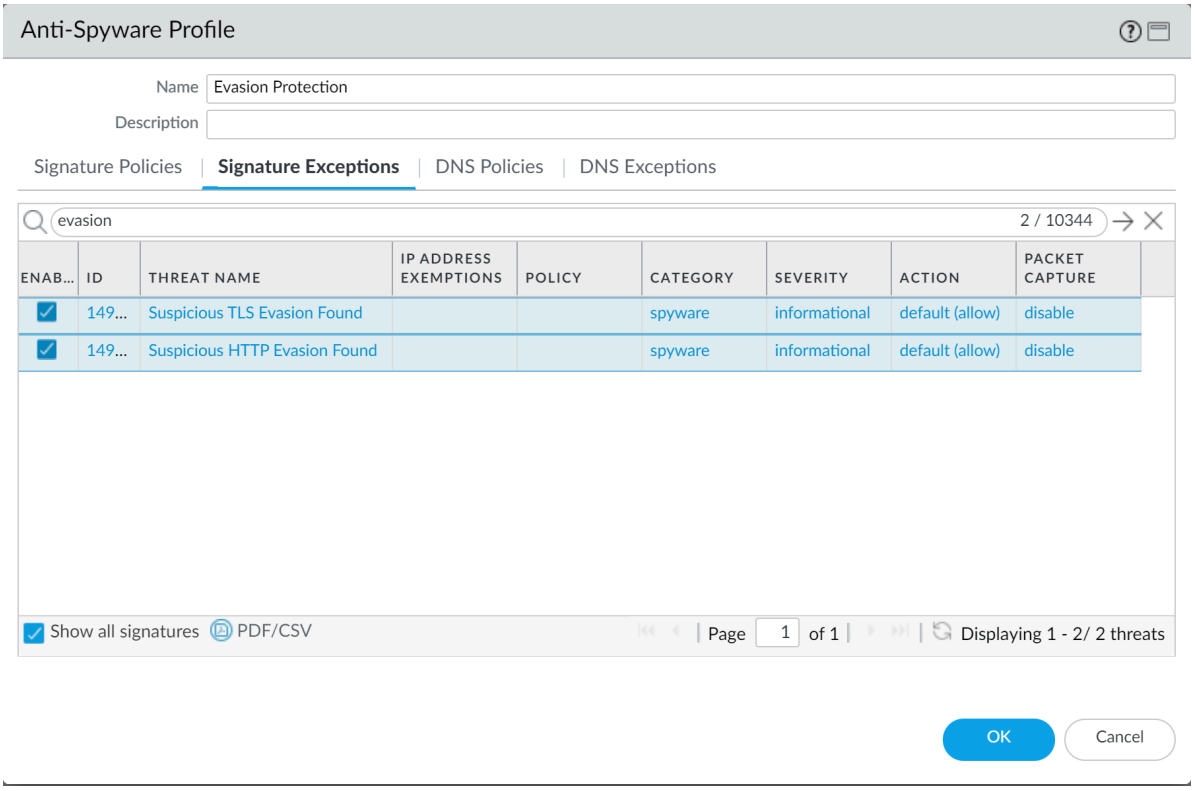
  Le proxy DNS ne fait pas partie du moteur de la politique de sécurité du pare-feu ; à la place, il ordonne au pare-feu de résoudre les noms d'hôtes DNS, tout en maintenant le mappage entre le domaine et l'IP, ce qui est crucial pour empêcher l'évasion TLS/HTTP.

  - Configurez un objet proxy DNS.

    Lorsqu'il sert de proxy DNS, le pare-feu résout les requêtes DNS et met en cache les associations d'adresses IP à un nom d'hôte pour résoudre rapidement et efficacement les requêtes DNS futures.
  - Activer les signatures d'évasion

    Les signatures d'évasion qui détectent des requêtes HTTPS ou TLS fabriquées peuvent envoyer des alertes lorsque des clients se connectent à un domaine autre que celui qui est indiqué dans la requête DNS d'origine. Assurez-vous de configurer le proxy DNS avant d'activer les signatures d'évasion. Sans proxy DNS, les signatures d'évasion peuvent déclencher des alertes lorsqu'un serveur DNS dans une configuration d'équilibrage de

charge DNS retourne des adresses IP différentes (pour les serveurs qui hébergent des ressources identiques) au pare-feu et au client en réponse à la même requête DNS.

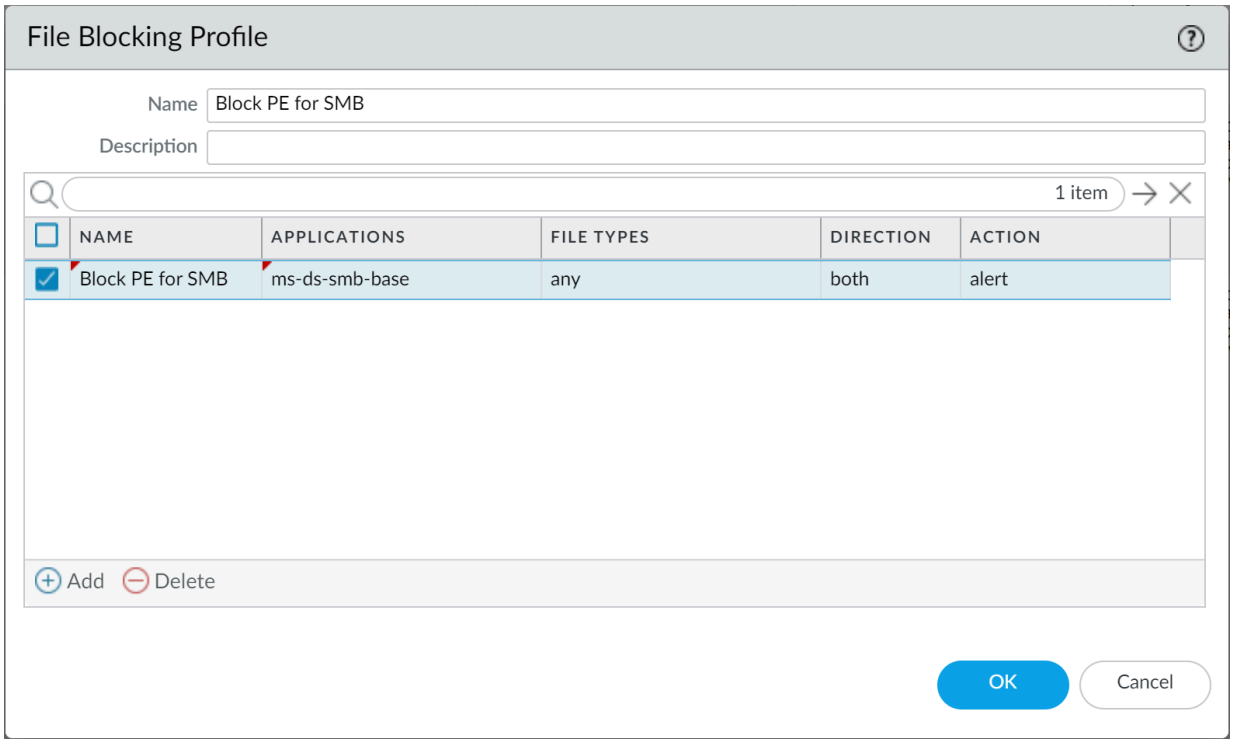


- Pour les déploiements utilisant Prisma Access ou des réseaux sans serveur DNS interne, configurez votre politique DNS pour utiliser l'adresse IP de l'entonnoir de Palo Alto Networks (72.5.65.111) au lieu du FQDN de l'entonnoir par défaut (sinkhole.paloaltonetworks.com).

  Le gouffre DNS utilisé par le profil Anti-Spyware permet au pare-feu de falsifier une réponse à une requête DNS pour les domaines qui correspondent à la catégorie configurée pour une action de gouffre au serveur de gouffre spécifié, afin de faciliter l'identification des hôtes compromis. Lorsque le nom de domaine complet par défaut du gouffre est utilisé, le pare-feu envoie l'enregistrement CNAME en réponse au client, dans l'espoir qu'un serveur DNS interne résoudra l'enregistrement CNAME, ce qui permettra aux communications malveillantes du client vers le serveur de gouffre configuré d'être enregistrées et facilement identifiables. Toutefois, si des clients utilisant Prisma Access, se trouvent dans des réseaux sans serveur DNS interne ou utilisent d'autres logiciels ou outils qui ne peuvent pas résoudre correctement un CNAME en une réponse d'enregistrement A, la requête DNS est supprimée, ce qui se traduit par des détails incomplets du journal du trafic qui sont cruciaux pour l'analyse des menaces.
- Pour les serveurs, créez des règles de politique de sécurité qui n'autorisent que les applications que vous autorisez sur chaque serveur. Vérifiez que le port standard pour l'application

correspond au port d'écoute sur le serveur. Par exemple, pour garantir que seul le trafic SMTP est autorisé sur votre serveur de messagerie, définissez l'Application sur **smtp (smtp)** et définissez le Service sur **application-default (par défaut de l'application)**. Si votre serveur n'utilise qu'un sous-ensemble de ports standard (par exemple, si votre serveur SMTP n'utilise que le port 587, tandis que les ports standard de l'application SMTP sont définis sur 25 et 587), créez un nouveau service personnalisé qui n'inclut que le port 587 et utilisez ce nouveau service dans votre règle de politique de sécurité plutôt que d'utiliser l'option Par défaut de l'application. De plus, assurez-vous de restreindre l'accès à des zones source et de destination ainsi qu'à des ensembles d'adresses IP donnés.

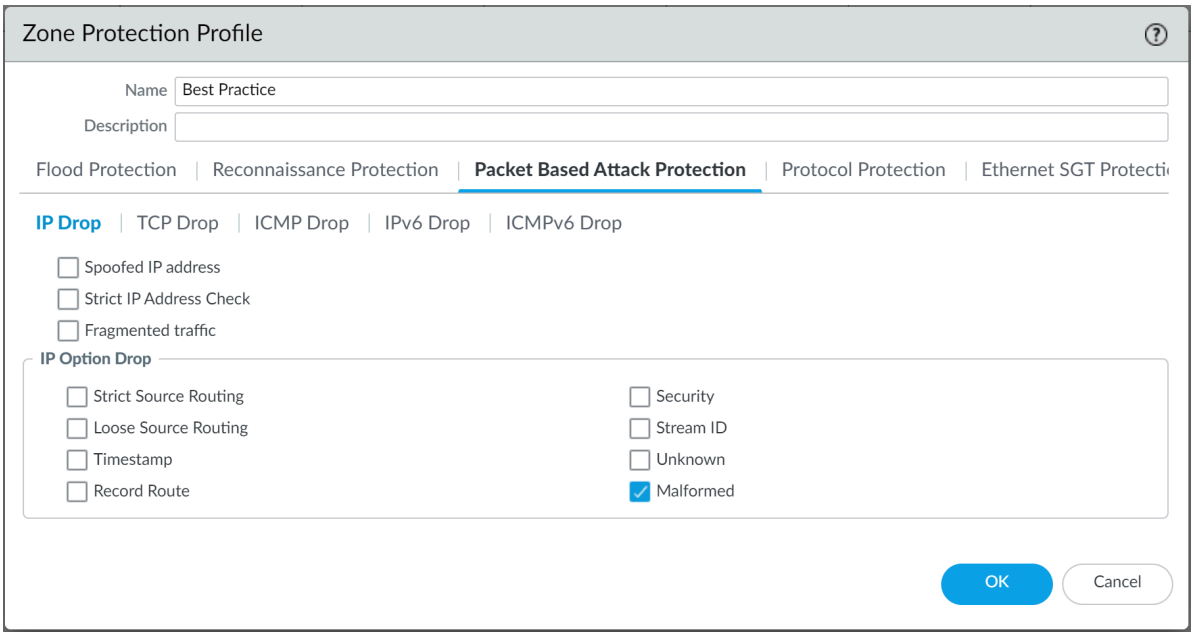
- Bloquez l'ensemble du trafic et des applications inconnu(es) à l'aide de la politique de sécurité. Normalement, les seules applications qui sont classées dans le trafic inconnu sont des applications internes ou personnalisées sur votre réseau et des menaces potentielles. Le trafic inconnu peut être des applications incompatibles ou des protocoles inhabituels ou anormaux, ou encore des applications connues qui utilisent des ports non standard ; dans tous les cas, le trafic inconnu doit être bloqué. Reportez-vous à la section Gestion des applications propres à l'entreprise ou inconnues.
- Procédez au paramétrage du blocage des fichiers pour empêcher les types de fichiers Portable Executable (exécutable portable ; PE) du trafic Server Message Block (blocage des messages du serveur ; SMB) basé sur Internet de transiter entre des zones approuvées à des zones non approuvées (applications ms-ds-smb).



- Bloquez les variantes malveillantes des fichiers PE (exécutables portables), ELF et MS Office, ainsi que les scripts PowerShell et shell en temps réel. L'activation de WildFire Inline ML vous permet d'analyser les fichiers de façon dynamique à l'aide de l'apprentissage automatique sur le pare-feu. Cette couche supplémentaire de protection antivirus complète les signatures

basées sur WildFire afin de fournir une couverture étendue pour les fichiers dont les signatures n'existent pas encore.

- Créez un profil de protection de zone configuré pour éviter toute attaque basée sur les paquets (**Network (Réseau)** > **Network Profiles (Profils réseau)** > **Zone Protection (Protection de zone)**) :
  - Sélectionnez l'option de supprimer les paquets IP **Malformed (Mal formés)**Packet Based Attack Protection (**Protection contre les attaques basées sur les paquets)** > **IP Drop (Abandon d'IP)**).



- Activez l'option **Mismatched overlapping TCP segment (Segments TCP non concordants et se chevauchant)** (**Packet Based Attack Protection (Protection contre les attaques basées sur les paquets)** > **TCP Drop (Abandon TCP)**).

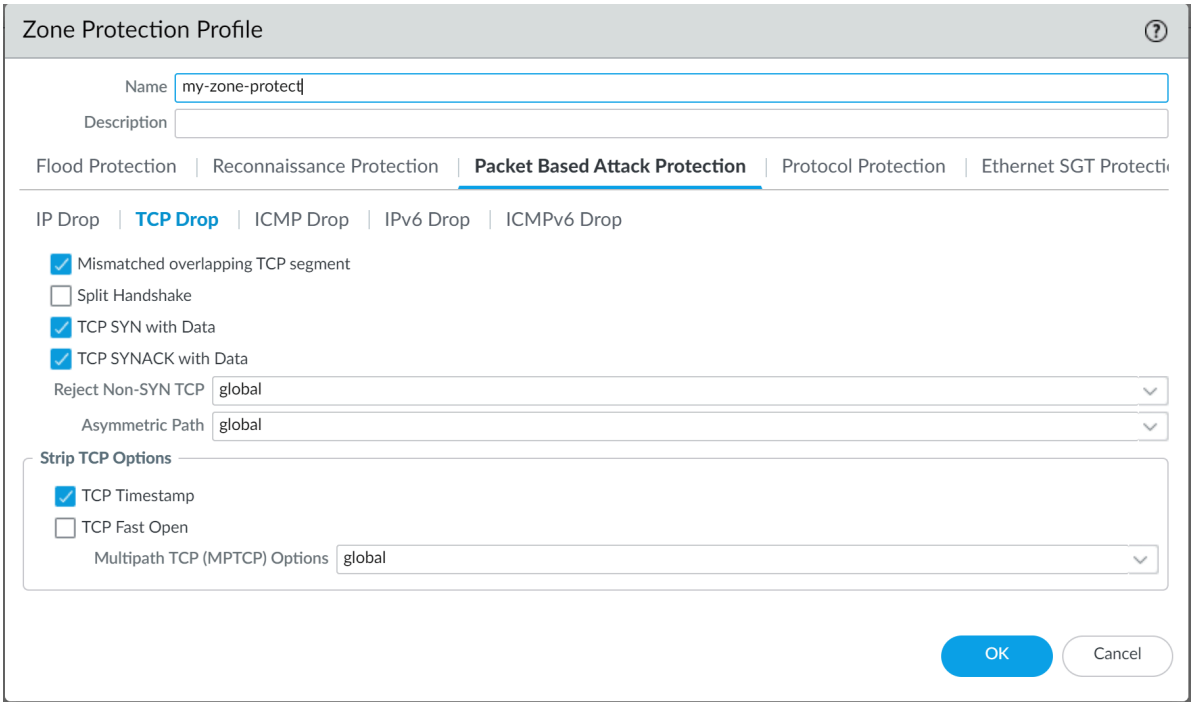
  En établissant délibérément des connexions avec des données superposées, mais différentes, les pirates informatiques essayent d'induire une interprétation erronée de l'action de la connexion et génèrent volontairement des faux positifs ou des faux négatifs. Les pirates utilisent également l'usurpation d'IP et la prédiction du numéro de séquence pour intercepter la connexion d'un utilisateur et y injecter leurs propres données. Sélectionnez l'option **Mismatched overlapping TCP segment (Segment TCP non concordant et se chevauchant)** pour indiquer que PAN-OS ignore les trames contenant des données non concordantes et se chevauchant. Les segments reçus sont ignorés lorsqu'ils sont inclus dans un autre segment, lorsqu'ils chevauchent une partie d'un autre segment ou lorsqu'ils contiennent l'ensemble d'un autre segment.
- Activez les options d'abandon **TCP SYN with Data (paquets TCP SYN contenant des données)** et d'abandon **TCP SYNACK with Data (paquets TCP SYN-ACK contenant des**

données) (Packet Based Attack Protection (Protection contre les attaques basées sur les paquets) > TCP Drop (Abandon TCP)).

L'abandon des paquets SYN et SYN-ACK qui contiennent des données dans la charge utile lors d'une connexion en trois étapes accroît la sécurité en bloquant les logiciels malveillants contenus dans la charge utile et en les empêchant d'extraire des données non autorisées avant que la liaison TCP a été établie.

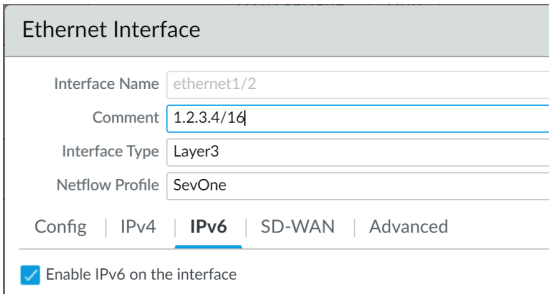
- Supprimez les horodatagesTCP des paquets SYN avant leur transfert par le pare-feu (**Packet Based Attack Protection (Protection contre les attaques basées sur les paquets) > TCP Drop (Abandon TCP)**).

  Lorsque vous activez l'option **Strip TCP Options - TCP Timestamp (Enlever les options TCP - horodatage TCP)**, la pile TCP des deux extrémités de la connexion TCP ne prendra pas en charge les horodatages TCP. Ceci prévient les attaques qui utilisent différents horodatages sur plusieurs paquets ayant le même numéro de séquence.

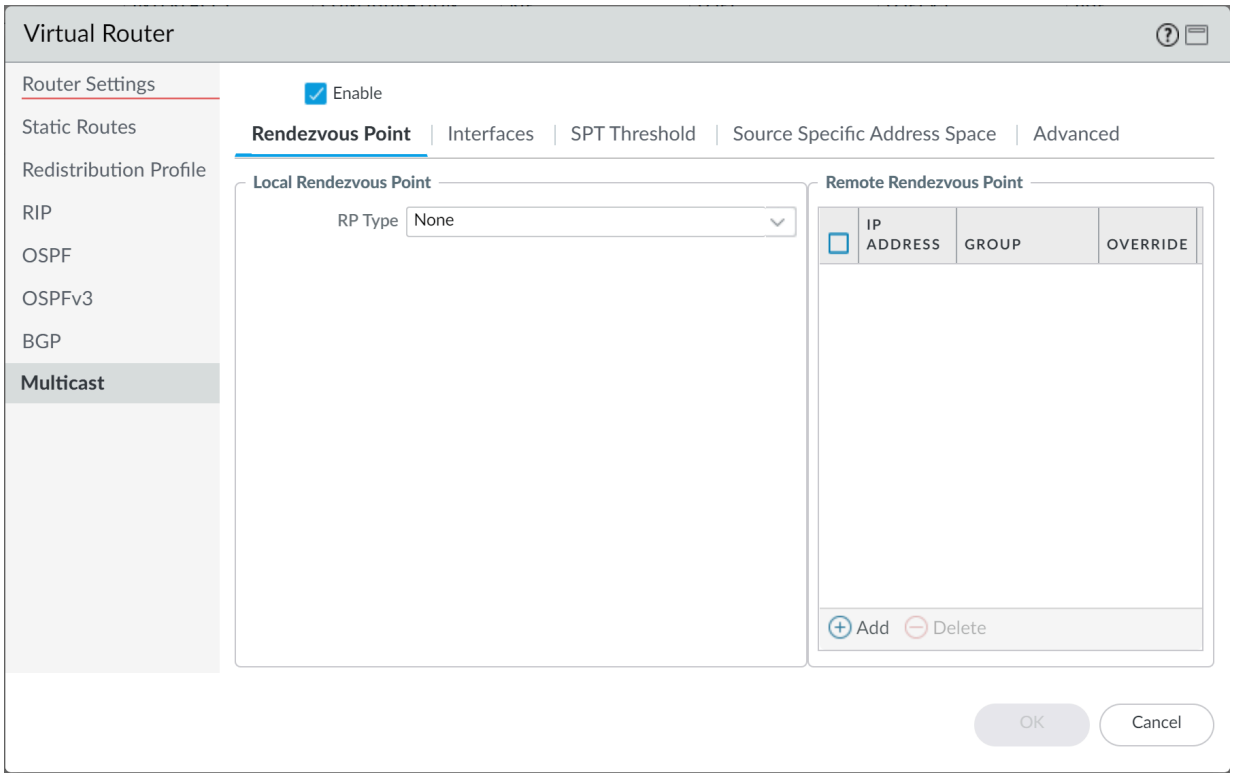


- Si vous configurez les adresses IPv6 sur vos hôtes réseau, assurez-vous d'activer la prise en charge de IPv6, si vous ne l'avez déjà fait (**Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)** > **IPv6 (IPv6)**).

  L'activation de la prise en charge de IPv6 autorise l'accès aux hôtes IPv6 et permet le filtrage des paquets IPv6 encapsulés dans des paquets IPv4, ce qui évite l'exploitation des adresses IPv6 multicast sur IPv4 pour la reconnaissance réseau.



- Activez le support pour le trafic multicast afin que le pare-feu puisse appliquer une politique au trafic multicast (**Network (Réseau)** > **Virtual Router (Routeur virtuel)** > **Multicast (Multidiffusion)**).



- Désactivez les options vous permettant de **Forward datagrams exceeding UDP content inspection queue (Transmettre les datagrammes qui excèdent la file d'attente d'inspection du contenu UDP)** et **Forward segments exceeding TCP content inspection queue (Transmettre les datagrammes qui excèdent la file d'attente d'inspection du contenu TCP)** (**Device (Périphérique)** > **Setup (Configuration)** > **Content-ID (Content-ID)** > **Content-ID Settings (Paramètres de Content-ID)**).

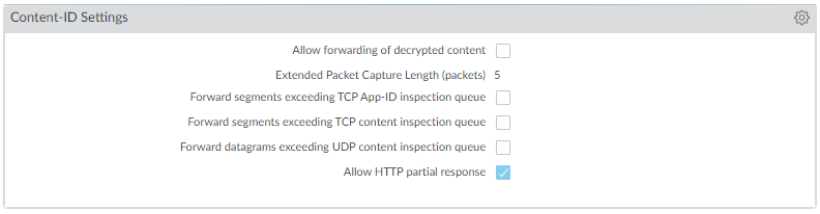
  Par défaut, lorsque la file d'attente d'inspection du contenu TCP ou UDP est pleine, le pare-feu saute l'inspection de contenu pour les segments TCP ou les datagrammes UDP qui excèdent la limite établie pour la file d'attente, soit 64. Le désactivation de cette option garantit l'inspection du contenu pour tous les segments TCP et les datagrammes UDP autorisés par le pare-feu. Dans des circonstances particulières (par exemple, si la plateforme du pare-feu n'est pas bien dimensionnée pour s'harmoniser à un cas pratique), la désactivation de ce paramètre peut compromettre la performance de l'application.

- Désactivez la **Allow HTTP partial response (option Autoriser la réponse partielle HTTP)** (**Device (Périphérique)** > **Setup (Configuration)** > **Content-ID (Content-ID)** > **Content-ID Settings (Paramètres Content-ID)**).

  L'option de réponse partielle HTTP permet à un client d'extraire seulement une partie d'un fichier. Lorsqu'un pare-feu de nouvelle génération identifie et supprime un fichier malveillant dans le chemin d'accès d'un transfert, il met fin à la session TCP à l'aide d'un paquet RST. Si le navigateur Web implémente l'option de plage HTTP, il peut commencer une nouvelle session pour extraire uniquement la partie restante du fichier, ce qui empêche le pare-feu de déclencher à nouveau la même signature en raison de l'absence de contexte dans la session initiale, tout en permettant au navigateur Web de réassembler le fichier et de livrer le contenu malveillant. Pour éviter ce genre de situation, il suffit de désactiver cette option.

  Autoriser la réponse partielle HTTP est activé sur le pare-feu par défaut. Cela offre une disponibilité maximale mais augmente le risque d'une cyberattaque réussie. Pour une sécurité maximale, désactivez cette option pour empêcher le navigateur Web de démarrer une nouvelle session pour récupérer le reste d'un fichier après que le pare-feu a mis fin à la session d'origine en raison d'une activité malveillante. La désactivation de la réponse partielle HTTP affecte les transferts de données HTTP qui utilisent l'en-tête RANGE, ce qui peut entraîner des anomalies de service pour certaines applications. Après avoir désactivé la réponse partielle HTTP, validez le fonctionnement de vos applications stratégiques.

  Si vous rencontrez une interruption du transfert de données HTTP sur une application stratégique, vous pouvez créer une stratégie de remplacement d'application pour cette application spécifique. Étant donné que application Override contourne App-ID (y compris l'inspection des menaces et du contenu), créez une stratégie Application Override uniquement pour l'application critique spécifique et spécifiez les sources et les destinations pour limiter la règle (principe de l'accès au moindre privilège). Ne créez pas de stratégie de remplacement d'application, sauf si vous le devez. Pour plus d'informations sur les stratégies de remplacement d'application, reportez-vous à https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVLCA0.



- Créez un profil de protection contre les vulnérabilités qui bloque les anomalies de protocole et toutes les vulnérabilités ayant un niveau de gravité faible et plus élevé.

  Une anomalie de protocole se produit lorsque le comportement d'un protocole s'écarte de l'utilisation standard et conforme. Par exemple, un paquet malformé, une application mal conçue ou une application qui s'exécute sur un port non standard sont tous des anomalies de protocole et pourraient servir de techniques d'évasion.

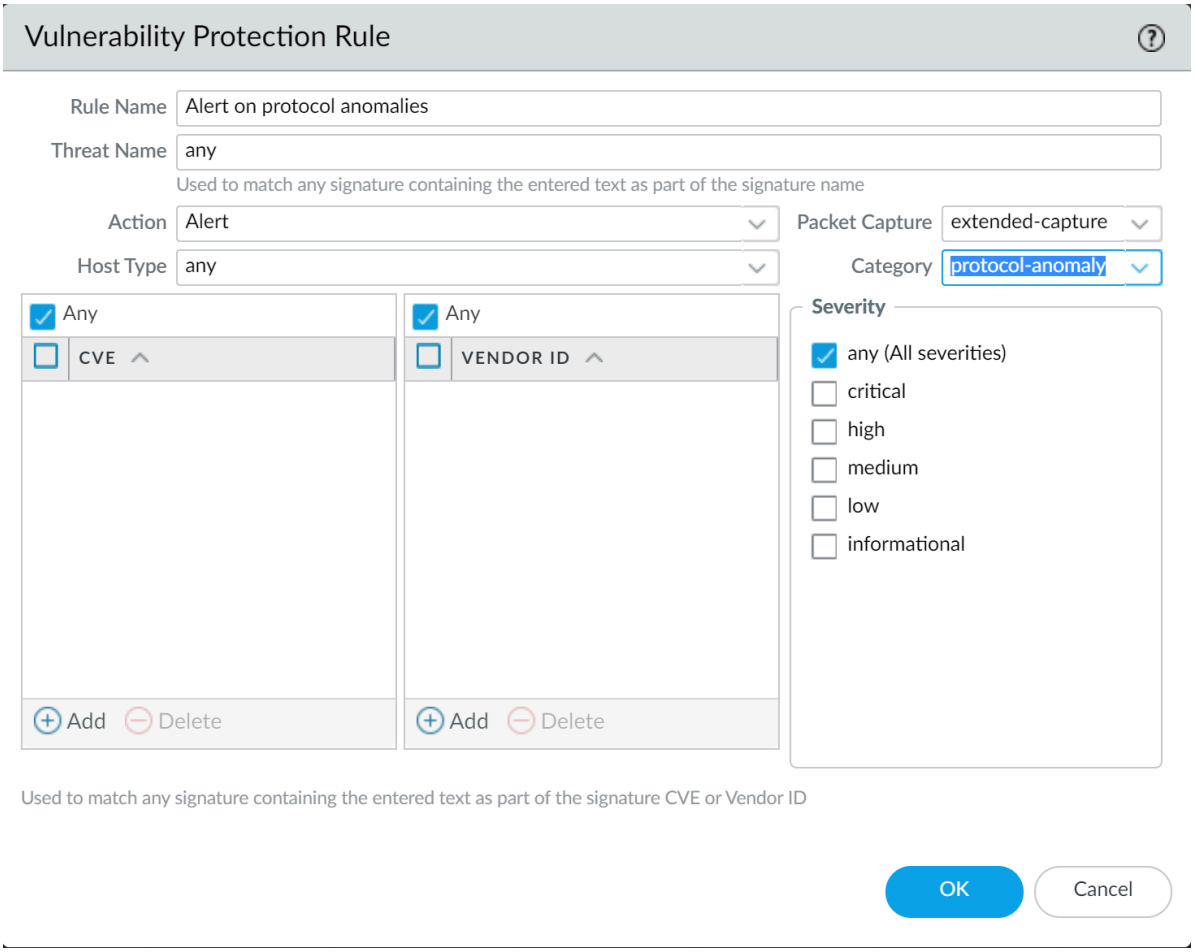
  Si vous disposez d'un réseau stratégique, où l'entreprise privilégie la disponibilité des applications, vous devriez commencer par recevoir des alertes lorsque des anomalies de protocole sont détectées pendant un certain temps pour vous assurer qu'aucune application stratégique interne n'utilise de protocoles établis d'une manière non standard. Si vous découvrez que certaines applications critiques déclenchent des signatures d'anomalies de protocole, vous pouvez alors les exclure de l'application des anomalies de protocole. Pour ce faire, ajoutez une autre règle au profil de protection contre les vulnérabilités qui autorise les anomalies de protocole et associez le profil à la règle de politique de sécurité qui applique le trafic vers les applications critiques et depuis ces dernières.

  Assurez-vous que les règles du profil de protection contre les vulnérabilités et que les règles du profil de sécurité qui autorisent les anomalies de protocole détectées dans les applications critiques internes se trouvent au-dessus des règles qui bloquent les anomalies de protocole. Le trafic est comparé aux règles de la politique de sécurité et aux règles des profils de protection contre les vulnérabilités de haut en bas ; il est mis en œuvre en fonction de la première règle correspondante.

  - Commencez par recevoir des alertes relatives aux anomalies de protocole :

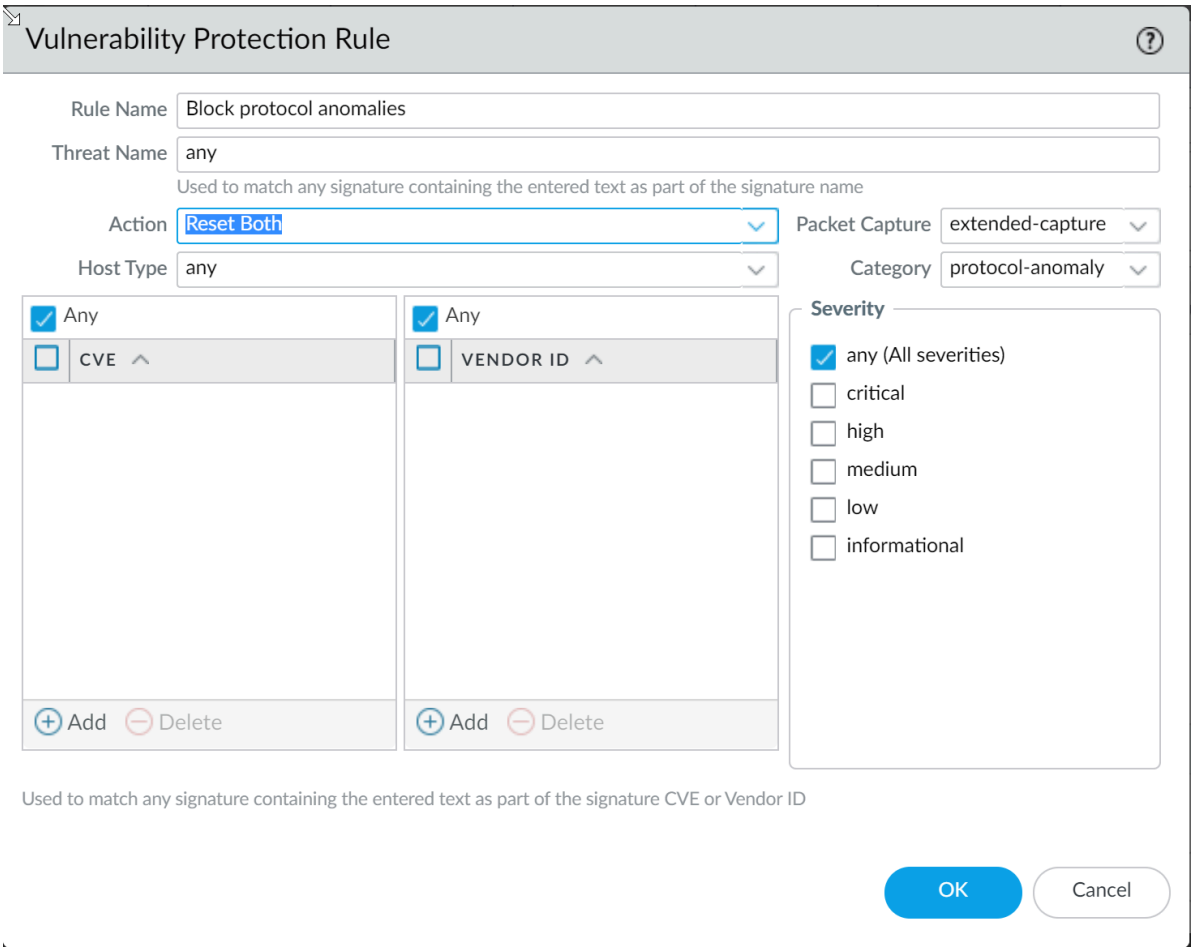
    Créez une règle de profil de protection contre les vulnérabilités pour laquelle l'**Action (Action)** est définie sur Alert (Alerter), la **Category (Catégorie)** est définie sur protocol-anomaly (anomalie de protocole), et la **Severity (Gravité)** est définie sur Any (Tout). Surveillez votre trafic pour déterminer si des applications critiques internes utilisent des protocoles établis de manière non standard. Si c'est le cas, continuez à autoriser les

anomalies de protocole pour ces applications, puis bloquez les anomalies de protocole de toutes les autres applications.



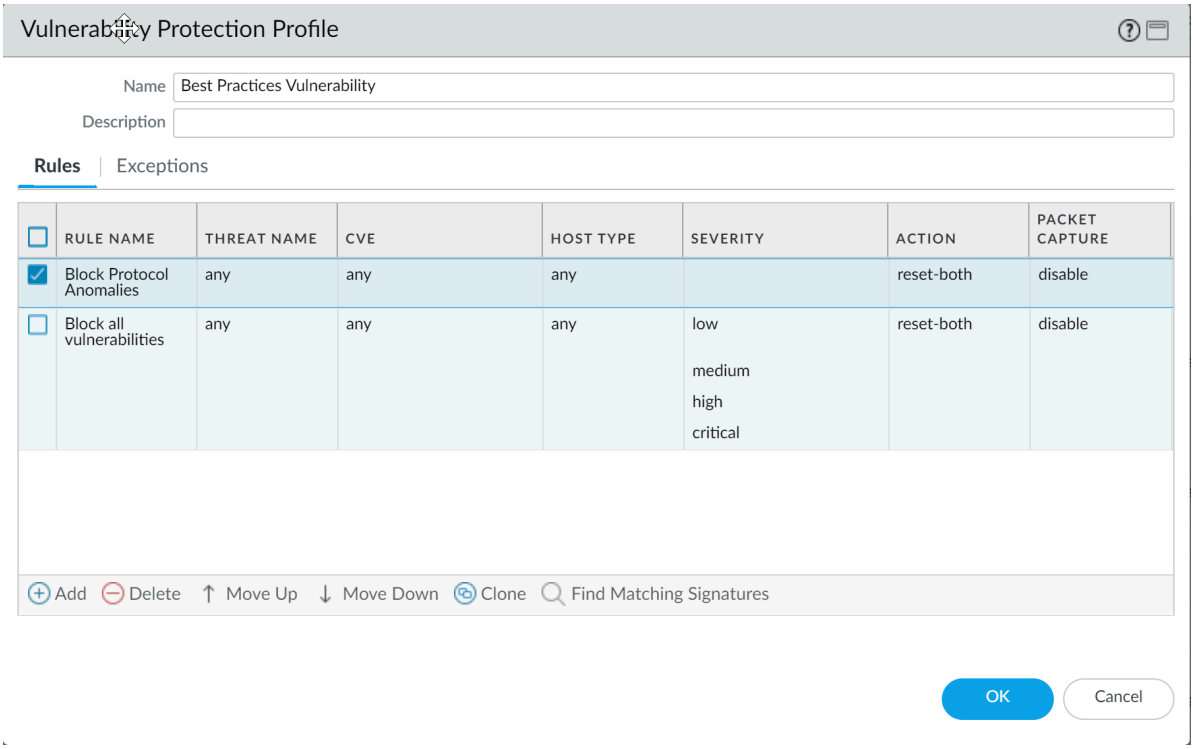
- Bloquez les anomalies de protocole :

  Créez une règle de profil de protection contre les vulnérabilités pour laquelle la **Category (Catégorie)** est définie sur protocol-anomaly (anomalie de protocole), l'**Action (Action)** est définie sur Reset Both (Réinitialiser les deux), et la **Severity (Gravité)** définie sur Any (Tout).



- Vous pouvez éventuellement autoriser les anomalies de protocole pour les applications critiques qui utilisent des protocoles établis de manière non standard. Pour ce faire, créez une règle de profil de protection contre les vulnérabilités qui autorise les anomalies de protocole : définissez l'**Action** de la règle sur Allow (Autoriser), la **Category (Catégorie)** sur protocol-anomaly (anomalie de protocole) et la **Severity (Sévérité)** sur Any (Tout). Associez la règle de profil de protection contre les vulnérabilités à la règle de la politique de sécurité qui applique le trafic vers les applications critiques et depuis ces dernières.

- Ajoutez une autre règle au profil de protection contre les vulnérabilités pour bloquer toutes les vulnérabilités ayant un niveau de gravité faible et plus élevé. Cette règle doit figurer après la règle qui bloque les anomalies de protocole.



- [ ] Passez à l'association des profils de sécurité suivants à vos règles de politique de sécurité pour bénéficier d'une protection basée sur les signatures :
  - Un profil antispyware pour bloquer tous les logiciels espions ayant un niveau de gravité faible et plus élevé.
  - Un profil antivirus pour bloquer tout contenu correspondant à une signature antivirus.

Partage de Données de Prévention des Menaces avec Palo Alto Networks

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

La télémétrie est le processus de collecte et de transmission des données à analyser. Lorsque vous activez la télémétrie sur le pare-feu, le pare-feu collecte et transmet régulièrement les données qui contiennent des informations sur les applications, les menaces, et l'état des périphériques vers Palo Alto Networks. Partager des données de prévention des menaces apporte les bénéfices suivants :

- Des signatures de surveillance de logiciels espion et de vulnérabilités renforcées sont fournies à tous ses clients à échelle mondiale. Par exemple, lorsqu'une menace particulière déclenche des signatures de surveillance de vulnérabilité ou de logiciel espion, le pare-feu partage les URL associés avec cette menace avec l'équipe de recherche de menaces Palo Alto Networks, pour qu'elle puisse classer ces URL comme malveillantes.
- L'exécution de tests rapides et d'évaluation de signatures de surveillance de menaces, sans impact sur votre réseau, afin que les signatures de surveillance de menaces critiques soient rendues accessibles à tous les clients de Palo Alto Networks plus rapidement.
- Précision et détection des codes malveillants accrues au sein du Filtrage des URL PAN-DB, des signatures (C2) de commande et de contrôle basées sur DNS, et de Wildfire.

Palo Alto Networks utilise les données de prévention des menaces issues de la télémétrie pour les rendre accessibles à tous les utilisateurs de Palo Alto Networks. Tous les utilisateurs de Palo Alto Networks bénéficient des données que chaque participant à la télémétrie partage, ce qui fait de la télémétrie une approche communautaire pour la prévention des menaces. Palo Alto Networks ne partage pas vos données de télémétrie avec d'autres clients ou d'autres organisations tierces.

Pour en savoir plus sur la télémétrie, y compris ses avantages, ses utilisations et sa configuration, reportez-vous à la section Télémétrie des périphériques.

Ressources Advanced Threat Prevention

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

Pour plus d'informations sur les meilleures pratiques de prévention des menaces, reportez-vous aux sources suivantes :

- Création de signatures de menaces personnalisées
- Meilleures pratiques pour sécuriser votre réseau contre les fuites au niveau des couches 4 et 7
- Bonnes pratiques en matière de URL Filtering
- Meilleures pratiques du Zero Trust
- Protection DoS et Protection de Zones Respectant les Bonnes Pratiques

Pour afficher une liste des menaces et applications que les produits Palo Alto Networks peuvent identifier, consultez les liens ci-dessous :

- Applipedia : fournit des informations sur les applications que Palo Alto Networks peut identifier.
- Archivage sécurisé des menaces: répertorie les menaces que les produits Palo Alto Networks peuvent identifier. Vous pouvez rechercher des menaces par vulnérabilité, logiciel espion ou virus. Cliquez sur l'icône Détails en regard du numéro d'identification pour plus d'informations sur une menace.

Configurer Threat Prevention

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

Avant de pouvoir activer et configurer l'analyse cloud en ligne, vous devez obtenir et installer une licence Threat Prevention ou Advanced Threat Prevention (pour accéder aux fonctionnalités d'analyse cloud en ligne) en plus de toute licence de plateforme à partir de laquelle elle est exploitée. Les licences sont activées à partir du portail d'assistance client Palo Alto Networks et doivent être actives avant que vous puissiez activer l'une des fonctionnalités de prévention des menaces. En outre, Threat Prevention (semblable à d'autres services de sécurité Palo Alto Networks) est administrée par le biais de profils de sécurité, qui dépendent à leur tour de la configuration des politiques d'application des réseaux, telles que définies par les règles de politique de sécurité. Avant d'activer Threat Prevention, il est recommandé de vous familiariser avec les composants de base de la plate-forme de sécurité dans laquelle les abonnements de sécurité sont activés. Reportez-vous à votre documentation du produit pour plus d'informations.

Pour activer et configurer votre abonnement Prévention des menaces afin qu'il fonctionne de manière optimale au sein de votre déploiement de sécurité réseau, reportez-vous aux tâches ci-dessous. Bien qu'il ne soit peut-être pas nécessaire de mettre en œuvre tous les processus illustrés ici, Palo Alto Networks recommande de passer en revue toutes les tâches pour vous familiariser avec les options disponibles pour un déploiement réussi. Il est également recommandé de suivre les meilleures pratiques fournies par Palo Alto Networks pour une convivialité et une sécurité optimales.

Paramétrage des profils Antivirus, Antispyware et Protection contre les vulnérabilités

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

Chaque pare-feu de dernière génération Palo Alto Networks est fourni avec les profils Antivirus, Antispyware et Protection contre les vulnérabilités prédéfinis que vous pouvez associer aux politiques de sécurité. Il y a un seul profil Antivirus prédéfini, **DEFAULT (par défaut)**, qui utilise l'action par défaut pour chaque protocole (blocage du trafic HTTP, FTP et SMB, et alerte pour le trafic SMTP, IMAP et POP3). Il existe deux profils Antispyware et Protection contre les vulnérabilités prédéfinis :

- **default (par défaut)** : applique l'action par défaut à l'ensemble des événements de protection contre les vulnérabilités/logiciels espions du client et du serveur dont le niveau de gravité est critique, élevé et moyen. Il ne détecte pas les événements dont le niveau de gravité est faible et informations.
- **strict** : applique la réponse de blocage à l'ensemble des événements de protection contre les vulnérabilités/logiciels espions du client et du serveur dont le niveau de gravité est critique, élevé et moyen. Par ailleurs, il utilise l'action par défaut pour les événements dont le niveau de gravité est faible et informations.

Afin de vous assurer que le trafic entrant sur votre réseau ne comporte aucune menace, associez les profils prédéfinis à vos politiques d'accès Web de base. Lorsque vous surveillez le trafic sur votre réseau et étendez votre base de règles de politique, vous pouvez créer des profils plus granulaires pour répondre à vos besoins spécifiques en matière de sécurité.

Utilisez le flux de travail suivant pour paramétrer les Profils de Sécurité relatifs aux Antivirus, Antispyware et Protection contre les vulnérabilités.

- Strata Cloud Manager
- PAN-OS et Panorama

Configurer l'antivirus, l'anti-spyware et la protection contre les vulnérabilités (Cloud Management)

STEP 1 | Utilisez les informations d'identification associées à votre compte d'assistance Palo Alto Networks et connectez-vous au Strata Cloud Manager sur le hub.

L'abonnement Prévention des menaces regroupe les fonctionnalités antivirus, antispyware et de protection contre les vulnérabilités dans une seule licence et fait partie de votre abonnement Prisma Access. Pour obtenir des informations sur les applications et services offerts avec Prisma Access, reportez-vous à Toutes les applications et tous les services disponibles. Pour vérifier les abonnements pour lesquels vous disposez actuellement de licences actives, Vérifiez ce qui est pris en charge avec votre licence.

STEP 2 | (Facultatif) Créez des profils de sécurité personnalisés pour les antivirus, les antispyware, et la protection contre les vulnérabilités.

Vous pouvez également utiliser les profils prédéfinis des bonnes pratiques.

Passez en toute sécurité *aux* profils de sécurité exemplaire *pour disposer de meilleure posture de sécurité.*

- Pour créer des profils WildFire et Antiviruspersonnalisés, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **WildFire et Antivirus** et **Add Profile (Ajouter un profil)**. Utilisez les étapes de transition vers un profil antivirus pour atteindre votre objectif en toute sécurité
- Pour créer des profils antispyware personnalisés, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Anti-Spyware (Antispyware)** et **Add Profile (Ajouter un profil)**. Utilisez les étapes de transition vers un profil antispyware pour atteindre votre objectif en toute sécurité
- Pour créer des profils de protection contre les vulnérabilités personnalisés, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Vulnerability protection (Protection contre les vulnérabilités** > **Security Services (Services de sécurité)** et **Add Profile (Ajouter un profil)**. Utilisez les étapes de transition vers un profil de protection contre les vulnérabilités pour atteindre votre objectif en toute sécurité

STEP 3 | Attachez des profils de sécurité à vos **Security Policy Rules (Règles de politique de sécurité)**. Prisma Access applique par défaut les meilleures pratiques des règles de politique de sécurité.

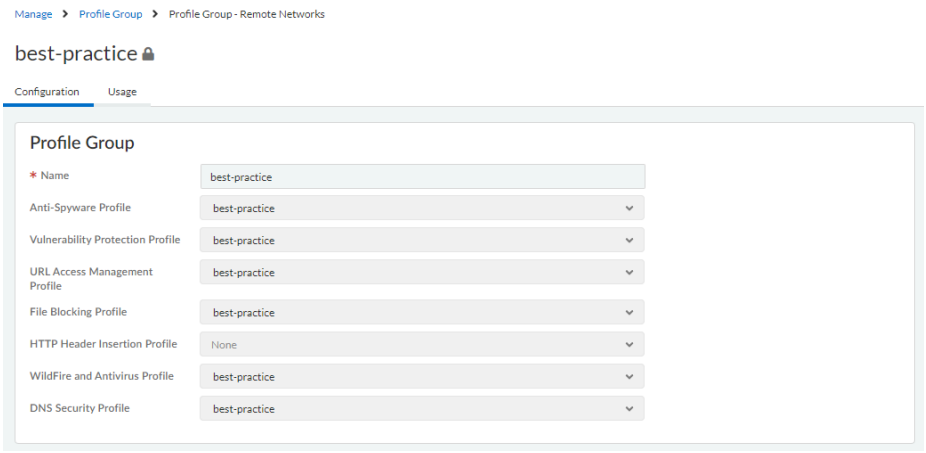
Lorsque vous configurez une règle de politique de sécurité qui utilise un profil de protection contre les vulnérabilités pour bloquer les connexions lors de la détection d'exploits ou de tentatives d'accès non autorisé, Prisma Access bloque automatiquement ce trafic et enregistre ces incidents (se reporter à Surveiller les adresses IP bloquées*).*

1. Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Security Policy (Politique de sécurité)** et sélectionnez la règle que vous souhaitez modifier ou **Add Rule (Ajouter une règle)**.
2. Dans **Action and Advanced Inspection (Action et inspection avancée)**, sélectionnez le **Profile Group (Groupe de profils)** qui inclut les profils de sécurité suivants : **WildFire et**

Antivirus, **Anti-Spyware (Antispyware)**et **Vulnerability Protection (Protection contre les vulnérabilités)**.

*Vous pouvez créer de nouveaux groupes de profils dans **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Profile Groups (Groupes de profils)**. Pour plus d'informations, reportez-vous à Activer un profil de sécurité.*

*Par défaut, le groupe de profils **best practice (meilleures pratiques)** est activé avec la configuration des meilleures pratiques pour tous les profils de sécurité disponibles.*



STEP 4 | Validez vos modifications.

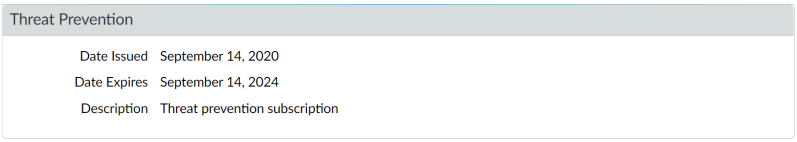
Configurer l'antivirus, l'anti-spyware et la protection contre les vulnérabilités (NGFW (Managed by PAN-OS or Panorama))

*Palo Alto Networks définit une action par défaut pour toutes les signatures antispyware et de protection contre les vulnérabilités. Pour afficher l'action par défaut, sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware (Antispyware)** ou **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Vulnerability Protection (Protection contre les vulnérabilités)**, puis choisissez un profil. Cliquez sur l'onglet Exceptions puis sur Montrer toutes les signatures pour voir une liste de toutes les signatures et l'**Action** correspondante par défaut. Pour modifier l'action par défaut, vous devez créer un nouveau profil, puis spécifier une **Action** et/ou ajouter des exceptions de signature individuelle dans les **Exceptions** du profil.*

STEP 1 | Vérifiez que vous disposez d'un abonnement Prévention des menaces.

L'abonnement Prévention des menaces regroupe les fonctions Antivirus, Anti-logiciel espion et Protection contre les vulnérabilités. Pour vérifier si vous disposez d'un abonnement Prévention

des menaces actif, sélectionnez **Device (Périphérique)** > **Licenses (Licences)** et vérifiez que la date d'expiration de **Threat Prevention (Prévention des Menaces)** se situe dans l'avenir.



STEP 2 | Téléchargez la dernière mise à jour du contenu :

1. Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**, puis cliquez sur **Check Now (Vérifier maintenant)** au bas de la page, pour récupérer les dernières signatures.
2. Dans la colonne **Actions**, cliquez sur **Download (Télécharger)** et installez les dernières mises à jour Antivirus, et ensuite téléchargez et **Install (Installez)** les dernières mises à jour pour les Applications et les Menaces.

STEP 3 | Planifiez les mises à jour de contenu.

Passez en revue les Meilleures pratiques pour les mises à jour du contenu de menace et des applications *pour connaître les informations importantes sur le déploiement des mises à jour.*

1. Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**, puis cliquez sur **Schedule (Calendrier)** pour récupérer automatiquement les mises à jour de signatures pour les **Antivirus** et les **Applications and Threats (Applications et Menaces)**.
2. Précisez la fréquence et la durée des mises à jour :
   - **download-only (télécharger uniquement)** : Le pare-feu télécharge automatiquement les dernières mises à jour selon le calendrier défini mais vous devez les **Install (Installer)** manuellement.
   - **download-and-install (télécharger et installer)** : Le pare-feu télécharge automatiquement les dernières mises à jour selon le calendrier défini et les installe.
3. Cliquez sur **OK** pour sauvegarder le calendrier de mises à jour ; une validation n'est pas requise.
4. (Facultatif) Vous pouvez également saisir le nombre d'heures dans le champ **Threshold (Seuil)** pour indiquer l'antériorité minimale d'une mise à jour avant tout téléchargement. Par exemple, si vous définissez le **Threshold (Seuil)** à **10**, la signature doit dater d'au moins 10 heures avant d'être téléchargée, quel que soit le calendrier.
5. (Configuration HD uniquement) Vous pouvez également choisir de **Sync To Peer (Synchroniser avec l'homologue)**, pour activer la synchronisation de mise à jour de contenu après le téléchargement/l'installation (les paramètres du calendrier ne sont pas transmis au pare-feu homologue ; vous devez configurer manuellement le calendrier sur chaque pare-feu).

   D'autres considérations sont à prendre en compte quand vous choisissez de **Sync To Peer (Synchroniser avec l'homologue)** et la façon de le mettre en place, selon votre déploiement HD :

   - **HD actif/passif** : si le port MGT est utilisé pour le téléchargement des mises à jour de contenu, vous devez configurer les deux pare-feu pour qu'ils procèdent aux

téléchargements et aux installations de manière indépendante. Toutefois, si vous utilisez un port de données pour les mises à jour de contenu, le pare-feu passif ne téléchargera ni n'installera aucune mise à jour avant de devenir actif. Pour garder les calendriers synchronisés sur les deux pare-feu quand vous utilisez un port de données pour les mises à jour, programmez les mises à jour sur les deux pare-feu et ensuite activez **Sync To Peer (Synchroniser avec l'homologue)** pour permettre le téléchargement des mises à jour et leur transmission au pare-feu passif, quel que soit le pare-feu actif.

- **HD actif/actif** : si le port MGT est utilisé pour le téléchargement des mises à jour de contenu sur les deux pare-feu, vous devez sélectionner **download-and-install (télécharger et installer)** sur les deux pare-feu et ne pas activer l'option **Sync To Peer (Synchroniser avec l'homologue)**. Toutefois, si vous utilisez un port de données, sélectionnez **download-and-install (télécharger et installer)** sur les deux pare-feu, puis activez **Sync To Peer (Synchroniser avec l'homologue)**. Ainsi, si l'état d'un pare-feu devient actif secondaire, cette option permet au pare-feu actif de télécharger et d'installer les mises à jour et de les transmettre au pare-feu actif secondaire.

STEP 4 | (Facultatif) Créez des profils de sécurité personnalisés pour les antivirus, les antispyware, et la protection contre les vulnérabilités.

Vous pouvez également utiliser les profils stricts ou par défaut prédéfinis.

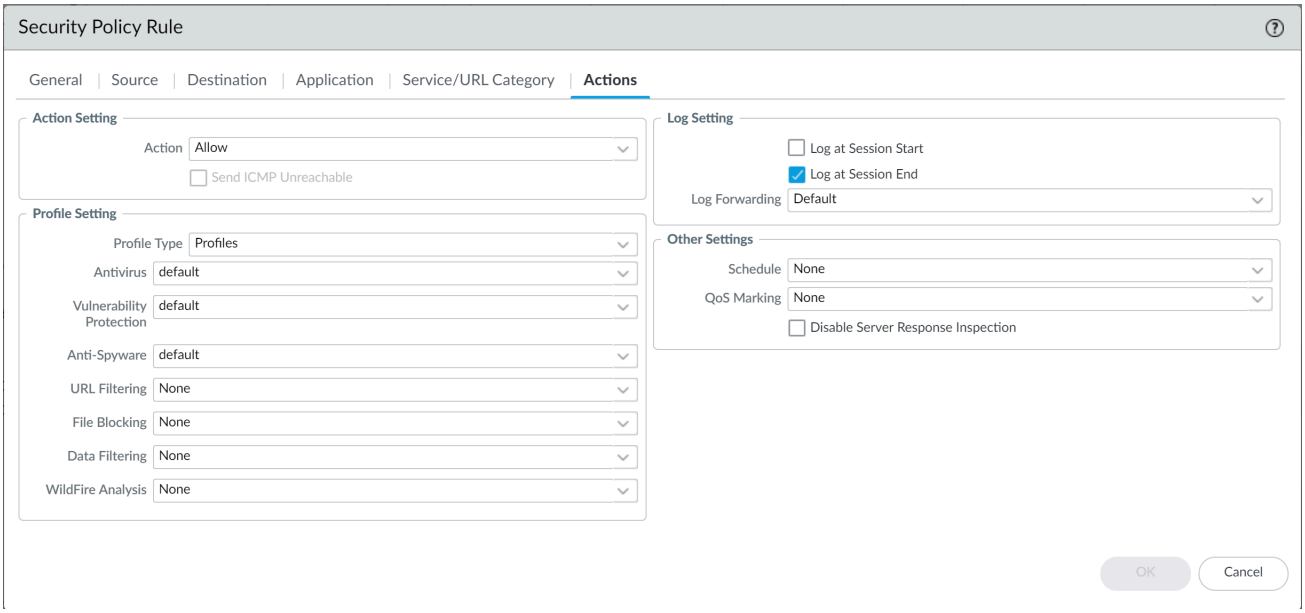
Passez en toute sécurité *aux* profils de sécurité exemplaire *pour disposer de meilleure posture de sécurité.*

- Pour créer des Profils Antivirus personnalisés, sélectionnez **Objects (Objets)** > **Security Profiles (Profils de Sécurité)** > **Antivirus** et **Add (Ajouter)** un nouveau profil. Utilisez les étapes de transition vers un profil antivirus pour atteindre votre objectif en toute sécurité
- Pour créer des Profils Antispyware personnalisés, sélectionnez **Objects (Objets)** > **Security Profiles (Profils de Sécurité)** > **Anti-spyware (Antispyware)** et **Add (Ajouter)** un nouveau profil. Utilisez les étapes de transition vers un profil antispyware pour atteindre votre objectif en toute sécurité
- Pour créer des Profils de protection contre les vulnérabilités, sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Vulnerability protection (Protection contre les vulnérabilités)** et **Add (Ajouter)** un nouveau profil. Utilisez les étapes de transition vers un profil de protection contre les vulnérabilités pour atteindre votre objectif en toute sécurité

STEP 5 | Associez les profils de sécurité à vos règles de politique de sécurité.

Quand vous configurez le pare-feu avec une règle de Politique de sécurité qui utilise un profil de Protection contre les vulnérabilités pour bloquer des connexions, le pare-feu bloque automatiquement ce trafic au niveau matériel (reportez-vous à la section Surveillance des Adresses IP bloquées).

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et sélectionnez la règle que vous voulez modifier.
2. Dans l'onglet **Actions**, sélectionnez **Profiles (Profils)** comme **Profile Type (Type de Profil)**.
3. Sélectionnez les profils de sécurité que vous avez créés pour **Antivirus**, **Anti-Spyware (Antispyware)**, et **Vulnerability Protection (Protection contre les Vulnérabilités)**.



STEP 6 | Validez vos modifications.

Cliquez sur **Commit (Valider)**.

Configurer l'analyse cloud en ligne

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités)

L'analyse cloud en ligne est une fonctionnalité d'Advanced Threat Prevention qui permet de détecter en temps réel les menaces avancées et très évasives de type zero day commande et contrôle (C2) et les vulnérabilités de l'injection de commandes et de l'injection SQL en interrogeant le service cloud Advanced Threat Prevention. La protection de l'analyse cloud en ligne est fournie par le biais de vos profils de sécurité Antispyware et Protection contre les vulnérabilités, les menaces avancées de C2 (commande et contrôle) et de logiciel espion étant gérées par le premier, et les vulnérabilités d'injection de commandes et d'injection SQL par le second.

Les pare-feu pris en charge exploitant PAN-OS 11.2 et les déploiements ultérieurs peuvent également accéder au Deep Learning local pour Advanced Threat Prevention. Le Deep Learning local complète le composant Analyse cloud en ligne d'Advanced Threat Prevention en fournissant un mécanisme permettant d'effectuer une analyse rapide fondée sur le deep learning local des menaces de type zero day et d'autres menaces évasives. Les mises à jour des modèles de Deep Learning local sont fournies par des mises à jour de contenu. En raison des ressources système supplémentaires nécessaires à l'exécution des modules de détection de Deep Learning local, ce dernier n'est disponible que sur les plateformes suivantes :

- PA-5400 Series, sauf l'appareil PA-5450.
- VM-Series (doit allouer au moins 16 Go de mémoire totale)
- Cloud public VM-Series
- Cloud privé VM-Series

Pour activer et configurer l'analyse cloud en ligne et le Deep Learning local, vous devez activer votre licence Advanced Threat Prevention et créer (ou modifier) le profil de sécurité Antispyware and de Protection contre les vulnérabilités. Configurez ensuite les paramètres de politique de chaque moteur d'analyse de catégorie, puis attachez les profils à une règle de politique de sécurité.

Pour plus d'informations sur la création de règles de politique de sécurité, reportez-vous au chapitre Politique du Guide de l'administrateur PAN-OS®.

- Strata Cloud Manager
- PAN-OS et Panorama

Configurer l'analyse cloud en ligne (PAN-OS et Panorama)

L'analyse cloud en ligne d'Advanced Threat Prevention prend en charge plusieurs moteurs de détection, qui nécessitent différentes versions minimales de PAN-OS pour activer :

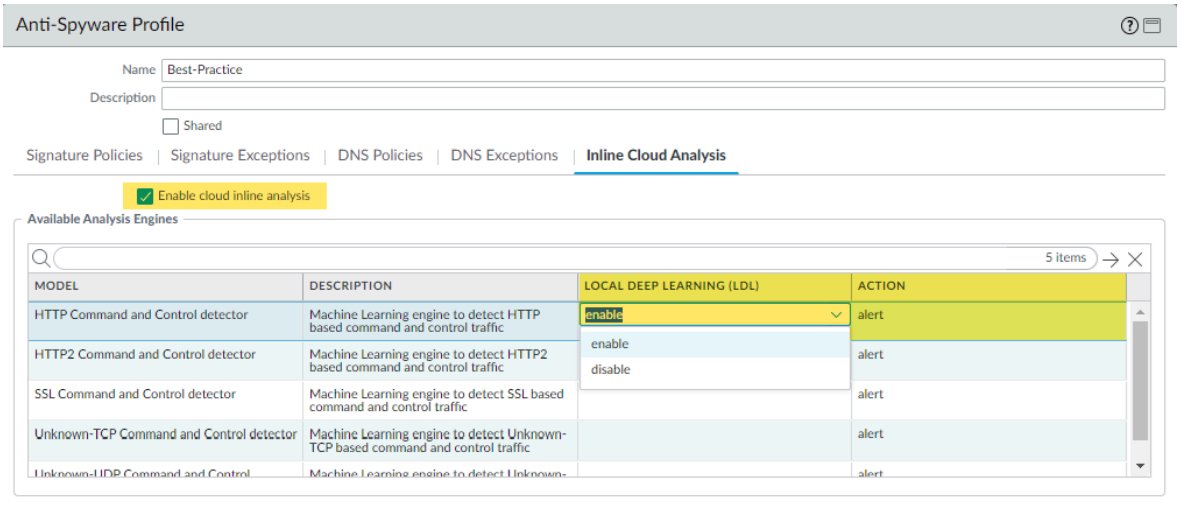
- *La détection des menaces avancées de C2 (commande et contrôle) et des logiciels espions nécessite PAN-OS 10.2 et versions ultérieures.*
- *La détection des menaces d'exploitation de type zero-day nécessite PAN-OS 11.0 et versions ultérieures.*
- *La prise en charge de LDL (Deep Learning local) nécessite PAN-OS 11.2 et versions ultérieures.*

STEP 1 | Connectez-vous à l'interface Web PAN-OS.

STEP 2 | Pour tirer parti de l'analyse cloud en ligne, vous devez disposer d'un abonnement actif à Advanced Threat Prevention.

Pour vérifier les abonnements pour lesquels vous disposez de licences actuellement actives, sélectionnez **Device (Périphérique)** > **Licenses (Licences)** et vérifiez que les licences sont disponibles et ne sont pas expirées.

STEP 3 | Mettez à jour ou créez un nouveau profil de sécurité antispyware pour activer l'analyse cloud en ligne (afin d'analyser le trafic à la recherche des menaces avancées de C2 (commande et contrôle) et des logiciels espions en temps réel).



1. Sélectionnez un **profil Anti-Spyware** existant ou **ajoutez** -en un nouveau (**Objects** > **Security Profiles** > **Anti-Spyware**).

2. Sélectionnez votre profil Antispyware, puis accédez à **Inline Cloud Analysis (Analyse cloud en ligne)** et **Enable inline cloud analysis (Activer l'analyse cloud en ligne)**.
3. (Deep Learning local [pris en charge dans PAN-OS 11.2 et versions ultérieures]) Sélectionnez **enable (activer)** pour chaque moteur d'analyse disponible avec une option **Local Deep Learning (LDL) (Deep Learning Local)**. Il existe actuellement deux moteurs d'analyse disponibles comportant un mode LDL en option : **HTTP Command and Control detector (Détecteur de commande et contrôle HTTP)** et **HTTP2 Command and Control detector (Détecteur de commande et contrôle HTTP2)**.
4. Spécifiez une **action** à entreprendre lorsqu'une menace est détectée à l'aide d'un moteur d'analyse correspondant.

   *L'action par défaut pour chaque moteur d'analyse est **alert (alerte)**, cependant, Palo Alto Networks recommande de définir toutes les actions sur **Reset-Both (Réinitialiser les deux)** pour la meilleure posture de sécurité.*

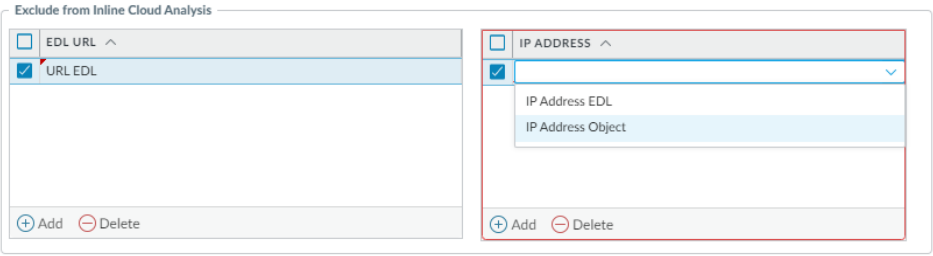
   - **Allow (Autoriser)** : La demande est autorisée et aucune entrée de journal n'est créée.
   - **Alerte**: la demande est autorisée et une entrée de journal des menaces est générée.
   - **Drop**— Supprime la demande ; une action de réinitialisation n'est pas envoyée à l'hôte/à l'application.
   - **Reset Client (Réinitialiser le client)** : la connexion côté client est réinitialisée.
   - **Reset Server (Réinitialiser le serveur)** : la connexion côté serveur est réinitialisée.
   - **Reset Both (Réinitialiser les deux)** : Pour le protocole TCP, la connexion est réinitialisée sur le client et le serveur.
5. Cliquez sur **OK** pour quitter la boîte de dialogue de configuration du profil Anti-Spyware et **Commit (Validez)** vos modifications.

STEP 4 | (Facultatif) Ajoutez des exceptions d'URL et/ou d'adresse IP à votre profil Anti-Spyware si Inline Cloud Analysis produit des faux positifs. Vous pouvez ajouter des exceptions en spécifiant une liste dynamique externe (types de liste d'adresses URL ou IP) ou un objet **Adresses** .

1. Ajoutez une exception d'objet **Listes dynamiques externes** ou **Adresses** [IP].
2. Objets > Profils de sécurité > Profil antispyware
3. Sélectionnez un profil Anti-Spyware pour lequel vous souhaitez exclure des URL et/ou des adresses IP spécifiques, puis sélectionnez **Inline Cloud Analysis**.
4. **Ajoutez** une **URL EDL** ou une **adresse IP** , selon le type d'exception que vous souhaitez ajouter, puis sélectionnez une liste dynamique externe d'URL ou d'adresse IP préexistante. Si aucune n'est disponible, créez une nouvelle external dynamic list (liste dynamique

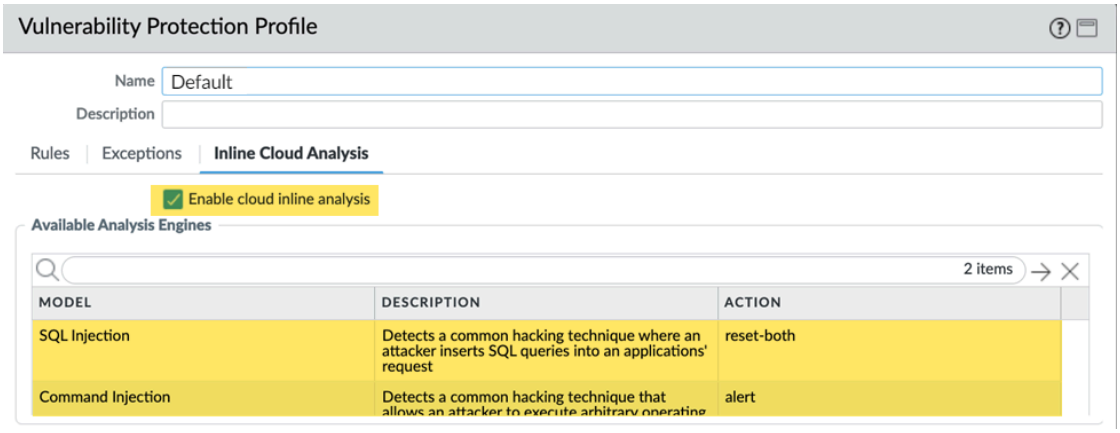
externe). Pour les exceptions d'adresse IP, vous pouvez éventuellement sélectionner une liste d'objets **Adresses** .

*Les profils antispyware configurés comme **Shared (Partagés)** sur les pare-feu gérés par Panorama ne peuvent pas avoir d'objets d'adresse IP ajoutés à la liste des exceptions de l'analyse cloud en ligne.*



5. Cliquez sur **OK** pour enregistrer le profil Anti-Spyware et **valider** vos modifications.

STEP 5 | (Pris en charge dans PAN-OS 11.0 et versions ultérieures) Mettez à jour ou créez un nouveau profil de sécurité de protection contre les vulnérabilités pour activer l'analyse cloud en ligne (afin d'analyser le trafic à la recherche des vulnérabilités d'injection de commandes et d'injection SQL en temps réel).



1. Sélectionnez un profil de sécurité de protection contre les vulnérabilités existant ou **Add (Ajoutez)** un nouveau (**Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Vulnerability Protection (Protection contre les vulnérabilités)**).
2. Sélectionnez votre profil de protection contre les vulnérabilités, puis accédez à **Inline Cloud Analysis (Analyse cloud en ligne)** et cliquez sur **Enable cloud inline analysis (Activer l'analyse cloud en ligne)**.
3. Spécifiez une **Action** à entreprendre lorsqu'un exploit de vulnérabilité est détecté à l'aide d'un moteur d'analyse correspondant. Deux moteurs d'analyse sont actuellement

disponibles : **SQL Injection (Injection SQL)** et **Command Injection (Injection de commandes)**.

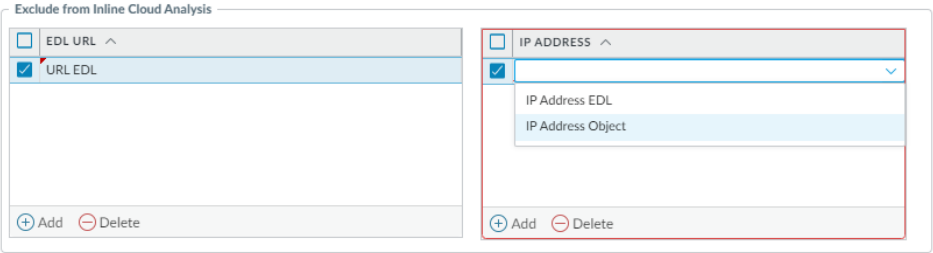
- **Allow (Autoriser)** : La demande est autorisée et aucune entrée de journal n'est créée.
- **Alerte**: la demande est autorisée et une entrée de journal des menaces est générée.
- **Reset Client (Réinitialiser le client)** : la connexion côté client est réinitialisée.
- **Reset Server (Réinitialiser le serveur)** : la connexion côté serveur est réinitialisée.
- **Reset Both (Réinitialiser les deux)** : Pour le protocole TCP, la connexion est réinitialisée sur le client et le serveur.

4. Cliquez sur **OK** pour quitter la boîte de dialogue de configuration du profil de protection contre les vulnérabilités et **Commit (Validez)** vos modifications.

STEP 6 | (Facultatif) Ajoutez des exceptions d'URL et/ou d'adresse IP à votre profil de protection contre les vulnérabilités si l'analyse cloud en ligne produit des faux positifs. Vous pouvez ajouter des exceptions en spécifiant une liste dynamique externe (types de liste d'adresses URL ou IP) ou un objet **Adresses** .

1. Ajoutez une exception d'objet **Listes dynamiques externes** ou **Adresses** [IP].
2. Sélectionnez **Objects > Security Profiles > Vulnerability (Objets > Profils de sécurité > Vulnérabilité)** pour revenir à votre profil de protection contre les vulnérabilités.
3. Sélectionnez un profil de vulnérabilité pour lequel vous souhaitez exclure des URL et/ou des adresses IP spécifiques, puis sélectionnez **Inline Cloud Analysis (Analyse cloud en ligne)**.
4. **Ajoutez** une **URL EDL** ou une **adresse IP** , selon le type d'exception que vous souhaitez ajouter, puis sélectionnez une liste dynamique externe d'URL ou d'adresse IP préexistante. Si aucune n'est disponible, créez une nouvelle external dynamic list (liste dynamique externe). Pour les exceptions d'adresse IP, vous pouvez éventuellement sélectionner une liste d'objets **Adresses** .

   *Les profils de vulnérabilité configurés comme **Shared (Partagés)** sur les pare-feu gérés par Panorama ne peuvent pas avoir d'objets d'adresse IP ajoutés à la liste des exceptions de l'analyse cloud en ligne.*



5. Cliquez sur **OK** pour enregistrer le profil de protection contre les vulnérabilités et **Commit (Valider)** vos modifications.

STEP 7 | Configurez le délai d'expiration et l'action à entreprendre lorsque la requête dépasse la latence maximale.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Content-ID (ID de contenu)** > **Threat Prevention Inline Cloud Analysis (Analyse cloud en ligne pour Threat Prevention)**.
2. Spécifiez la valeur du délai d'expiration et l'action associée à entreprendre lorsque les limites de latence sont atteintes pour les requêtes d'analyse cloud en ligne :
   - Latence maximale (ms) : spécifiez le temps de traitement maximal acceptable, en secondes, pour que l'analyse cloud en ligne renvoie un résultat.
   - Autoriser la latence maximale : permet au pare-feu d'entreprendre l'action d'autorisation lorsque la latence maximale est atteinte. La désélection de cette option définit l'action du pare-feu sur bloquer.
   - Journaliser le trafic non analysé : permet au pare-feu d'enregistrer les requêtes de trafic qui présentent des caractéristiques anormales indiquant la présence de menaces commande et contrôle (C2) avancées et évasives, mais qui n'ont pas été traitées par les analyseurs cloud en ligne de Threat Prevention.
3. Cliquez sur **OK** pour confirmer vos modifications.

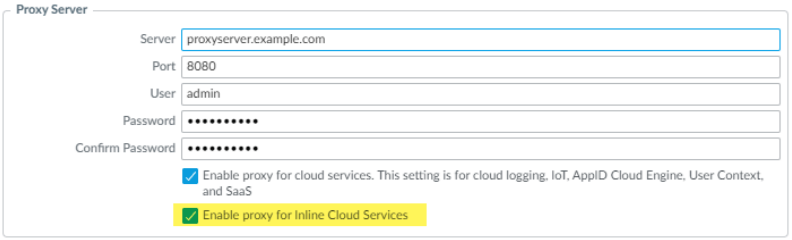
STEP 8 | Installer un certificat de périphérique Répétez pour tous les pare-feu activés pour l'analyse cloud en ligne.

STEP 9 | (Obligatoire lorsque le pare-feu est déployé avec un serveur proxy explicite) Configurez le serveur proxy utilisé pour accéder aux serveurs qui facilitent les requêtes générées par toutes les fonctionnalités d'analyse cloud en ligne configurées. Un seul serveur proxy peut

être spécifié et s'applique à tous les services de mise à jour de Palo Alto Networks, y compris tous les services de cloud et de journalisation en ligne configurés.

1. (PAN-OS 11.2.3 et versions ultérieures) Configurez le serveur proxy via PAN-OS.
   1. Sélectionnez **Device (Périphérique)** > **Configuration** > **Services** et modifiez les détails des **Services**.
   2. Spécifiez les paramètres du **Proxy Server (Serveur proxy)** et cliquez sur **Enable proxy for Inline Cloud Services (Activer le proxy pour les services cloud en ligne)**. Vous pouvez fournir une adresse IP ou un FQDN dans le champ **Server (Serveur)**.

      Le mot de passe du serveur proxy doit contenir au moins six caractères.

   3. Cliquez sur **OK**.
2. (Pour les versions suivantes uniquement : PAN-OS 10.2.11 et versions ultérieures et PAN-OS 11.1.5 et versions ultérieures) Configurez le serveur proxy via la CLI du pare-feu.
   1. Accédez à la CLI du pare-feu.
   2. Configurez les paramètres du serveur proxy de base à l'aide des commandes CLI suivantes :

      ```
      set deviceconfig system secure-proxy-server <FQDN_or_IP>
       set deviceconfig system secure-proxy-port <1-65535>
      ```



```
set deviceconfig system secure-proxy-user <value> set
deviceconfig system secure-proxy-password <value>
```

Le mot de passe du serveur proxy doit contenir au moins six caractères.

3. Autorisez le serveur proxy à envoyer des requêtes aux serveurs de services cloud en ligne à l'aide de la commande CLI suivante :

```
debug dataplane mica set inline-cloud-proxy enable
```

4. Affichez l'état opérationnel actuel de la prise en charge du proxy pour les services cloud en ligne à l'aide de la commande CLI suivante :

```
debug dataplane mica show inline-cloud-proxy
```

Par exemple :

```
debug dataplane mica show inline-cloud-proxy Le proxy pour
 les services avancés est désactivé
```

STEP 10 | (Facultatif) Définissez le nom de domaine complet (FQDN) de contenu cloud utilisé par le pare-feu pour gérer les demandes de service d'analyse cloud en ligne. Le nom de domaine complet par défaut se connecte à hawkeye.services-edge.paloaltonetworks.com, puis se résout au serveur de services cloud le plus proche. Vous pouvez remplacer la sélection

automatique du serveur en spécifiant un serveur de contenu cloud régional qui répond le mieux à vos exigences en matière de résidence et de performances des données.

Le nom de domaine complet de contenu cloud est une ressource utilisée à l'échelle mondiale et affecte la façon dont les autres services qui dépendent de cette connexion envoient des charges utiles de trafic.

Vérifiez que le pare-feu utilise le bon FQDN Content Cloud (**Device (Périphérique)** > **Setup (Configuration)** > **Content-ID (ID de contenu)** > **Content Cloud Setting (Paramètre du Cloud de contenu)**) pour votre région et modifiez le FQDN si nécessaire :

Si votre NGFW est configuré en ligne pour faciliter un déploiement de sécurité SaaS, veuillez noter que les FQDN situés en France et au Japon ne prennent actuellement pas en charge la fonctionnalité de sécurité SaaS.

- Centre des États-Unis (Iowa, États-Unis) : **us.hawkeye.services-edge.paloaltonetworks.com**
- Europe (Francfort, Allemagne) : **eu.hawkeye.services-edge.paloaltonetworks.com**
- Asie-Pacifique (Singapour) : **apac.hawkeye.services-edge.paloaltonetworks.com**
- Inde (Bombay) : **in.hawkeye.services-edge.paloaltonetworks.com**
- Royaume-Uni (Londres, Angleterre) : **uk.hawkeye.services-edge.paloaltonetworks.com**
- France (Paris, France) : **fr.hawkeye.services-edge.paloaltonetworks.com**
- Japon (Tokyo, Japon) : **jp.hawkeye.services-edge.paloaltonetworks.com**
- Australie (Sydney, Australie) : **au.hawkeye.services-edge.paloaltonetworks.com**
- Canada (Montréal, Canada) : **ca.hawkeye.services-edge.paloaltonetworks.com**
- Suisse (Zurich, Suisse) : **ch.hawkeye.services-edge.paloaltonetworks.com**

STEP 11 | (Facultatif) Vérifiez l'état de la connectivité de votre pare-feu au service cloud Advanced Threat Prevention.

Utilisez la commande CLI suivante sur le pare-feu pour afficher l'état de la connexion.

```
show ctd-agent status security-client
```

Par exemple :

```
show ctd-agent status security-client ... Security Client
 AceMlc2(1) Serveur cloud actuel : hawkeye.services-
edge.paloaltonetworks.com Connexion cloud : connecté ...
```

Sortie CLI raccourcie pour plus de brièveté.

Si vous ne parvenez pas à vous connecter au service cloud Advanced Threat Prevention, vérifiez que le domaine suivant n'est pas bloqué : hawkeye.services-edge.paloaltonetworks.com.

STEP 12 | (Facultatif) Surveiller Advanced Threat Prevention

Configurer l'analyse cloud en ligne (Strata Cloud Manager)

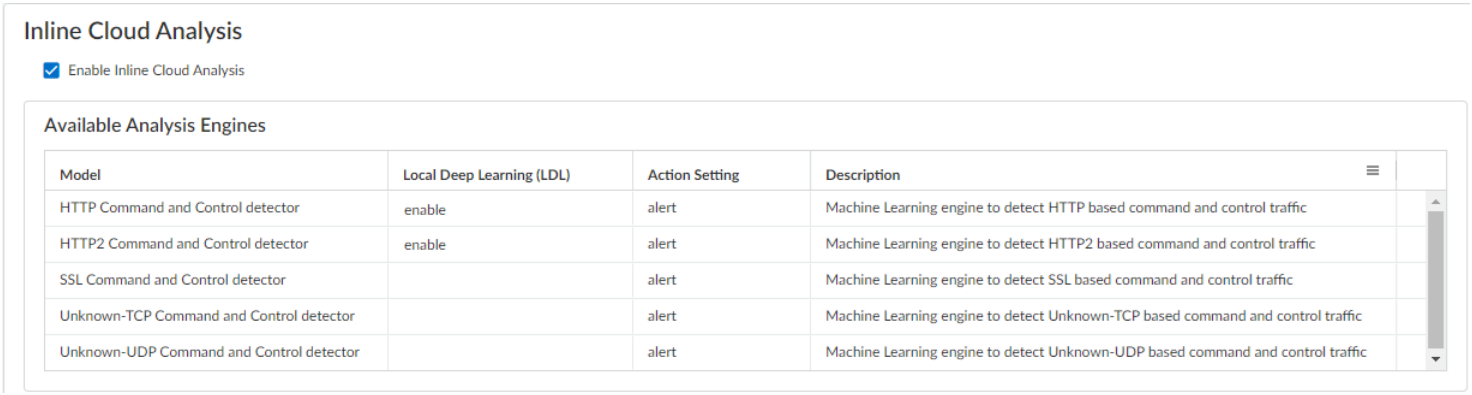
STEP 1 | Pour tirer parti de l'analyse cloud en ligne, vous devez disposer d'un abonnement Prisma Access actif qui donne accès aux fonctionnalités d'Advanced Threat Prevention. Pour obtenir des informations sur les applications et services offerts avec Prisma Access, reportez-vous à Toutes les applications et tous les services disponibles.

Pour vérifier les abonnements pour lesquels vous disposez actuellement de licences actives, Vérifiez ce qui est pris en charge avec votre licence.

STEP 2 | Utilisez les informations d'identification associées à votre compte d'assistance Palo Alto Networks et connectez-vous au Strata Cloud Manager sur le hub.

STEP 3 | Mettez à jour ou créez un nouveau profil de sécurité antispyware pour activer l'analyse cloud en ligne (afin d'analyser le trafic à la recherche des menaces avancées de C2 [commande et contrôle] et des logiciels espions en temps réel).

1. Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Anti-Spyware (Antispyware)**.
2. Sélectionnez votre profil de sécurité antispyware et accédez au volet **Inline Cloud Analysis (Analyse cloud en ligne)** et cliquez sur **Enable Inline Cloud Analysis (Activer l'analyse cloud en ligne)**.



3. Sélectionnez **enable (activer)** pour chaque moteur d'analyse disponible avec une option **Local Deep Learning (LDL) (Deep Learning local)**. Il existe actuellement deux moteurs d'analyse disponibles comportant un mode LDL en option : **HTTP Command and Control detector (Détecteur de commande et contrôle HTTP)** et **HTTP2 Command and Control detector (Détecteur de commande et contrôle HTTP2)**.
4. Spécifiez une **action** à entreprendre lorsqu'une menace est détectée à l'aide d'un moteur d'analyse correspondant.

   *L'action par défaut pour chaque moteur d'analyse est **alert (alerte)**, cependant, Palo Alto Networks recommande de définir toutes les actions sur **Reset-Both (Réinitialiser les deux)** pour la meilleure posture de sécurité.*

   - **Allow (Autoriser)** : La demande est autorisée et aucune entrée de journal n'est créée.
   - **Alerte**: la demande est autorisée et une entrée de journal des menaces est générée.
   - **Drop**— Supprime la demande ; une action de réinitialisation n'est pas envoyée à l'hôte/à l'application.
   - **Reset Client (Réinitialiser le client)** : la connexion côté client est réinitialisée.
   - **Reset Server (Réinitialiser le serveur)** : la connexion côté serveur est réinitialisée.
   - **Reset Both (Réinitialiser les deux)** : Pour le protocole TCP, la connexion est réinitialisée sur le client et le serveur.
5. Cliquez sur **OK** pour quitter la boîte de dialogue de configuration du profil de sécurité antispyware et **Commit (Valider)** vos modifications.

STEP 4 | (Facultatif) Ajoutez des exceptions d'URL et/ou d'adresse IP à votre profil Anti-Spyware si Inline Cloud Analysis produit des faux positifs. Vous pouvez ajouter des exceptions en

spécifiant une liste dynamique externe (types des liste d'adresses URL ou d'IP) ou un objet de politique**Addresses (Adresses)**.

1. Ajoutez une exception d'objet **Listes dynamiques externes** ou **Adresses** [IP].
2. Sélectionnez **Manage (Gérer)** > **Configuration** > **Anti-Spyware (Antispyware)**.
3. Sélectionnez un profil anti-spyware pour lequel vous souhaitez exclure des URL ou des adresses IP spécifiques, puis accédez au volet **Inline Cloud Analysis (Analyse cloud en ligne)**.
4. **Add EDL/URL (Ajouter EDL/URL)** ou **Add IP Address (Ajouter une adresse IP)** selon le type d'exception que vous souhaitez ajouter, puis sélectionnez une liste dynamique externe d'URL ou d'adresses IP préexistante. Si aucune n'est disponible, créez un nouvel objet de politique de liste dynamique externe). Pour les exceptions d'adresse IP, vous pouvez éventuellement sélectionner une liste d'objets **Adresses** .

5. Cliquez sur **OK** pour enregistrer le profil Anti-Spyware et **valider** vos modifications.

STEP 5 | (Facultatif) Surveiller Advanced Threat Prevention

Prévention des attaques par force brute

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

Une attaque par force brute utilise un important volume de requêtes/réponses d'une même adresse ID source ou de destination pour pénétrer par effraction dans un système. Le pirate utilise une méthode essai-et-erreur pour deviner la réponse à un défi ou une requête.

Le profil de protection contre les vulnérabilités contient des signatures permettant de protéger contre les attaques par force brute. Chaque signature dispose d'un ID, d'un nom de menace et d'un niveau de gravité. Elle se déclenche lors de l'enregistrement d'un modèle. Le modèle indique les conditions et l'intervalle d'identification du trafic en tant qu'attaque par force brute ; certaines signatures sont associées à une autre signature enfant dont la gravité est moindre et qui indique le modèle de correspondance. Lorsqu'un modèle correspond à la signature ou à la signature enfant, il déclenche l'action par défaut de la signature.

Pour appliquer une protection :

- Associez le profil de protection contre les vulnérabilités à une règle de politique de sécurité. Reportez-vous à la section Paramétrage des profils Antivirus, Antispyware et Protection contre les vulnérabilités.
- Installez les mises à jour du contenu qui renferment de nouvelles signatures pour vous protéger des menaces émergentes pour le pare-feu. Reportez-vous à la section Installer les mises à jour de contenu et logicielles

Personnalisation de l'action et des conditions de déclenchement de la signature d'une attaque par force brute

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

Le pare-feu contient deux types de signatures d'attaques par force brute : des signatures parent et des signatures enfant. Une signature enfant est l'occurrence unique d'un modèle de trafic correspondant à la signature. Une signature parent est associée à une signature enfant et se déclenche lorsque plusieurs événements se produisent au cours d'un intervalle de temps donné et correspondent au modèle de trafic défini dans la signature enfant.

En général, une signature enfant applique l'action *autoriser* par défaut, car un événement unique n'est pas révélateur d'une attaque. On s'assure ainsi que le trafic légitime n'est pas bloqué et que des journaux de menaces ne sont pas générés pour des événements anodins. Palo Alto Networks vous recommande de ne pas modifier l'action par défaut sans y avoir bien réfléchi.

En général, la signature d'une attaque par force brute est un événement notable en raison de son modèle récurrent. Au besoin, vous pouvez procéder de l'une des manières suivantes pour personnaliser l'action de la signature d'une attaque par force brute :

- Créez une règle pour modifier l'action par défaut de toutes les signatures de la catégorie Force brute. Vous pouvez choisir d'autoriser, d'alerter, de bloquer, de réinitialiser ou de supprimer le trafic.
- Définissez une exception pour une signature spécifique. Par exemple, vous pouvez rechercher des CVE et définir une exception pour ces derniers.

Pour une signature parent, les conditions de déclenchement et l'action peuvent être modifiées ; pour une signature enfant, seule l'action peut être modifiée.

Pour atténuer efficacement une attaque, spécifiez l'action bloquer-adresse ip plutôt que l'action « supprimer » ou « réinitialiser » pour la plupart des signatures d'attaques par force brute.

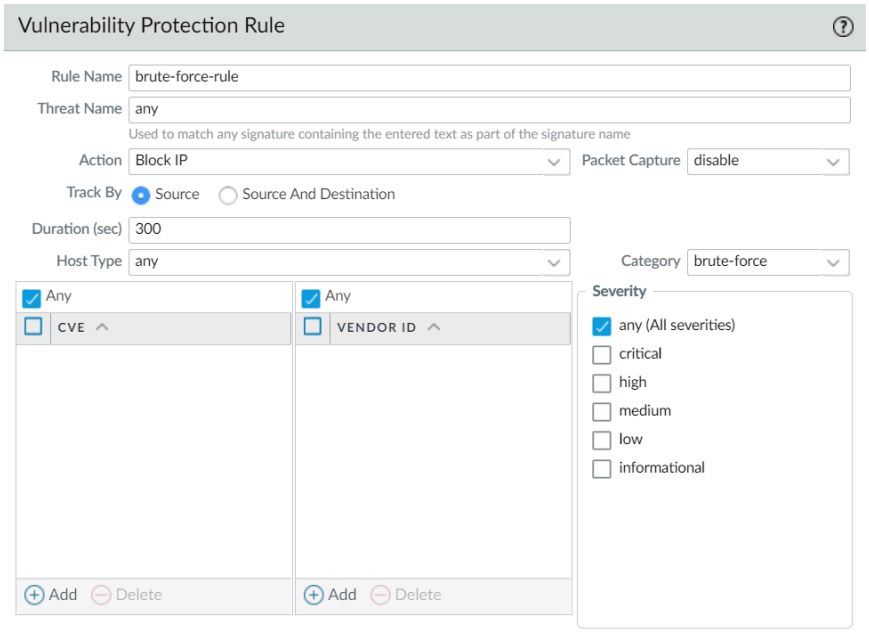
STEP 1 | Créez un nouveau profil de protection contre les vulnérabilités.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Vulnerability Protection (Protection contre les vulnérabilités)** et **Add (Ajoutez)** un profil.
2. Donnez un **Name (Nom)** au profil de protection contre les vulnérabilités.
3. (Facultatif) Saisissez une **Description (Description)**.
4. (Facultatif) Précisez si le profil est **Partagé** avec :
   - **Tous les systèmes virtuels (vsys) sur un pare-feu comportant plusieurs vsys** - S'il est effacé (désactivé), le profil est disponible uniquement dans le système virtuel sélectionné dans l'onglet **Objects (Objets)**.
   - **Tous les groupes de périphériques sur Panorama** - S'il est effacé (désactivé), le profil est disponible uniquement dans le groupe de périphériques sélectionné dans l'onglet **Objects (Objets)**.
5. (Facultatif—Panorama uniquement) Sélectionnez **Disable override (Désactiver le contrôle prioritaire)** pour empêcher les administrateurs de remplacer les paramètres de ce profil de protection contre les vulnérabilités dans les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres de tous les groupes de périphériques qui héritent du profil.

STEP 2 | Créez une règle qui définit l'action de toutes les signatures d'une catégorie.

1. À l'onglet **Rules (Règles)**, **Add (Ajoutez)** une nouvelle règle et donnez-lui un **Rule Name (Nom de règle)**.
2. (Facultatif) Indiquez un nom de menace particulier (**any (Indifférent)** est défini par défaut).
3. Définissez l'**Action (Action)**. Dans cet exemple, elle est définie sur **Block IP (Bloquer les adresses IP)**.

   Si vous définissez un profil de protection contre les vulnérabilités sur Block IP (Bloquer les adresses IP), le pare-feu se sert d'abord du matériel pour bloquer les adresses IP. Si le trafic d'attaque dépasse la capacité de blocage du matériel, le pare-feu utilise alors des mécanismes de blocage par logiciel pour bloquer les adresses IP restantes.
4. Définissez **Category (Catégorie)** sur **brute-force (force-brute)**.
5. (Facultatif) Si le blocage est sélectionné, précisez le **Host Type (Type d'hôte)** sur lequel effectuer le blocage : **server (serveur)** ou **client** (par défaut **any [indifférent]**).
6. Consultez l'étape 3 pour personnaliser l'action pour une signature spécifique.
7. Consultez l'étape 4 pour personnaliser le seuil de déclenchement pour une signature parent.



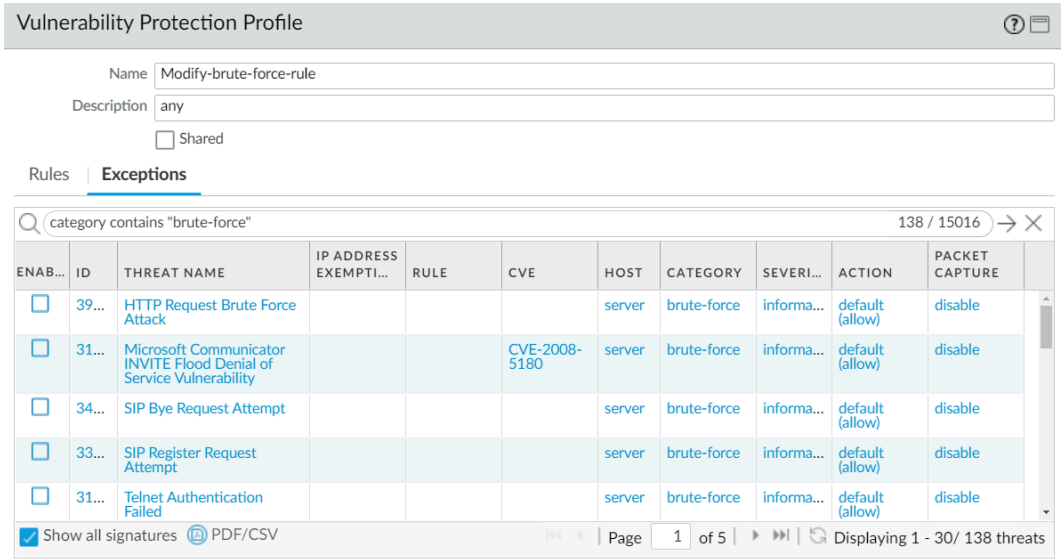
8. Cliquez sur **OK (OK)** pour enregistrer la règle et le profil.

STEP 3 | (Facultatif) Personnalisez l'action d'une signature spécifique.

1. À l'onglet **Exceptions (Exceptions)**, cliquez sur **Show all signatures (Afficher toutes les signatures)** pour trouver la signature que vous souhaitez modifier.

   Pour afficher toute les signatures dans la catégorie force-brute, recherchez `category contains 'brute-force'`.

2. Pour modifier une signature spécifique, cliquez sur l'action par défaut prédéfinie dans la colonne Action (Action).



3. Définissez l'action : **Allow (Autoriser)**, **Alert (Alerter)**, **Block Ip (Bloquer les adresses IP)** ou **Drop (Abandonner)**. Si vous sélectionnez **Block Ip (Bloquer les adresses IP)**, exécutez les tâches suivantes :

   1. Indiquez le **Time (Délai)** (en secondes) au bout duquel l'action sera déclenchée.
   2. Indiquez s'il faut **Track By (Suivre en fonction de)** et bloque l'adresse IP à l'aide de la **IP source (Adresse IP source)** ou de la **IP source and destination (Adresse IP source et de destination)**.

4. Cliquez sur **OK**.
5. Pour chaque signature modifiée, cochez la case dans la colonne **Enable (Activer)**.
6. Cliquez sur **OK**.

STEP 4 | Personnalisation des conditions de déclenchement d'une signature parent.

Une signature parent modifiable affiche cette icône : .

Dans cet exemple, les critères de recherche étaient la catégorie force-brute et CVE-2008-1447.

1. Modifiez ( ) l'attribut « Délai » et le critère d'agrégation de la signature.
2. Pour modifier le seuil de déclenchement, indiquez le **Number of Hits (Nombre d'accès)** par nombre de **seconds (secondes)**.
3. Indiquez si vous souhaitez agréger le nombre d'accès (**Aggregation Criteria (Critère d'agrégation)**) par **source (source)**, **destination (destination)** ou par **source-and-destination (source et destination)**.
4. Cliquez sur **OK**.

STEP 5 | Associez ce nouveau profil à une règle de politique de sécurité.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et **Add (ajoutez)** ou modifiez une règle de politique de sécurité.
2. À l'onglet **Actions (Actions)**, sélectionnez **Profiles (Profils)** en tant que **Profile Type (Type de profil)** du paramètre Profil.
3. Sélectionnez votre profil de **Vulnerability Protection (Protection contre les vulnérabilités)**.
4. Cliquez sur **OK**.

STEP 6 | Validez vos modifications.

1. Cliquez sur **Commit (Valider)**.

Activer les signatures d'évasion

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

Les signatures d'évasion Palo Alto Networks détectent des requêtes HTTPS ou TLS fabriquées et peuvent envoyer une alerte pour aviser des instances sur lesquelles un client se connecte à un domaine autre que celui qui est indiqué dans une requête DNS. Les signatures d'évasion sont en vigueur uniquement lorsque le pare-feu est également autorisé à agir en tant que proxy DMS et à résoudre des requêtes de noms de domaine. Il est recommandé de suivre les étapes suivantes pour activer les signatures d'évasion.

STEP 1 | Activez un pare-feu qui est intermédiaire des clients et serveurs pour qu'il agisse en tant que proxy DNS.

Configuration d'un objet proxy DNS, y compris :

- Précisez les interfaces sur lesquelles vous souhaitez que le pare-feu écoute les requêtes DNS.
- Définissez les serveurs DNS avec lesquels le pare-feu communique pour résoudre les requêtes DNS.
- Configurez des entrées FQDN à l'adresse IP statique que le pare-feu peut résoudre localement, sans avoir à contacter des serveurs DNS.
- Activez la mise en cache des mappages nom d'hôte/adresse IP résolus.

STEP 2 | Obtenez la version de contenu Applications et menaces la plus récente (au moins la version 579 ou toute version ultérieure).

1. Sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**.
2. Cliquez sur **Check Now (Vérifier maintenant)** pour télécharger les dernières mises à jour du contenu Applications et Menaces.
3. Téléchargez et installez la version du contenu Applications et Menaces 579 (ou version ultérieure).

STEP 3 | Définissez la manière dont le pare-feu devrait mettre appliquer le trafic mis en correspondance avec des signatures d'évasion.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware (Antispyware)** et **Add (Ajoutez)** ou modifiez un profil antispyware.
2. Sélectionnez **Exceptions (Exceptions)** et sélectionnez **Show all signatures (Afficher toutes les signatures)**.
3. Filtrez les signatures selon le mot-clé `evasion`.
4. Pour toutes les signatures d'évasion, définissez l'**Action (Action)** sur n'importe quel paramètre autre que l'action par défaut ou autoriser (l'action définie par défaut pour les

signatures d'évasion est Autoriser). Par exemple, définissez l'**Action (Action)** des ID de signature 14978 et 14984 sur **alert (alerter)** ou **drop (abandonner)**.

5. Cliquez sur **OK (OK)** pour enregistrer le profil antispyware mis à jour.
6. Associez le profil antispyware à une règle de politique de sécurité : Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis choisissez la politique que vous souhaitez modifier et cliquez sur l'onglet **Actions (Actions)**. Dans les Paramètres de profil, cliquez sur la liste déroulante en regard de **Anti-Spyware (Antispyware)** et sélectionnez le profil antispyware que vous venez de modifier pour appliquer les signatures d'évasion.

STEP 4 | Validez vos modifications.

Cliquez sur **Commit (Valider)**.

Créer des exceptions de menace

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

Palo Alto Networks définit une action recommandée par défaut (comme bloquer ou alerter) pour les signatures de menaces. Vous pouvez utiliser un ID de menace pour exclure une signature de menace de l'application ou pour modifier l'action appliquée pour cette signature de menace. Par exemple, vous pouvez modifier l'action relative aux signatures de menaces qui entraînent de faux positifs sur votre réseau.

Configurez les exceptions de menace des signatures antivirus, des signatures de vulnérabilités, des signatures antispyware et des signatures DNS pour changer l'action appliquée à une menace. Cependant, avant de commencer, assurez-vous que les menaces sont correctement détectées et appliquées en fonction des paramètres de signature par défaut ou des meilleures pratiques pour une posture de sécurité optimale :

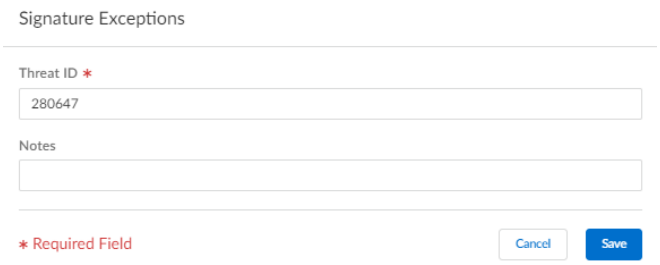
- Obtenez les dernières mises à jour des signatures antivirus, des menaces et applications et de WildFire (pour le pare-feu).
- Paramétrage des profils Antivirus, Antispyware et Protection contre les vulnérabilités et appliquez ces profils de sécurité à votre politique de sécurité.
- Strata Cloud Manager
- PAN-OS et Panorama

Créer des exceptions de menace (Strata Cloud Manager)

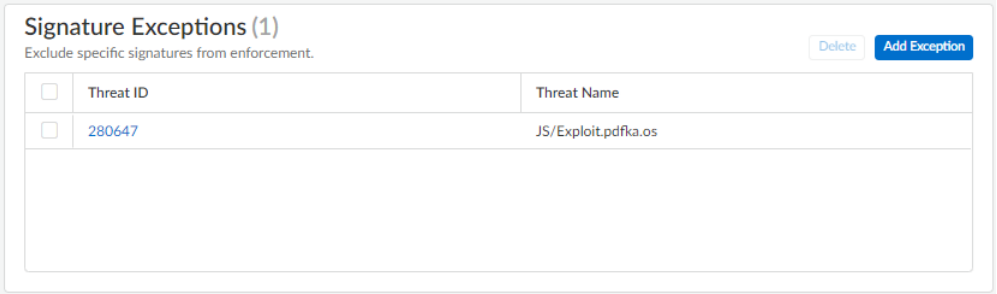
STEP 1 | Excluez les signatures antivirus de l'application.

Bien que vous puissiez utiliser un profil WildFire et Antivirus pour exclure des signatures antivirus de l'application, vous ne pouvez pas modifier l'action appliquée à une signature antivirus spécifiée. Toutefois, vous pouvez définir l'action applicable lorsque des virus sont détectés dans différents types de trafic en modifiant le profil de sécurité ***Enforcement Actions (Mesures d'application)****.*

1. Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **WildFire and Antivirus (WildFire et Antivirus)**.
2. **Add Profile (Ajouter un profil)** ou sélectionnez un profil WildFire et Antivirus existant dont vous souhaitez exclure une signature de menace et accédez à l'onglet **Advanced Settings (Paramètres avancés)**.
3. Depuis le menu **Signature Exceptions (Exceptions de signature)**, **Add Exception (Ajouter une exception)** et fournir le **Threat ID (ID de menace)** de la signature de menace que vous souhaitez exclure de l'application. Vous pouvez éventuellement ajouter des notes à l'exception de signature.



4. **Save (Enregistrer)** l'exception de signature lorsque vous avez terminé.
5. Un ID de signature de menace valide renseigne automatiquement le champ du nom de la menace. Vous pouvez afficher une liste complète des exceptions de signature actives ainsi que **Delete (Supprimer)** les entrées qui ne sont plus nécessaires.

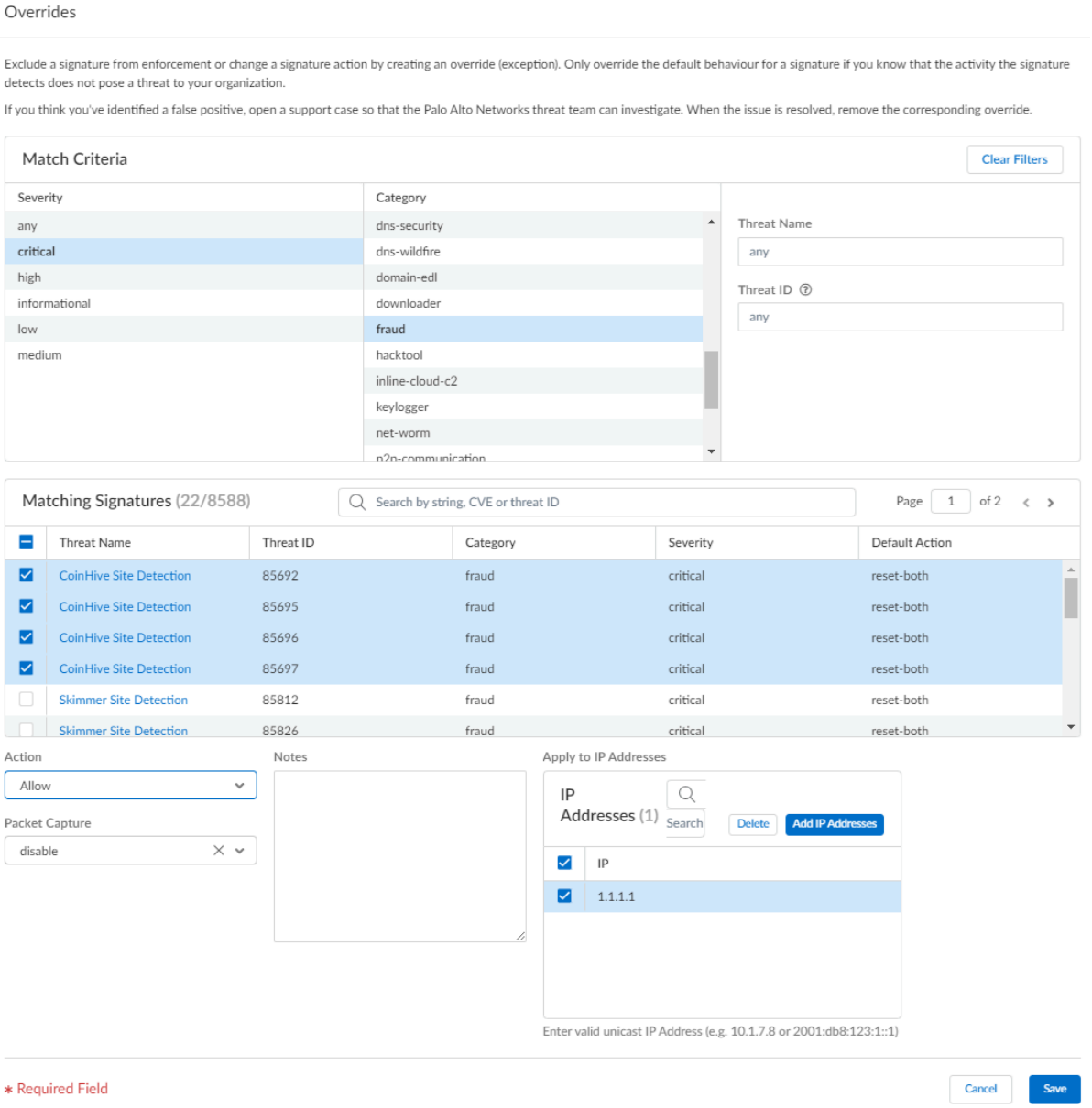


6. Répétez l'opération pour ajouter des exceptions supplémentaires ou cliquez sur **Save (Enregistrer)** après avoir ajouté toutes vos exceptions de menace.

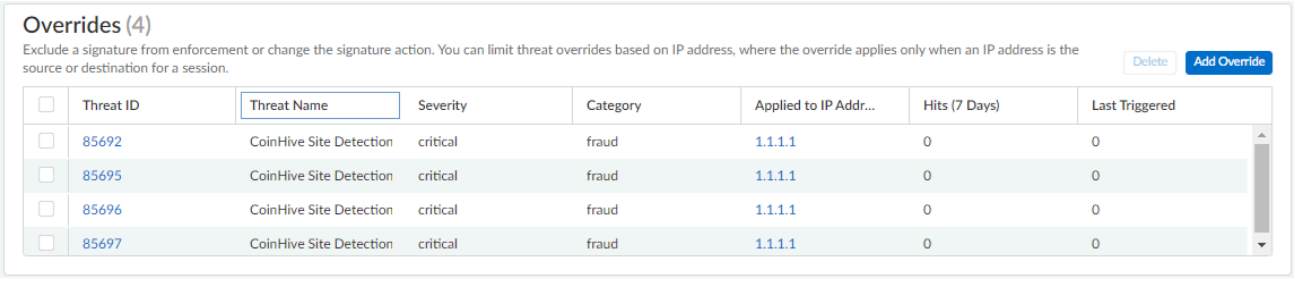
STEP 2 | Modifiez l'application des signatures de vulnérabilité et de logiciel espion (sauf les signatures DNS ; bien qu'il s'agisse d'un type de signature de logiciel espion, les signatures DNS sont gérées par le biais de l'abonnement à la sécurité DNS dans Prisma Access).

1. Sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Anti-Spyware (Antispyware)** ou **Manage (Gérer)** > **Configuration** > **NGFW et Prisma Access** > **Security Services (Services de sécurité)** > **Vulnerability Protection (Protection contre les vulnérabilités)**, selon le type de signature.
2. **Add Profile (Ajouter un profil)** ou sélectionnez un profil anti-spyware ou de protection contre les vulnérabilités existant à partir duquel vous souhaitez modifier l'application de la signature, puis sélectionnez **Add Override (Ajouter un contrôle prioritaire)**.
3. Recherchez des signatures de logiciels espions ou de vulnérabilités en fournissant les **Match Criteria (Critères de correspondance)** pertinents. Cela filtre automatiquement les signatures disponibles et affiche les résultats dans la section **Matching signatures (Signatures correspondantes)**.
4. Cochez la case de la ou des signatures dont vous souhaitez modifier l'application.

5. Fournissez l'**Action**, la **Packet capture (Capture de paquet)**et les **IP adresses (Adresses IP)** auxquelles vous souhaitez que les règles d'application modifiées s'appliquent pour les signatures sélectionnées.



6. **Save (Enregistrer)** votre configuration mise à jour de l'application des signatures.
7. Vous pouvez consulter une liste complète d'**Overrides (Contrôles prioritaires)**, y compris diverses statistiques, et **Delete (Supprimer)** les entrées qui ne sont plus nécessaires.

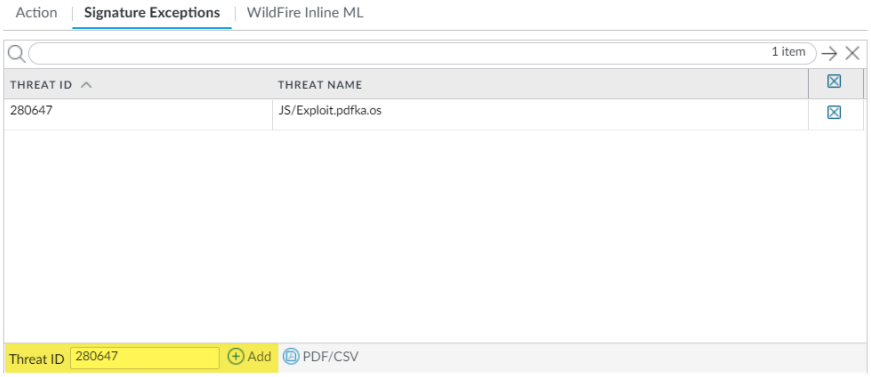


Créer des exceptions de menace (NGFW (Managed by PAN-OS or Panorama))

STEP 1 | Excluez les signatures antivirus de l'application.

*Bien que vous puissiez utiliser un profil antivirus pour exclure des signatures antivirus de l'application, vous ne pouvez modifier l'action que le pare-feu applique relativement à une signature antivirus donnée. Vous pouvez toutefois définir l'action que le pare-feu doit appliquer sur les virus détectés dans divers types de trafic en modifiant les décodeurs (**Objects (Objets)** > **Security Profiles (profils de sécurité)** > **Antivirus (Antivirus)** > **<antivirus-profile>** >**Antivirus**).*

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Antivirus (Antivirus)**.
2. **Add (Ajoutez)** ou modifiez un profil antivirus existant duquel vous souhaitez exclure une signature de menace, puis sélectionnez **Signature Exception (Exception de signature)**.
3. **Add (Ajoutez)** le **Threat ID (ID de menace)** de la signature de menaces que vous souhaitez exclure de l'application.

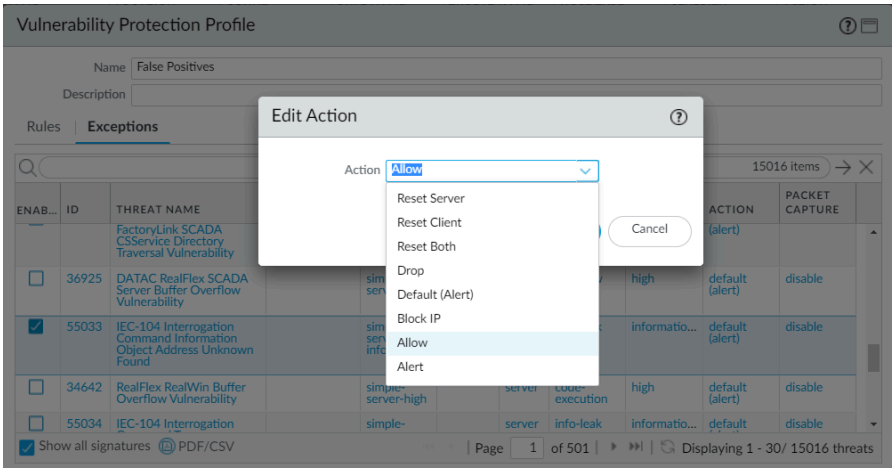


4. Cliquez sur **OK (OK)** pour enregistrer le profil antivirus.

STEP 2 | Modifiez l'application des signatures de protection contre les logiciels malveillants ou contre les vulnérabilités (à l'exception des signatures DNS ; passez à l'option suivante pour modifier l'application des signatures DNS, qui sont un type de signature antispyware).

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware (Antispyware)** ou **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Vulnerability Protection (Protection contre les vulnérabilités)**.
2. **Add (Ajoutez)** ou modifiez un profil antispyware ou de protection contre les vulnérabilités existant duquel vous souhaitez exclure la signature de menace, puis sélectionnez **Signature Exceptions (Exceptions de signature)** pour les profils de protection antispyware ou **Exceptions** pour les profils de protection contre les vulnérabilités.
3. **Show all signatures (Affichez toutes les signatures)**, puis appliquer un filtre pour sélectionner la signature dont vous souhaitez modifier les règles d'application.
4. Cochez la case qui se situe sous la colonne **Enable (Activer)** correspondant à la signature dont vous souhaitez modifier l'application.

5. Sélectionnez l'**Action (Action)** que vous souhaitez que le pare-feu applique relativement à cette signature de menaces.



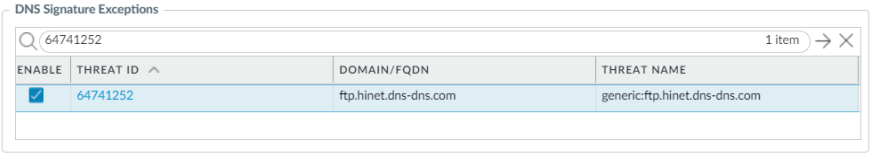
   Dans le cas des signatures que vous souhaitez exclure de l'application parce qu'elles produisent des faux positifs, définissez l'**Action (Action)** sur **Allow (Autoriser)**.

6. Cliquez sur **OK (OK)** pour enregistrer votre profil antispyware ou votre profil de protection contre les vulnérabilités, qu'il soit nouveau ou modifié.

STEP 3 | Modifiez l'application des signatures DNS.

Par défaut, les recherches DNS vers des noms d'hôte malveillants qui contiennent des signatures DNS sont détectées et mises en entonnoir.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware (Antispyware)**.
2. **Add (Ajoutez)** ou modifiez le profil antispyware duquel vous souhaitez exclure la signature de menaces, puis sélectionnez **DNS Exceptions (Exceptions de DNS)**.
3. Recherchez l'ID de menace DNS pour la signature de DNS que vous souhaitez exclure de l'application et cochez la case de la signature applicable :



4. Cliquez sur **OK (OK)** pour enregistrer votre profil antispyware, qu'il soit nouveau ou modifié.

Utilisation de requêtes DNS pour identifier des hôtes infectés sur le réseau

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

L'action de mise en entonnoir DNS des profils Antispyware permet au pare-feu de falsifier une réponse à une requête DNS d'un domaine malveillant connu, ou un domaine personnalisé pour que vous puissiez identifier les hôtes sur votre réseau qui ont été infectés par le logiciel malveillant. Un hôte compromis peut initier la communication avec un serveur de commande et contrôle (C2). Une fois la connexion établie, un pirate peut contrôler à distance l'hôte infecté afin d'infiltrer davantage le réseau ou d'exfiltrer les données.

Les requêtes DNS vers n'importe quel domaine inclus dans la liste de signatures DNS de Palo Alto Networks sont mises en entonnoir vers une adresse IP de serveur Palo Alto Networks.

Le pare-feu possède deux sources de signatures DNS qu'il peut utiliser pour identifier les domaines malveillants et C2 :

- (Exige un abonnement Advanced | Threat Prevention) Signatures DNS locales : il s'agit d'un ensemble intégré restreint de signatures DNS pouvant être utilisé par le pare-feu pour identifier les domaines malveillants. Le pare-feu obtient de nouvelles signatures DNS dans le cadre des mises à jour antivirus quotidiennes.
- (Exige un abonnement à la sécurité DNS) Signatures de sécurité DNS : le pare-feu accède au service cloud de la sécurité DNS de Palo Alto Networks pour rechercher des domaines malveillants en les comparant à la base de données complète des signatures DNS. Certaines signatures (que seule la sécurité DNS fournit) peuvent uniquement détecter les attaques C2 qui utilisent les techniques d'apprentissage machine, comme les Domain Generation Algorithms (algorithmes de génération de domaines ; DGA) et la tunnellisation DNS. Pour plus d'informations sur l'abonnement à la sécurité DNS, reportez-vous au guide sur la sécurité DNS.

  Si vous souhaitez spécifier une action d'entonnoir pour les signatures de la sécurité DNS, vous pouvez configurer ces paramètres dans le cadre de votre profil de sécurité DNS.

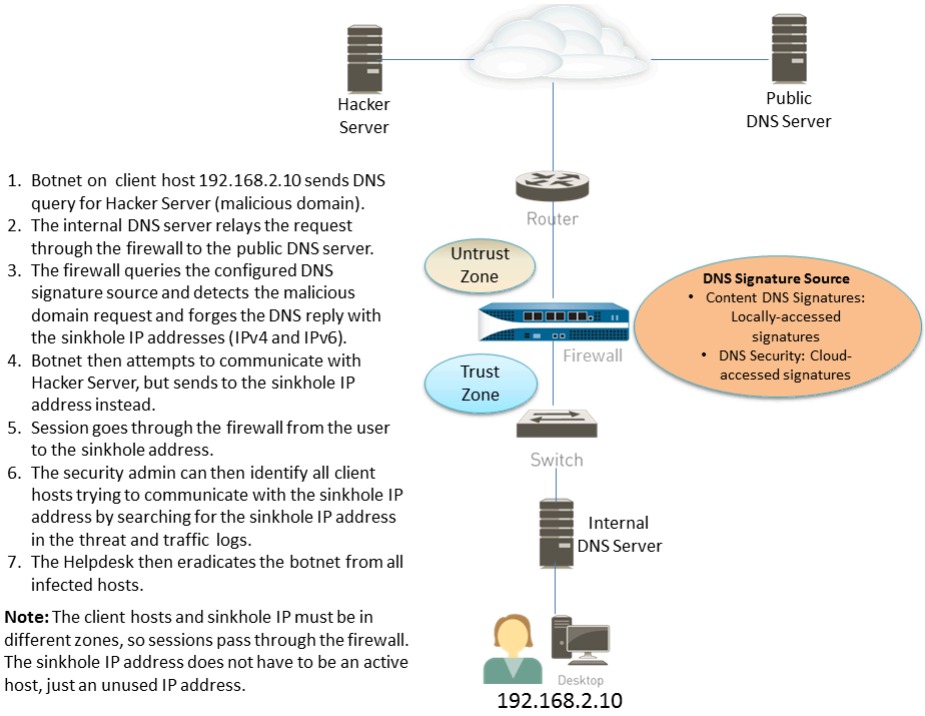
Les requêtes DNS aux domaines dans l'ensemble de signatures DNS local ou l'ensemble de signatures de sécurité DNS sont redirigées vers un serveur Palo Alto Networks, et l'hôte est incapable d'accéder au domaine malveillant. Les rubriques suivantes fournissent des détails sur l'activation de la mise en entonnoir DNS pour que vous puissiez identifier les hôtes infectés.

- Fonctionnement de la mise en entonnoir DNS
- Configuration de la mise en entonnoir DNS
- Configuration de la mise en entonnoir DNS pour une liste de domaines personnalisée
- Configuration de l'adresse IP entonnoir vers un serveur local sur votre réseau
- Voir les hôtes infectés qui ont tenté de se connecter à un domaine malveillant

Fonctionnement de la mise en entonnoir DNS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

La mise en entonnoir DNS vous permet d'identifier les hôtes infectés sur le réseau protégé utilisant le trafic DNS dans les cas où le pare-feu ne peut pas voir la requête DNS du client infecté (c'est-à-dire que le pare-feu ne peut pas voir l'auteur de la requête DNS). Dans un déploiement type où le pare-feu est au nord du serveur DNS local, le journal des menaces identifie le résolveur DNS local comme la source du trafic plutôt que l'hôte réellement infecté. La mise en entonnoir des requêtes DNS malveillantes résout ce problème de visibilité en falsifiant les réponses aux requêtes d'un hôte client adressées à des domaines malveillants, ainsi les clients tentant de se connecter à des domaines malveillants (pour la commande et le contrôle, par exemple) essaieront plutôt de se connecter à une adresse IP d'entonnoir par défaut de Palo Alto Networks (ou à une adresse IP que vous définissez si vous choisissez de procéder à la Configuration de la mise en entonnoir DNS pour une liste de domaines personnalisée). Les hôtes infectés peuvent alors être facilement identifiés dans les journaux du trafic.



Configuration de la mise en entonnoir DNS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

Pour activer l'entonnoir DNS, attachez le profil antispyware par défaut à une règle de politique de sécurité du pare-feu (se reporter Paramétrage des profils Antivirus, Antispyware et Protection contre les vulnérabilités). Les requêtes DNS envoyées à tout domaine compris dans la source de signatures DNS de Palo Alto Networks que vous avez spécifié sont résolues en adresse IP entonnoir Palo Alto Networks. À l'heure actuelle, les adresses IP sont les suivantes : sinkhole.paloaltonetworks.com pour IPv4 et ::1 pour l'adresse IPv6 en boucle. Ces adresse peuvent changer et peuvent être modifiées dans les mises à jour de contenu.

STEP 1 | Activez la mise en entonnoir DNS pour la liste de domaines personnalisée d'une liste dynamique externe.

1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware (Antispyware)**.
2. Modifiez un profil existant ou sélectionnez un des profils par défaut et clonez-le.
3. Donnez un **Name (Nom)** au profil, puis sélectionnez l'onglet **DNS Policies (Politiques de DNS)**.
4. Vérifiez que **default-paloalto-dns** est présent dans la **Signature Source (Source de signature)**.
5. (Facultatif) Dans la liste déroulante **Packet Capture (Capture de paquets)**, sélectionnez **single-packet (un seul paquet)** pour capturer le premier paquet de la session ou **extended-capture (capture étendue)** pour définir de 1 à 50 paquets. Vous pouvez ensuite utiliser les captures de paquets pour une analyse plus approfondie.

STEP 2 | Vérifiez les paramètres de mise en entonnoir sur le profil antispyware.

1. Sur l'onglet **DNS Policies (Politiques de DNS)**, vérifiez que **Policy Action** on DNS Queries (Action de politique pour les requêtes DNS) est définie sur **sinkhole (entonnoir)**.
2. À la section DNS Sinkhole Settings (Paramètres de mise en entonnoir DNS), vérifiez que l'option **Sinkhole (Entonnoir)** est activée. Pour votre facilité, l'adresse IP entonnoir par défaut est définie sur un serveur de Palo Alto Networks. Palo Alto Networks peut automatiquement actualiser cette adresse IP par l'intermédiaire de mises à jour de contenu.

   Si vous souhaitez modifier l'adresse **Sinkhole IPv4 (IPv4 d'entonnoir)** ou **Sinkhole IPv6 (IPv6 d'entonnoir)** vers un serveur local sur votre réseau ou vers une adresse de boucle, reportez-vous à la section Configuration de l'adresse IP entonnoir vers un serveur local sur votre réseau.
3. Cliquez sur **OK (OK)** pour enregistrer le profil antispyware.

STEP 3 | Associez le profil antispyware à une règle de politique de sécurité.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis sélectionnez une règle de politique de sécurité.
2. Dans l'onglet **Actions (Actions)**, cochez la case **Log at Session Start (Journalisation en début de session)** pour activer la journalisation.
3. Dans la section Paramètre de profil, cliquez sur la liste déroulante **Profile Type (Type de profil)** pour voir tous les **Profiles (Profils)**. Sélectionnez le nouveau profil dans la liste déroulante **Anti-spyware (Antispyware)**.
4. Cliquez sur **OK (OK)** pour enregistrer la règle de politique.

STEP 4 | Testez que l'action de la politique est appliquée en surveillant l'activité sur le pare-feu.

1. Sélectionnez **ACC (ACC)** et ajoutez un domaine d'URL en tant que filtre général pour afficher l'activité des menaces et l'activité bloquée pour le domaine auquel vous avez accédé.
2. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menace)** et filtrez par `(action eq sinkhole)` pour afficher les journaux des domaines mis en entonnoir.

Configuration de la mise en entonnoir DNS pour une liste de domaines personnalisée

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

Pour activer la mise en entonnoir DNS pour une liste de domaines personnalisée, vous devez créer une liste dynamique externe qui englobe les domaines, autoriser l'action de mise en entonnoir dans un profil antispyware et associer le profil à une règle de politique de sécurité. Lorsqu'un client tente d'accéder à un domaine malveillant qui figure dans cette liste, le pare-feu remplace l'adresse IP de destination du paquet par l'adresse IP du serveur Palo Alto Networks définie par défaut pour la mise en entonnoir ou par celle définie par un utilisateur.

Pour chaque nom de domaine personnalisé qui est inclus dans la liste dynamique externe, le pare-feu génère des signatures de logiciel espion basées sur DNS. La signature se nomme Requête DNS malveillante personnalisée <domain name> et correspond à un type de spyware de niveau de gravité moyen ; chaque signature est un hachage 24 octets du nom de domaine.

Pour plus d'informations sur les limites d'entrée de la liste de domaines, reportez-vous à Liste dynamique externe.

STEP 1 | Activez la mise en entonnoir DNS pour la liste de domaines personnalisée d'une liste dynamique externe.

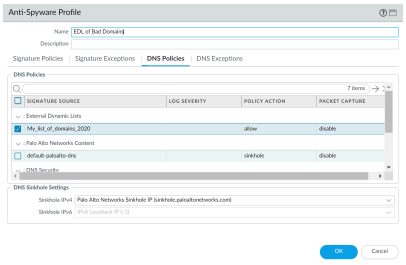
1. Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware (Antispyware)**.
2. Modifiez un profil existant ou sélectionnez un des profils par défaut et clonez-le.
3. Donnez un **Name (Nom)** au profil, puis sélectionnez l'onglet **DNS Policies (Politiques de DNS)**.
4. Sélectionnez un EDL à partir de la source de signature **External Dynamic Lists (Listes dynamiques externes)**.

   *Si vous avez déjà créé une liste dynamique externe de type : **Domain List (Liste de domaines)**, vous pouvez la sélectionnez ici. Les listes dynamiques externes de type URL ou Adresse IP que vous pourriez avoir créées ne figurent pas dans la liste.*
5. Configurez la liste dynamique externe à partir du profile antispyware (reportez-vous à la section Configuration du pare-feu pour qu'il accède à une liste dynamique externe). Le **Type (Type)** est prédéfini sur **Domain List (Liste de domaines)**.
6. (Facultatif) Dans la liste déroulante **Packet Capture (Capture de paquets)**, sélectionnez **single-packet (un seul paquet)** pour capturer le premier paquet de la session ou **extended-capture (capture étendue)** pour définir de 1 à 50 paquets. Vous pouvez ensuite utiliser les captures de paquets pour une analyse plus approfondie.

STEP 2 | Vérifiez les paramètres de mise en entonnoir sur le profil antispyware.

1. Sur l'onglet **DNS Policies (Politiques de DNS)**, vérifiez que **Policy Action** on DNS Queries (Action de politique pour les requêtes DNS) est définie sur **sinkhole (entonnoir)**.
2. À la section DNS Sinkhole Settings (Paramètres de mise en entonnoir DNS), vérifiez que l'option **Sinkhole (Entonnoir)** est activée. Pour votre facilité, l'adresse IP entonnoir par défaut est définie sur un serveur de Palo Alto Networks. Palo Alto Networks peut automatiquement actualiser cette adresse IP par l'intermédiaire de mises à jour de contenu.

   Si vous souhaitez modifier l'adresse **Sinkhole IPv4 (IPv4 d'entonnoir)** ou **Sinkhole IPv6 (IPv6 d'entonnoir)** vers un serveur local sur votre réseau ou vers une adresse de boucle, reportez-vous à la section Configuration de l'adresse IP entonnoir vers un serveur local sur votre réseau.



3. Cliquez sur **OK (OK)** pour enregistrer le profil antispyware.

STEP 3 | Associez le profil antispyware à une règle de politique de sécurité.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis sélectionnez une règle de politique de sécurité.
2. Dans l'onglet **Actions (Actions)**, cochez la case **Log at Session Start (Journalisation en début de session)** pour activer la journalisation.
3. Dans la section Paramètre de profil, cliquez sur la liste déroulante **Profile Type (Type de profil)** pour voir tous les **Profiles (Profils)**. Sélectionnez le nouveau profil dans la liste déroulante **Anti-spyware (Antispyware)**.
4. Cliquez sur **OK (OK)** pour enregistrer la règle de politique.

STEP 4 | Vérifiez que l'action de politique est appliquée.

1. Afficher les entrées de la liste dynamique externe qui appartiennent à la liste de domaine et accédez à un domaine de la liste.
2. Pour surveiller l'activité sur le pare-feu :
   1. Sélectionnez **ACC (ACC)** et ajoutez un domaine d'URL en tant que filtre général pour afficher l'activité des menaces et l'activité bloquée pour le domaine auquel vous avez accédé.
   2. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menace)** et filtrez par `(action eq sinkhole)` pour afficher les journaux des domaines mis en entonnoir.

STEP 5 | Vérifiez si des entrées de la liste dynamique externe sont ignorées ou sautées.

Pour revoir les détails de la liste, servez-vous de la commande CLI suivante sur le pare-feu :

```
système de requête liste externe type d'affichage nom de
 domaine <list_name>
```

Par exemple :

```
request system external-list show type domain name
 My_List_of_Domains_2015 vsys1/EBLDomain: Prochaine mise à
 jour le : Jeu 21 Mai 10:15:39 2015 Source : https://1.2.3.4/
My_List_of_Domains_2015 Référencé : Oui Valide : Oui Nombre
 d'entrées : 3 domaines : www.example.com baddomain.com
 qqq.abcedfg.com
```

STEP 6 | (Facultatif) Récupérez la liste dynamique externe à la demande.

Pour forcer le pare-feu à récupérer la liste actualisée à la demande plutôt qu'au prochain intervalle d'actualisation (la fréquence de **Repeat (Répétition)** que vous avez définie pour la liste dynamique externe), servez-vous de la commande CLI suivante :

```
système de demande de type d'actualisation de la liste externe nom
 de domaine  <list_name>
```

Vous pouvez également utiliser l'interface du pare-feu pour la récupération d'une liste dynamique externe du serveur Web.

Configuration de l'adresse IP entonnoir vers un serveur local sur votre réseau

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

Par défaut, la mise en entonnoir DNS est activée pour toutes les signatures DNS de Palo Alto Networks, et l'adresse IP entonnoir est définie pour permettre l'accès à un serveur de Palo Alto Networks. Servez-vous des directives présentées dans cette section si vous souhaitez définir l'adresse IP entonnoir sur un serveur local de votre réseau.

Vous devez obtenir des adresses IPv4 et IPv6, qui serviront d'adresses IP entonnoir, car un logiciel malveillant peut exécuter des requêtes DNS via un de ces protocoles, ou les deux. L'adresse d'entonnoir DNS doit se trouver dans une zone différente des hôtes clients pour s'assurer, lorsqu'un hôte infecté tente d'ouvrir une session avec l'adresse IP d'entonnoir, qu'il sera acheminé via le pare-feu.

Les adresses d'entonnoir doivent être réservées à cet effet et ne doivent pas nécessairement être associées à un hôte physique. Vous pouvez éventuellement utiliser un serveur « pot de miel » comme hôte physique pour analyser le trafic malveillant de manière plus approfondie.

Les étapes de configuration qui suivent utilisent les exemples d'adresses d'entonnoir DNS suivantes :

Adresse d'entonnoir DNS IPv4 : 10.15.0.20

Adresse d'entonnoir DNS IPv6 : fd97:3dec:4d27:e37c:5:5:5:5

STEP 1 | Configurez l'interface et la zone de l'entonnoir.

Le trafic provenant de la zone sur laquelle les hôtes clients résident doit être acheminé vers la zone sur laquelle l'adresse IP d'entonnoir est définie. Le trafic sera ainsi consigné.

Utilisez une zone dédiée pour le trafic d'entonnoir car l'hôte infecté enverra du trafic à cette zone.

1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)**, puis choisissez l'interface que vous souhaitez configurer comme votre interface d'entonnoir.
2. Dans la liste déroulante **Interface Type (Type d'interface)**, sélectionnez **Layer3 (Couche 3)**.
3. Pour ajouter une adresse IPv4, sélectionnez l'onglet **IPv4 (IPv4)**, sélectionnez **Static (Statique)**, puis cliquez sur **Add (Ajouter)**. Dans cet exemple, ajoutez 10.15.0.20 comme adresse d'entonnoir DNS IPv4.

4. Sélectionnez l'onglet **IPv6 (IPv6)**, cliquez sur **Static (Statique)**, puis sur **Add (Ajouter)** et saisissez une adresse IPv6 et un masque de sous-réseau. Dans cet exemple, saisissez fd97:3dec:4d27:e37c::/64 comme adresse d'entonnoir DNS IPv6.
5. Cliquez sur **OK (OK)** pour enregistrer les paramètres.
6. Pour ajouter une zone pour l'entonnoir, sélectionnez **Network (Réseau)** > **Zones (Zones)**, puis cliquez sur **Add (Ajouter)**.
7. Saisissez un **Name (Nom)** de zone.
8. Dans la liste déroulante **Type (Type)**, sélectionnez **Layer3 (Couche 3)**.
9. Dans la section **Interfaces (Interfaces)**, cliquez sur **Add (Ajouter)** et ajoutez l'interface que vous venez de configurer.
10. Cliquez sur **OK**.

STEP 2 | Activation de la mise en entonnoir DNS

Par défaut, la mise en entonnoir est activée pour toutes les signatures DNS Palo Alto Networks. Pour modifier l'adresse de l'entonnoir sur votre serveur local, reportez-vous à l'étape 2 dans Configurer la mise en entonnoir DNS pour une liste de domaines personnalisés.

STEP 3 | Modifiez la règle de sécurité autorisant le trafic des hôtes clients de la zone approuvée vers la zone non approuvée afin d'inclure la zone d'entonnoir en tant que destination et d'associer le profil antispyware.

La modification de la ou des règles de politique de sécurité qui autorisent le trafic des hôtes clients de la zone approuvée vers la zone non approuvée vous permet de vous assurer que vous identifiez le trafic provenant d'hôtes infectés. L'ajout à la règle de la zone d'entonnoir en tant que destination permet aux clients infectés d'envoyer de fausses requêtes DNS à l'entonnoir DNS.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**.
2. Sélectionnez une règle existante qui autorise le trafic de la zone de l'hôte client vers la zone non approuvée.
3. Dans l'onglet **Destination (Destination)**, **Add (Ajoutez)** la zone d'entonnoir. Le trafic de l'hôte client peut ainsi être acheminé vers la zone d'entonnoir.
4. Dans l'onglet **Actions (Actions)**, cochez la case **Log at Session Start (Journalisation en début de session)** pour activer la journalisation. Ceci garantit que le trafic provenant d'hôtes clients de la zone approuvée sera consigné lors de l'accès à la zone non approuvée ou d'entonnoir.
5. Dans la section **Profile Setting (Paramètre de profil)**, sélectionnez le profil **Anti-Spyware (Antispyware)** dans lequel vous avez activé la mise en entonnoir DNS.
6. Cliquez sur **OK (OK)** pour enregistrer la règle de politique de sécurité, puis sur **Commit (Valider)**.

STEP 4 | Pour confirmer que vous allez pouvoir identifier les hôtes infectés, vérifiez que le trafic entre l'hôte client de la zone approuvée vers la nouvelle zone d'entonnoir est consigné.

Dans cet exemple, l'hôte client infecté est 192.168.2.10 et l'adresse d'entonnoir IPv4 est 10.15.0.20.

1. Sur un hôte client de la zone approuvée, ouvrez une invite de commande et exécutez la commande suivante :

   ```
   C:\>ping <sinkhole address>
   ```

   L'exemple suivant indique la requête ping sur l'adresse d'entonnoir DNS 10.15.0.2 et le résultat `Request timed out` car l'adresse IP d'entonnoir n'est pas associée à un hôte physique :

   ```
   C:\>ping 10.15.0.20 Ping 10.15.0.20 avec 32 octets de
    données : La demande a expiré. La demande a expiré.
    Statistiques de ping pour 10.15.0.20 : Packets: Envoyé = 4,
    Reçu = 0, Perdu = 4 (perte de 100 %)
   ```

2. Sur le pare-feu, sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)** et recherchez l'entrée de log avec la source 192.168.2.10 et la destination 10.15.0.20. Ceci confirme que le trafic vers l'adresse IP d'entonnoir passe par les zones du pare-feu.

   *Vous pouvez rechercher et/ou filtrer les journaux et n'afficher que les journaux avec la destination 10.15.0.20. Pour cela, cliquez sur l'adresse IP (10.15.0.20) dans la colonne **Destination (Destination)**. Le filtre (addr.dst in 10.15.0.20) est ainsi ajouté au champ de recherche. Cliquez sur l'icône Appliquer un filtre à droite du champ de recherche pour appliquer le filtre.*

STEP 5 | Testez que la mise en entonnoir DNS est bien configurée.

Vous simulez l'action que poserait un client infecté lorsqu'une application malveillante tente de contacter sa base.

1. Trouvez un domaine malveillant qui figure dans la base de données de signatures antivirus actuelle du pare-feu pour tester la mise en entonnoir.

   1. Sélectionnez **Device (Périphérique)** > **Dynamic (Dynamique) Updates (Mises à jour dynamiques)**, puis, dans la section **Antivirus (Antivirus)**, cliquez sur le lien **Release Notes (Notes de publication)** de la base de données antivirus installée. Vous pouvez également trouver les notes de version antivirus qui indiquent les mises à jour incrémentielles des signatures, à la section Mises à jour dynamiques du site de support Palo Alto Networks.
   2. Dans la deuxième colonne de la note de version, recherchez un élément de ligne avec une extension de domaine (par exemple, .com, .edu ou .net). La colonne de gauche indique le nom du domaine. Par exemple, dans la version Antivirus 1117-1560, un

élément dans la colonne de gauche est nommé « tbsbana » et la colonne de droite indique « net ».

La chaîne suivante correspond au contenu de cet élément de ligne dans la note de version :

```
conficker:tbsbana 1 variants: net
```

2. Sur l'hôte client, ouvrez une invite de commande.
3. Exécutez une commande NSLOOKUP sur une URL que vous avez identifiée comme un domaine malveillant.

   Par exemple, avec l'URL `track.bidtrk.com` :

```
C:\>nslookup track.bidtrk.com Server: my-local-
dns.local Address: 10.0.0.222 Réponse ne faisant pas
 autorité : Nom : track.bidtrk.com.org Adresses :
 fd97:3dec:4d27:e37c:5:5:5:510.15.0.20
```

   Notez, dans le résultat, que la commande NSLOOKUP sur le domaine malveillant a été falsifiée à l'aide des adresses IP d'entonnoir que nous avons configurées (10.15.0.20). Le domaine correspondant à une signature DNS malveillante, l'action d'entonnoir a été exécutée.
4. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menace)** et recherchez l'entrée du journal des menaces correspondante pour vérifier que l'action appropriée a été exécutée sur la requête NSLOOKUP.
5. Exécutez une commande ping sur **`track.bidtrk.com`**, ce qui générera du trafic réseau vers l'adresse d'entonnoir.

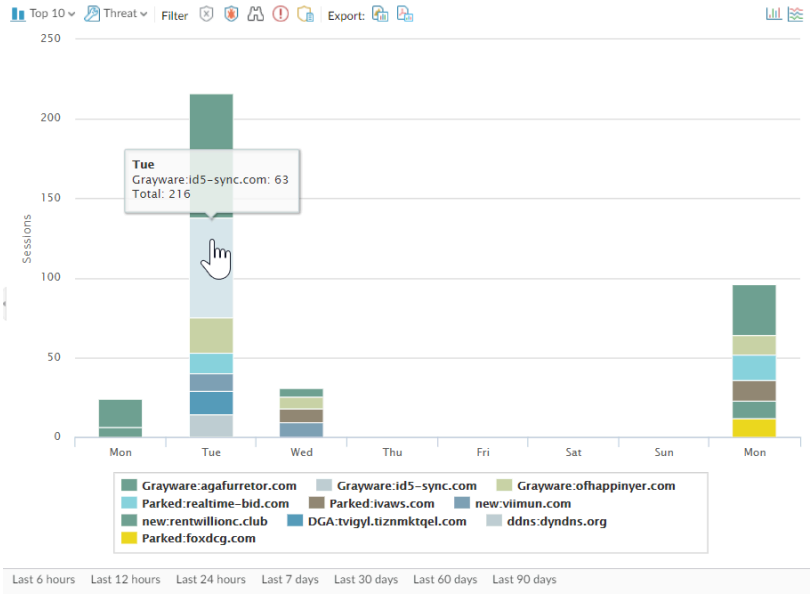
Voir les hôtes infectés qui ont tenté de se connecter à un domaine malveillant

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

Après avoir configuré la mise en entonnoir DNS et vérifié que le trafic vers un domaine malveillant est transmis à l'adresse d'entonnoir, vous devez surveiller régulièrement le trafic vers l'adresse d'entonnoir afin de pouvoir suivre les hôtes infectés et de supprimer les menaces.

- Utilisez App Scope pour identifier les hôtes clients infectés.
  1. Sélectionnez **Monitor (Surveillance)** > **App Scope (App Scope)**, puis **Threat Monitor (Surveillance des menaces)**.
  2. Cliquez sur le bouton **Show spyware (Afficher les logiciels espions)** en haut de la page affichée.
  3. Sélectionnez une plage horaire.

     La capture d'écran ci-dessous illustre trois instances de requêtes DNS suspectes qui ont été générées alors que l'hôte client de test exécutait une commande NSLOOKUP sur un domaine malveillant connu. Cliquez sur le graphique pour plus de détails sur l'événement.



- Configurez un rapport personnalisé afin d'identifier tous les hôtes clients qui ont envoyé du trafic à l'adresse IP d'entonnoir, 10.15.0.20 dans cet exemple.

  Transférez-le à un gestionnaire SNMP, un serveur Syslog et/ou à Panorama pour activer des alertes sur ces événements.

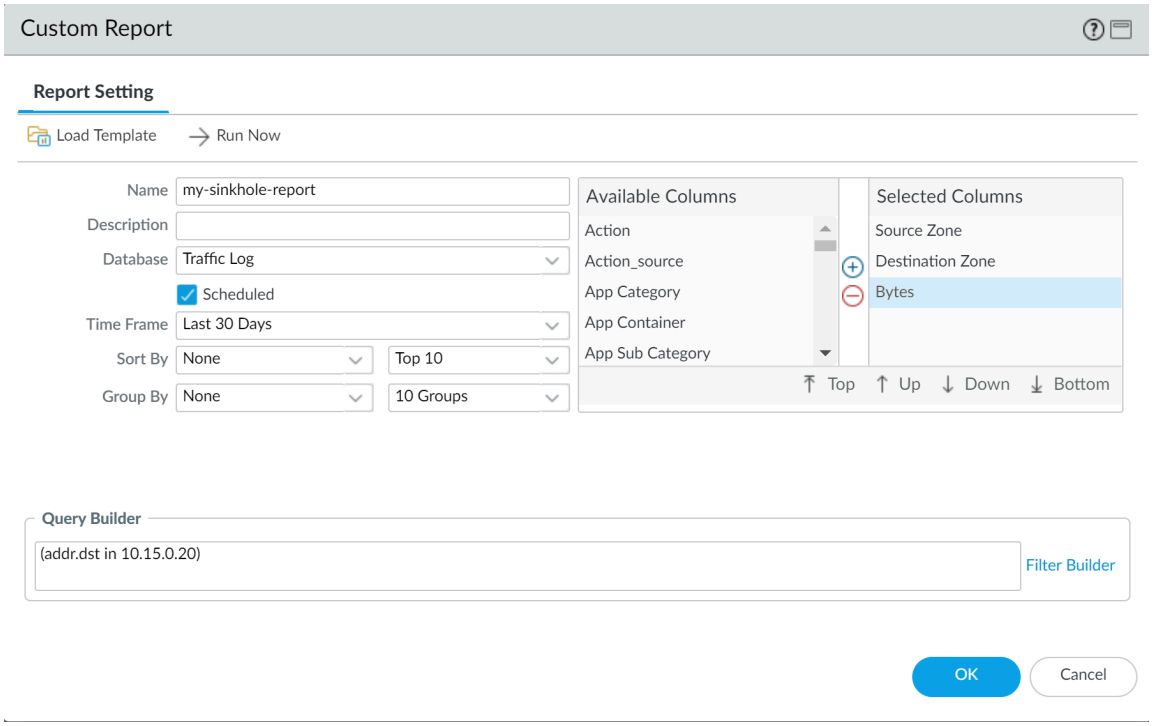
  Dans cet exemple, l'hôte client infecté exécutait une commande NSLOOKUP sur un domaine malveillant connu et répertorié dans la base de données de signatures DNS Palo Alto Networks. La requête a été envoyée au serveur DNS local, qui l'a ensuite transféré via le pare-feu à un serveur DNS externe. La politique de sécurité du pare-feu et le profil antispyware configuré ont comparé la requête avec la base de données de signatures DNS, puis falsifié la réponse avec l'adresse d'entonnoir 10.15.0.20 et fd97:3dec:4d27:e37c:5:5:5:5. Le client tente d'ouvrir une session et le journal du trafic enregistre l'activité avec l'hôte source et l'adresse de destination, qui est désormais redirigée vers l'adresse d'entonnoir falsifiée.

  Consultez le journal du trafic sur le pare-feu pour identifier tout hôte client qui envoie du trafic vers l'adresse d'entonnoir. Dans cet exemple, les journaux indiquent que l'adresse source 192.168.2.10 a envoyé la requête DNS malveillante. L'hôte peut alors être retrouvé et nettoyé. Sans l'option d'entonnoir DNS, l'administrateur ne verrait le serveur DNS local que comme le système à l'origine de la requête et ne verrait pas l'hôte client infecté. Si vous avez généré un

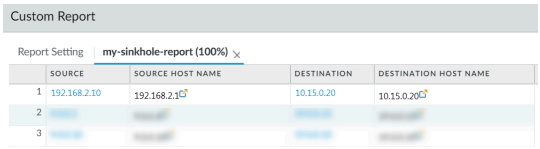
rapport sur le journal des menaces à l'aide de l'action Entonnoir, le journal indique le serveur DNS local, et non l'hôte infecté.

1. Sélectionnez **Monitor (Surveillance)** > **Manage Custom Reports (Gérer les rapports personnalisés)**.
2. Cliquez sur **Add (Ajouter)** et donnez un **Name (Nom)** au rapport.
3. Définissez un rapport personnalisé qui capture le trafic vers l'adresse d'entonnoir comme suit :
   - **Database (Base de données)** : sélectionnez **Traffic Log (Journal du trafic)**.
   - **Scheduled (Planifié)** : activez **Scheduled (Planifié)** pour que le rapport soit généré chaque nuit.
   - **Time Frame (Intervalle de temps)** : 30 jours.
   - **Selected Columns (Colonnes sélectionnées)** : sélectionnez **Source address (Adresse source)** ou **Source User (Utilisateur source)** (si vous avez configuré un User-ID), qui identifiera l'hôte client infecté dans le rapport, et **Destination address (Adresse de destination)**, qui correspondra à l'adresse d'entonnoir.
   - Dans la section au bas de l'écran, créez une requête personnalisée pour le trafic vers l'adresse d'entonnoir (10.15.0.20 dans cet exemple). Vous pouvez saisir l'adresse de destination dans la fenêtre **Query Builder (Générateur de requêtes)** (**addr.dst in 10.15.0.20**) ou sélectionner les valeurs suivantes dans chaque colonne et cliquer sur

Add (Ajouter) : Connecteur = and, Attribut = Destination Address, Opérateur = in, et Valeur = 10.15.0.20. Cliquez sur **Add (Ajouter)** pour ajouter la requête.



4. Cliquez sur **Run Now (Exécuter maintenant)** pour générer le rapport. Le rapport indiquera tous les hôtes clients qui ont envoyé du trafic à l'adresse d'entonnoir, indiquant ainsi les plus susceptibles d'être infectés. Vous pouvez alors suivre les hôtes et les analyser à la recherche de logiciels espions.



5. Pour afficher les rapports planifiés exécutés, sélectionnez **Monitor (Surveillance)** > **Reports (Rapports)**.

Signatures personnalisées

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

Vous pouvez créer des signatures de menaces personnalisées pour détecter et bloquer du trafic spécifique. Lorsque le pare-feu est géré par un serveur de gestion Panorama, le ThreatID est mappé avec la menace personnalisée correspondante sur le pare-feu pour permettre au pare-feu de générer un journal des menaces rempli avec le ThreatID personnalisé configuré. Pour en savoir plus, consultez notre guide Application personnalisée et signatures de menace.

Surveiller Advanced Threat Prevention

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

Palo Alto Networks fournit plusieurs options pour surveiller l'activité traitée par Advanced Threat Prevention afin de permettre la récupération de renseignements pour une gamme de produits qui s'appuient sur Advanced Threat Prevention et les données associées. Selon la plateforme du produit, vous pouvez accéder à des tableaux de bord de haut niveau qui fournissent également des statistiques sur les requêtes DNS et les tendances d'utilisation, y compris le contexte de l'activité réseau et les détails des requêtes DNS provenant d'utilisateurs spécifiques.

Vous pouvez également visualiser la façon dont Advanced Threat Prevention s'intègre aux autres applications et services de sécurité de Palo Alto Networks pour protéger votre organisation contre les menaces, et pour obtenir une vue de haut niveau de la santé opérationnelle globale de votre déploiement, via le centre de commande Strata Cloud Manager. Le centre de commande fonctionne comme votre page d'accueil NetSec et fournit un résumé complet de la santé, de la sécurité et de l'efficacité de votre réseau, dans un tableau de bord visuel interactif avec de multiples facettes de données pour une évaluation facile et rapide.

Pour une vue d'ensemble de haut niveau de l'activité du réseau, vous pouvez consulter le tableau de bord qui fournit une visibilité sur les données globales de gestion des menaces du réseau ainsi que sur diverses tendances DNS. Chaque carte de tableau de bord fournit une vue unique de l'impact d'une menace sur votre réseau, dans un format de rapport graphique. Cela fournit un aperçu rapide des entités les plus affectées par les menaces, en fonction de l'application, de l'utilisateur, et indique également les règles de sécurité qui appliquent les politiques de votre organisation.

Palo Alto Networks fournit plusieurs méthodes pour surveiller l'activité des menaces :

- Centre de commande Strata Cloud Manager
- Afficher les journaux des menaces
- Afficher le rapport d'Advanced Threat Prevention
- Surveiller les adresses IP bloquées
- En savoir plus sur les signatures de menaces

- Créer des rapports personnalisés en fonction des catégories de menaces

Afficher les journaux des menaces

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

Les catégories de menaces classent différents types de signatures de menaces pour vous aider à comprendre et à établir des liens entre les événements détectés par les signatures de menaces. Les catégories de menaces sont des sous-ensembles des types de signatures de menaces plus larges : logiciel espion, vulnérabilité et antivirus. Les entrées du journal des menaces affichent la **catégorie de menace** pour chaque événement enregistré.

Vous pouvez parcourir, rechercher et afficher les journaux Advanced Threat Prevention générés automatiquement lors de la détection d'une menace. En règle générale, cela inclut toute correspondance de signature de menace admissible qu'une fonctionnalité de Threat Prevention, y compris Inline ML, analyse, à moins qu'elle ne soit spécifiquement configurée avec un niveau de gravité de journal d'« aucun ». Les entrées des journaux fournissent de nombreux détails sur l'événement, y compris le niveau de menace et, le cas échéant, la nature de la menace.

- Strata Cloud Manager
- PAN-OS et Panorama

Afficher les journaux des menaces (Cloud Management)

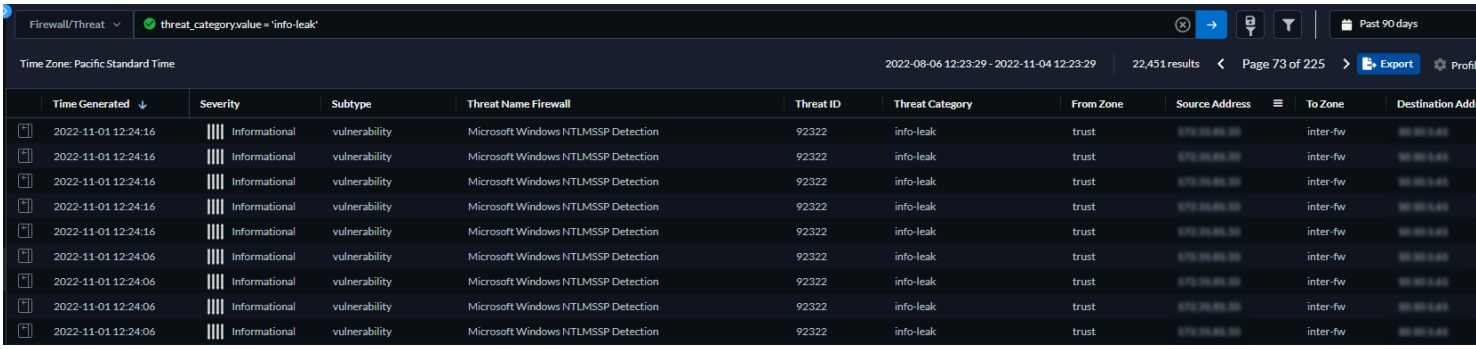
STEP 1 | Utilisez les informations d'identification associées à votre compte d'assistance Palo Alto Networks et connectez-vous au Strata Cloud Manager sur le hub.

> *Pour plus d'informations sur l'utilisation des tableaux de bord* Activity (Activité)*, reportez-vous à* Log Viewer (Visionneuse de journaux).

STEP 2 | Filtrez les journaux de menaces en fonction de la **Threat Category (Catégorie de menace)** ou du **Subtype (Sous-type)** de menace dans Prisma Access.

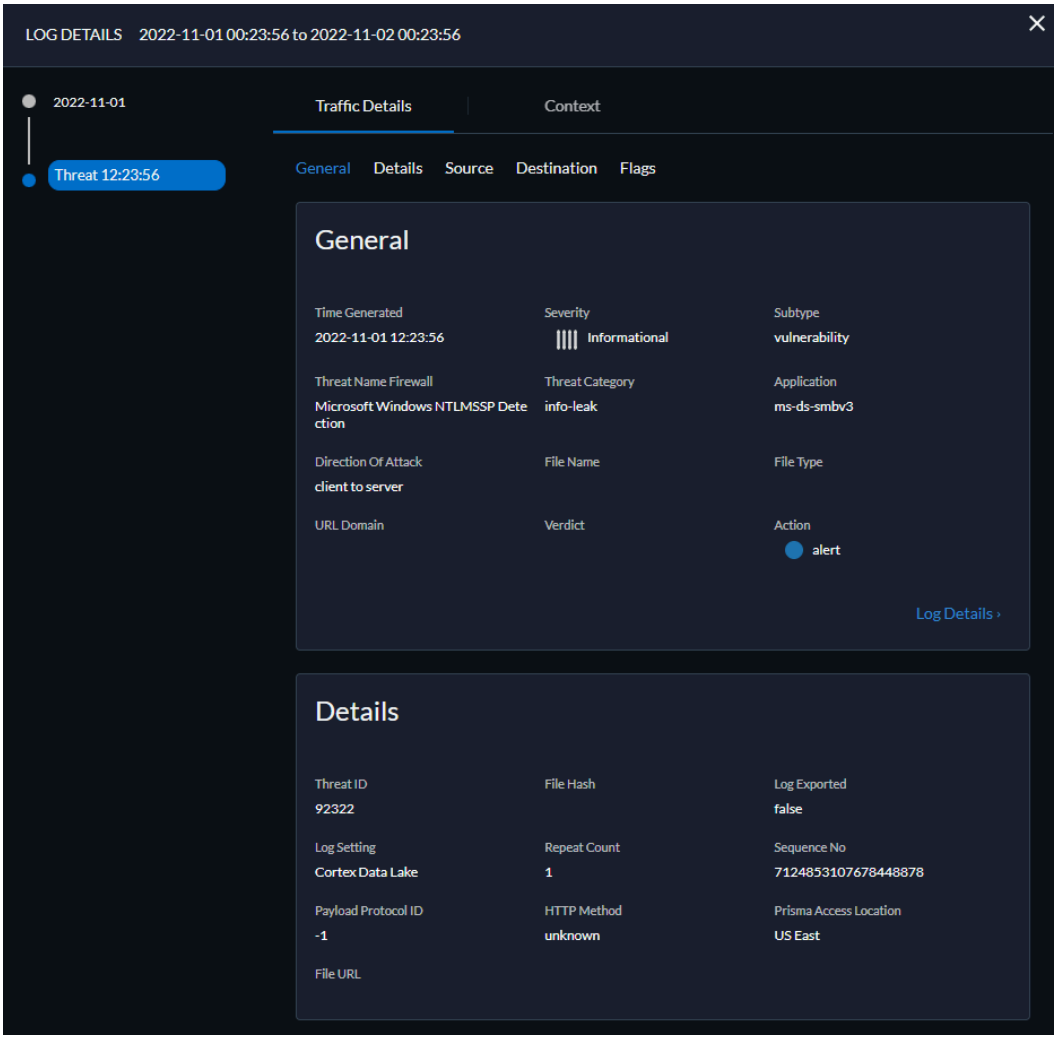
1. Sélectionnez **Incidents & Alerts (Incidents et alertes)** > **Log Viewer (Visionneuse de journaux)**.
2. Remplacez le type de journal à rechercher par **Threat (Menace)**.
3. Créez un filtre de recherche en utilisant l'un des sous-types de signature de menace utilisés par les profils Antivirus, Antispyware ou Protection contre les vulnérabilités (respectivement **antivirus**, **spyware (logiciel espion)**et **vulnerability (vulnérabilité)**) ou en fonction de la catégorie de menace à l'aide du générateur de requêtes. Par exemple,

vous pouvez utiliser `sub_type.value = 'spyware'` pour afficher les journaux des menaces qui ont été déterminées comme étant des logiciels espions. Pour rechercher d'autres sous-types, remplacez « spyware » dans l'exemple ci-dessus par un autre sous-type pris en charge (**vulnerability (vulnérabilité)** ou **spyware (logiciel espion)**). Vous pouvez également effectuer une recherche en fonction d'une **Threat Category (Catégorie de menace)** spécifique, telle qu'une vulnérabilité de fuite d'informations, en utilisant la requête suivante `threat_category.value = 'info-leak'`. Pour une liste des catégories valides que vous pouvez utiliser, reportez-vous à Catégories de signatures de menace. Ajustez les critères de recherche si nécessaire pour votre recherche, y compris des paramètres de requête supplémentaires (tels que le niveau de gravité et l'action) ainsi qu'une plage de dates.



4. Exécutez la requête une fois que vous avez fini d'assembler vos filtres.

5. Sélectionnez une entrée de journal dans les résultats pour afficher les détails du journal.



6. La **Category (Catégorie)** de menace est affichée dans le volet **Details (Détails)** de la vue détaillée du journal. D'autres détails pertinents sur la menace sont affichés dans les fenêtres correspondantes.

STEP 3 | Filtrez les journaux de menaces par les [catégories] de menaces qui ont été détectées à l'aide d'une analyse cloud en ligne (logiciel espion).

Le trafic C2 basé sur HTTP qui était initialement classé avec le nom de menace Détection du trafic HTTP Commande et contrôle analysé par le Cloud en ligne et qui est associé à plusieurs ID de menace, est désormais séparé en trois noms de menace uniques pour correspondre aux ID de menace uniques et décrire de manière plus précise les détections effectuées par Advanced Threat Prevention : ***Evasive HTTP C2 Traffic Detection (Détection de trafic HTTP C2 évasive*** *(ID de menace : 89950),* ***Evasive Cobalt Strike C2 Traffic Detection (Détection de trafic Cobalt Strike C2 évasif)*** *(ID de menace : 89955, 89956 et 89957), et* ***Evasive Empire C2 Traffic Detection (Détection de trafic Empire C2 évasif)*** *(ID de menace : 89958).*

Les journaux de trafic C2 basés sur HTTP générés avant le 11 décembre 2023 continueront à être classés avec le nom de menace Détection du trafic HTTP Commande et contrôle analysé par le Cloud en ligne.

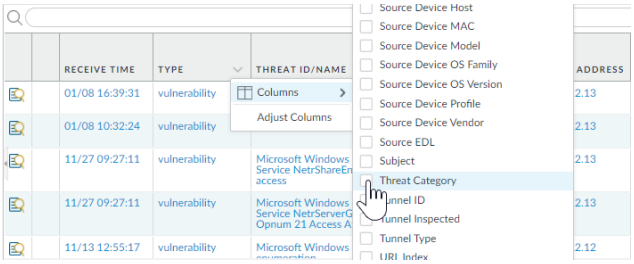
1. Sélectionnez **Incidents & Alerts (Incidents et alertes)** > **Log Viewer (Visionneuse de journaux)**.
2. Remplacez le type de journal à rechercher par **Threat (Menace)**.
3. Créez un filtre de recherche à l'aide d'une catégorie de menace utilisée exclusivement par l'analyse cloud en ligne (logiciel espion) : `threat_category.value = 'inline-cloud-c2'`. Vous pouvez limiter la recherche davantage en recoupant une valeur d'ID de menace qui correspond à un type C2 spécifique. Par exemple, `threat_category.value = 'inline-cloud-c2' AND Threat ID = 89958`, où 89958 indique l'ID de menace du trafic Empire C2 évasif..
4. Sélectionnez une entrée de journal pour afficher les détails d'une menace C2 détectée.
5. La **Category (Catégorie)** de menace est affichée sous le volet **General (Généralités)** des détails du journal. Les menaces C2 qui ont été détectées à l'aide de l'analyse cloud en ligne ont une catégorie de menace inline-cloud-c2. Vous pouvez recouper la valeur de l'**ID** de menace dans le volet **Details (Détails)** pour déterminer le type spécifique de C2 qui a été détecté.

STEP 4 | Filtrez les journaux des menaces par les [catégories] de menaces qui ont été détectées à l'aide d'une analyse cloud en ligne (vulnérabilité).

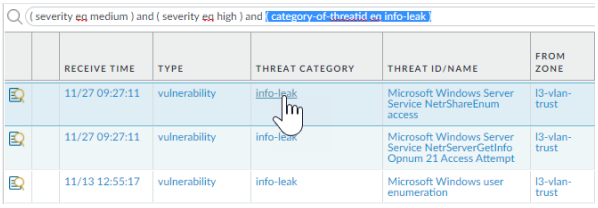
1. Sélectionnez **Incidents & Alerts (Incidents et alertes)** > **Log Viewer (Visionneuse de journaux)**.
2. Remplacez le type de journal à rechercher par **Threat (Menace)**.
3. Créez un filtre de recherche à l'aide d'une catégorie de menace utilisée exclusivement par l'analyse cloud en ligne (vulnérabilité) : `threat_category.value = 'inline-cloud-exploit'`.
4. Sélectionnez une entrée de journal pour afficher les détails des vulnérabilités d'injection de commande et d'injection SQL qui ont été détectées. Les menaces d'exploitation en ligne (injection SQL) ont un ID de 99950 tandis que les menaces d'exploitation en ligne (injection de commandes) ont un ID de 99951.

Afficher les journaux des menaces (NGFW (Managed by PAN-OS or Panorama))

- Filtrer les journaux des menaces par catégorie de menace.
  1. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menace)**.
  2. Ajoutez la colonne Threat Category (Catégorie de menace) pour pouvoir afficher la Catégorie de menace pour chaque entrée de journal :



  3. Pour filtrer en fonction de la catégorie de menace :
     - Utilisez le constructeur de requête de journal pour ajouter un filtre avec l'**Attribute (Attribut)** catégorie de menace et dans le champ **Value (Valeur)**, entrez une catégorie de menace.
     - Sélectionnez la catégorie de menace de toute entrée de journal pour ajouter cette catégorie au filtre :



- Filtrez les journaux de menaces par type de signature de menace.
  1. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menace)**.
  2. Ajoutez la colonne **Type**, si elle n'est pas présente, afin que vous puissiez afficher la catégorie de signature de menace pour chaque entrée de journal :
  3. Pour filtrer en fonction du type de signature :
     - Utilisez le générateur de requêtes de journal pour ajouter un filtre avec l'**Attribute (Attribut)** de la catégorie de signature de menace et dans le champ **Value (Valeur)**, saisissez un type de signature de menace. Vous pouvez sélectionner parmi **une vulnérabilité**, **un virus** et **un logiciel espion**, qui correspond aux signatures gérées par vos profils de sécurité Protection contre les vulnérabilités, Antivirus et Antispyware.
     - Sélectionnez le **Type** de n'importe quelle entrée de journal pour ajouter ce type de signature de menace au filtre. Vous pouvez également générer manuellement votre requête en utilisant le filtre et le type de signature de menace.

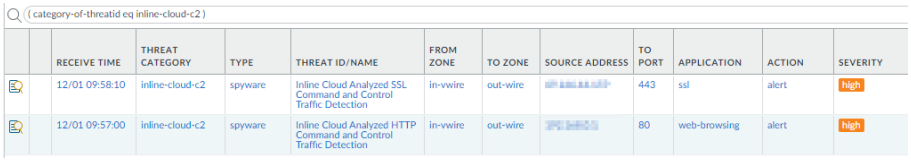
- Filtrez les journaux de menaces par les [catégories] de menaces qui ont été détectées à l'aide d'une analyse cloud en ligne (logiciel espion).

  Le trafic C2 basé sur HTTP qui était initialement classé avec le nom de menace Détection du trafic HTTP Commande et contrôle analysé par le Cloud en ligne et qui est associé à plusieurs ID de menace, est désormais séparé en trois noms de menace uniques pour correspondre aux ID de menace uniques et décrire de manière plus précise les détections effectuées par Advanced Threat Prevention : ***Evasive HTTP C2 Traffic Detection (Détection de trafic HTTP C2 évasive*** *(ID de menace : 89950),* ***Evasive Cobalt Strike C2 Traffic Detection (Détection de trafic Cobalt Strike C2 évasif)*** *(ID de menace : 89955, 89956 et 89957), et* ***Evasive Empire C2 Traffic Detection (Détection de trafic Empire C2 évasif)*** *(ID de menace : 89958).*

  Si vous n'installez pas le contenu de la mise à jour ou si vous examinez les journaux de trafic C2 basé sur HTTP générés avant le 11 décembre 2023 (date de publication de la mise à jour du contenu), tout le trafic C2 basé sur HTTP continuera d'être classé avec le nom de menace Détection du trafic HTTP Commande et contrôle analysé par le Cloud en ligne.

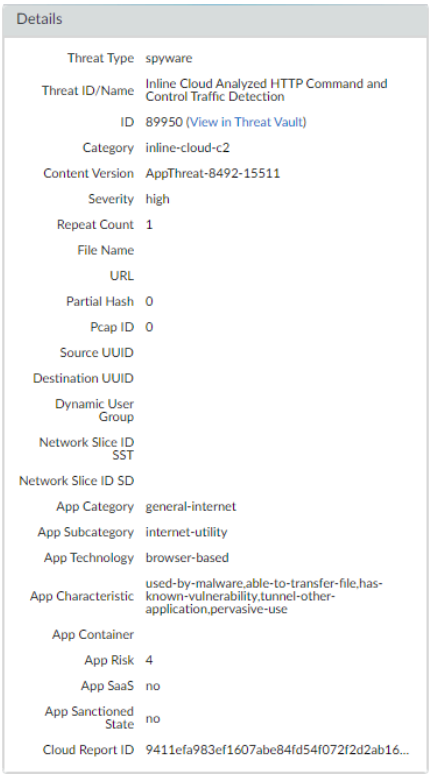
  1. Sélectionnez **Monitor (Surveiller)** > **Logs (Journaux)** > **Threat (Menace)**. Vous pouvez filtrer les journaux en fonction de certaines caractéristiques de la menace. Examinons les exemples suivants :

     - Sélectionnez à l'aide de `( category-of-threatid eq inline-cloud-c2 )` pour afficher les journaux des menaces C2 qui ont été analysées à l'aide du mécanisme d'analyse cloud en ligne d'Advanced Threat Prevention.
     - Vous pouvez limiter la recherche davantage en recoupant une valeur d'ID de menace qui correspond à un type C2 spécifique. Par exemple, `( category-of-threatid eq inline-cloud-c2 ) and (name-of-threatid eq 89958)`, où 89958 indique l'ID de menace du trafic empire C2 évasif.
     - Filtrez à l'aide de `(local_deep_learning eq yes)` pour afficher les journaux des menaces qui ont été analysées à l'aide du mécanisme d'analyse approfondie locale d'Advanced Threat Prevention.

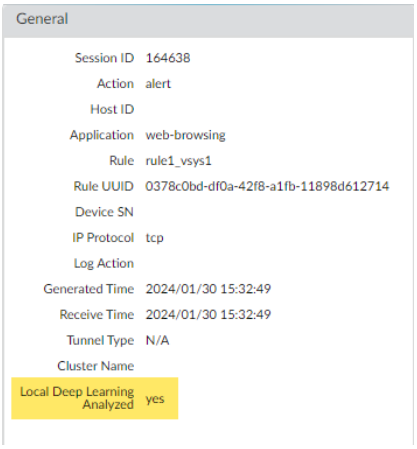
     

  2. Sélectionnez une entrée de journal pour afficher les détails d'une menace C2 détectée.
  3. La **catégorie** de menace s'affiche sous le volet **Détails** de la vue détaillée du journal. Les menaces C2 qui ont été détectées à l'aide de l'analyse cloud en ligne ont une catégorie

de menace inline-cloud-c2. Vous pouvez recouper la valeur de l'**ID** de menace pour déterminer le type spécifique de C2 qui a été détecté.

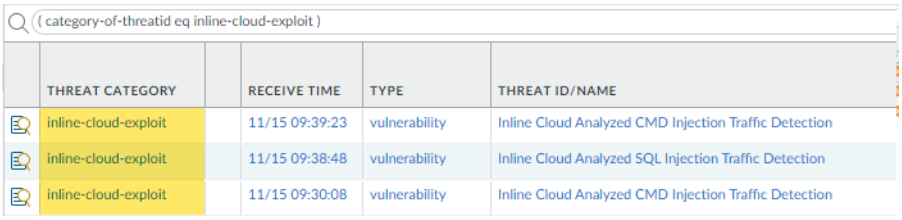


4. Si la menace a été analysée à l'aide du deep learning local, le champ **Local Deep Learning Analyzed (Deep Learning local analysé)** indique oui.

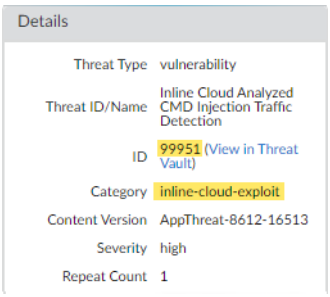


- Surveillez l'activité sur le pare-feu pour détecter les exploits de vulnérabilité qui ont été détectés à l'aide d'une analyse cloud en ligne (vulnérabilité).
  1. Sélectionnez **Monitor (Surveiller)** > **Logs (Journaux)** > **Threat (Menace)** et filtrez par `( category-of-threatid eq inline-cloud-exploit )` pour afficher les journaux qui ont été analysés à l'aide du mécanisme d'analyse cloud en ligne d'Advanced Threat Prevention. Les menaces d'exploitation en ligne (injection SQL) ont un ID de

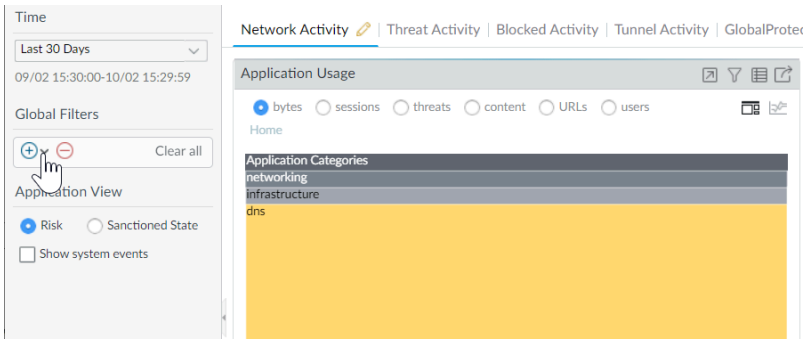
99950 tandis que les menaces d'exploitation en ligne (injection de commandes) ont un ID de 99951.



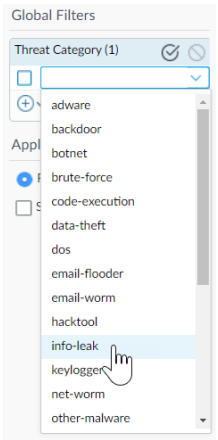
2. Sélectionnez une entrée de journal pour afficher les détails d'un exploit de vulnérabilité.
3. La **catégorie** de menace s'affiche sous le volet **Détails** de la vue détaillée du journal. Les exploits de vulnérabilité qui ont été détectés à l'aide de l'analyse cloud en ligne ont une catégorie de menace exploit-cloud-en-ligne.



- Filtrer l'activité ACC par catégorie de menace.
  1. Sélectionnez **ACC** et ajoutez une catégorie de menace en tant que filtre général :



  2. Sélectionnez la catégorie de menace pour filtrer tous les onglets ACC.



Afficher le rapport d'Advanced Threat Prevention

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

Le rapport Advanced Threat Prevention est disponible via l'API de l'archivage sécurisé des menaces et fournit des informations d'analyse et de détection détaillées, ainsi que des informations sur la transaction, la session et d'autres processus associés. Le rapport contient tout ou partie des informations décrites dans le tableau suivant en fonction des informations de session configurées sur le pare-feu qui a traité le fichier et des détails de l'analyse du fichier au format JSON.

Les NGFW ne disposent pas d'un accès direct aux rapports via PAN-OS ; vous devez plutôt référencer le cloud_reportid associé au journal des menaces et utiliser l'API d'archivage sécurisé des menaces pour rechercher et récupérer le rapport.

*Pour Prisma Access (par le biais de Strata Cloud Manager), le rapport peut être consulté à partir de la visionneuse de journaux (Afficher les journaux des menaces). Les entrées de journal avec un rapport généré sur Advanced Threat Prevention comportent un lien de téléchargement à côté de la valeur de l'ID du rapport sous la colonne **Cloud ReportID (ID de rapport Cloud)**.*

En-tête du rapport	Description
Informations générales	Contient des informations sur le pare-feu / la plate-forme de sécurité qui a traité la menace. • Le numéro d'identification du rapport cloud contenant les données du rapport sur les menaces avancées. • Messages d'erreur susceptibles d'avoir été générés lors de la création du rapport.
Informations sur PAN-OS	Contient des informations sur le pare-feu / la plate-forme de sécurité qui a traité la menace. • Interface du pare-feu (IPv4/IPv6)

En-tête du rapport	Description
	• Version du package de contenu • Nom d'hôte du pare-feu • Modèle de pare-feu • Numéro de série • Version de PAN-OS
Informations sur la session	Contient des informations de session basées sur le trafic lorsqu'il a traversé le pare-feu / la plate-forme de sécurité qui a transféré la menace. Les options suivantes sont disponibles'A0;: • IP source • Port source • IP de destination • Port de destination • ID de session • Horodatage de la session • Type de charge utile
Données de transaction	Les données de transaction fournissent un aperçu des détails de la charge utile et contiennent le ou les rapports du service de détection. Les options suivantes sont disponibles'A0;: • ID de transaction • Hachage SHA256 de la charge utile
Résultats du service de détection	Lorsque l'analyse des menaces est effectuée par le cloud Advanced Threat Prevention, cette section contient des entrées qui indiquent les résultats de l'analyse. Cela inclut le ou les rapports du service de détection, qui fournissent en outre les techniques classées MITRE ATT&CK® utilisées, ainsi que les détails de la charge utile. Les détections de commande et contrôle pour le framework Empire C2 affichent des informations contextuelles supplémentaires. Cela inclut les rapports générés à partir de la phase de mise en scène et de commande (post-exploitation) d'une attaque qui se produit dans des sessions distinctes. Les informations suivantes sont disponibles : • Description de l'attaque : décrit la nature de l'attaque C2.

En-tête du rapport	Description
	• Détails de l'attaque : indiquent la phase de l'attaque Empire C2 et décrit les échanges entre le serveur et le client. • Preuves de l'attaque : répertorient le comportement et les actions correspondant à l'attaque Empire C2 connue. *L'attaque C2 basée sur Empire est détectée à l'aide d'un détecteur de sous-module contenu dans le moteur d'analyse* ***Inline Cloud Analyzed HTTP Command and Control Traffic Detection (Détection du trafic HTTP Commande et contrôle analysé par le Cloud en ligne)*** *avec un ID de menace unique de 89958.*

Surveiller les adresses IP bloquées

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

Le pare-feu conserve une liste de blocage des adresses IP source qu'il bloque. Lorsque le pare-feu bloque une adresse IP source, par exemple lorsque vous configurez l'une des règles de politique suivantes, le pare-feu bloque le trafic dans le matériel avant que ces paquets n'utilisent des ressources du processeur ou de tampon de paquet :

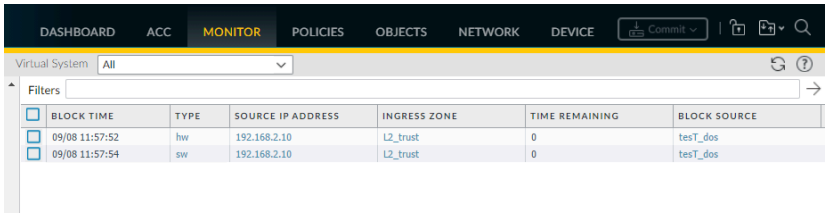
- Une règle classifiée de politique de Protection DoS avec l'action de **Protect (Protéger)** (une politique de Protection DoS classifiée spécifie que les connexions entrantes correspondent à une adresse IP source, une adresse IP de destination ou à une paire d'adresses IP source et de destination est associée à un profil de protection DoS classifié, comme décrit dans DoS Protection contre l'inondation de nouvelles sessions).
- Une règle de Politique de sécurité qui utilise un profil de protection contre les vulnérabilités

Le blocage des adresses IP matérielles est pris en charge sur les pare-feu des séries PA-3200, PA-5200, PA-5400 (à l'exception du PA-5450) et des pare-feu des séries PA-7000.

Vous pouvez afficher la liste des blocs, obtenir des informations détaillées sur une adresse IP dans la liste des blocs ou afficher le nombre d'adresses bloquées par le matériel et le logiciel. Vous pouvez supprimer une adresse IP de la liste si vous pensez qu'elle ne devrait pas être bloquée. Vous pouvez modifier la source des informations détaillées sur les adresses de la liste. Vous pouvez également modifier la durée pendant laquelle le matériel bloque les adresses IP.

- Afficher les entrées de la liste d'interdiction.
  1. Sélectionnez **Monitor (Surveillance)** > **Block IP List (Bloquer la liste d'adresses IP)**.

     Les entrées de la liste d'interdiction indiquent dans la colonne Type si elles ont été bloquées par le matériel (hw) ou le logiciel (sw).
  2. Voir au bas de l'écran :
     - Le nombre **Total Blocked IPs (Total des adresses IP bloquées)** sur le nombre d'adresses IP bloquées prises en charge par le pare-feu.
     - Pourcentage de la liste d'interdiction utilisée par le pare-feu.
  3. Pour filtrer les entrées affichées, sélectionnez une valeur dans une colonne (qui crée un filtre dans le champ **Filters (Filtres)**) et appliquez le filtre (→). Sinon, le pare-feu affiche les 1 000 premières entrées.
  4. Entrez un numéro de **Page** ou cliquez sur les flèches en bas de l'écran pour avancer dans les pages des entrées.
  5. Pour afficher les détails d'une adresse dans la liste des blocs, passez la souris sur une adresse IP source et cliquez sur le lien vers le bas. Cliquez sur le lien **Who Is (Qui est...)** qui affiche l'information Network Solutions Whois sur l'adresse.



- Supprimer les entrées de la liste d'interdiction.

  Supprimez une entrée si vous déterminez que l'adresse IP ne devrait pas être bloquée. Révisez ensuite la règle de politique qui a provoqué le blocage de l'adresse par le pare-feu.

  1. Sélectionnez **Monitor (Surveillance)** > **Block IP List (Bloquer la liste d'adresses IP)**.
  2. Sélectionnez une ou plusieurs entrées et cliquez sur **Delete (Supprimer)**.
  3. (Facultatif) Sélectionnez **Clear All (Tout effacer)** pour supprimer toutes les entrées de la liste.

- Désactivez ou réactivez le blocage de l'adresse IP matérielle à des fins de dépannage.

  Bien que le blocage de l'adresse IP matérielle soit désactivé, le pare-feu effectue toujours le blocage logiciel de toute adresse IP que vous avez configuré.

```
> set system setting hardware-acl-blocking [enable | disable]
```

  Pour préserver ressources du processeur ou de la mémoire tampon des paquets, gardez le blocage matériel de l'adresse IP activé sauf si le support technique de Palo Alto Networks vous demande de le désactiver, par exemple, si un débogage d'un flux de trafic est en cours.

- Réglez le nombre de secondes pendant lesquelles les adresses IP bloquées par le matériel restent sur la liste d'interdiction (la plage est comprise entre 1 et 3600 ; La valeur par défaut est 1).

```
> set system setting hardware-acl-blocking duration <seconds>
```

Maintenez une durée plus courte pour les entrées de liste d'interdiction matérielle que pour les entrées de liste d'interdiction logicielle afin de réduire la probabilité de dépasser la capacité de blocage du matériel.

- Modifier le site Web par défaut pour trouver plus d'informations sur une adresse IP de Solutions réseau Qui est à un site Web différent.

```
# set deviceconfig system ip-address-lookup-url <url>
```

- Afficher les nombres d'adresses IP sources bloquées par le matériel et le logiciel, par exemple pour afficher le taux d'une attaque.

  Afficher la somme totale des entrées d'adresse IP dans la liste des blocs et la table des blocs matériels (bloqués par le matériel et le logiciel) :

```
> show counter global name flow_dos_blk_num_entries
```

  Afficher le nombre d'entrées d'adresses IP sur la table des blocs matériels bloquées par le matériel :

```
> show counter global name flow_dos_blk_hw_entries
```

  Afficher le nombre d'entrées d'adresses IP dans la liste d'interdiction qui ont été bloquées par le logiciel :

```
> show counter global name flow_dos_blk_sw_entries
```

- Afficher les informations de liste d'interdiction par emplacement sur un pare-feu de la série PA-7000.

```
> show dos-block-table software filter slot <slot-number>
```

En savoir plus sur les signatures de menaces

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	☐ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

Les journaux de menaces du pare-feu enregistrent toutes les menaces détectées par le pare-feu en fonction des signatures de menaces (Paramétrage des profils Antivirus, Antispyware et Protection contre les vulnérabilités) et l'ACC affiche un aperçu des principales menaces sur votre réseau. Chaque événement que le pare-feu enregistre inclut un ID qui identifie la signature de menace associée.

Vous pouvez utiliser l'ID de menace trouvé avec un journal de menaces ou une entrée ACC pour :

- Vérifiez facilement si une signature de menace est configurée comme une exception à votre politique de sécurité (Créer des exceptions de menace).
- Trouvez les dernières informations sur le coffre-fort des menaces concernant une menace spécifique. Étant donné que l'Archivage sécurisé des menaces est intégré au pare-feu, vous pouvez visualiser les détails des menaces directement dans le contexte du pare-feu ou lancer une recherche d'Archivage sécurisé des menaces dans une nouvelle fenêtre de navigateur pour une menace enregistrée par le pare-feu.

Si une signature a été désactivée, l'UTID de la signature pourrait être réutilisé pour une nouvelle signature.

Passez en revue les notes de mise à jour de contenu pour prendre connaissance des notifications concernant de nouvelles signatures et les signatures désactivées. Les signatures peuvent être désactivées dans les cas suivants : l'activité que la signature détecte n'est plus utilisée par les pirates, la signature générait un nombre considérable de faux positifs ou la signature a été regroupée avec d'autres signatures en une seule signature (optimisation de signatures).

STEP 1 | Vérifier que le pare-feu est connecté à l'Archivage sécurisé des menaces.

Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifier le paramètre **Logging and Reporting (Journalisation et génération de rapports)** sur **Enable Threat Vault Access (Activer l'accès à l'archivage sécurisé des menaces)**. L'accès au coffre de menaces est activé par défaut.

STEP 2 | Recherchez l'ID de menace pour les menaces détectées par le pare-feu.

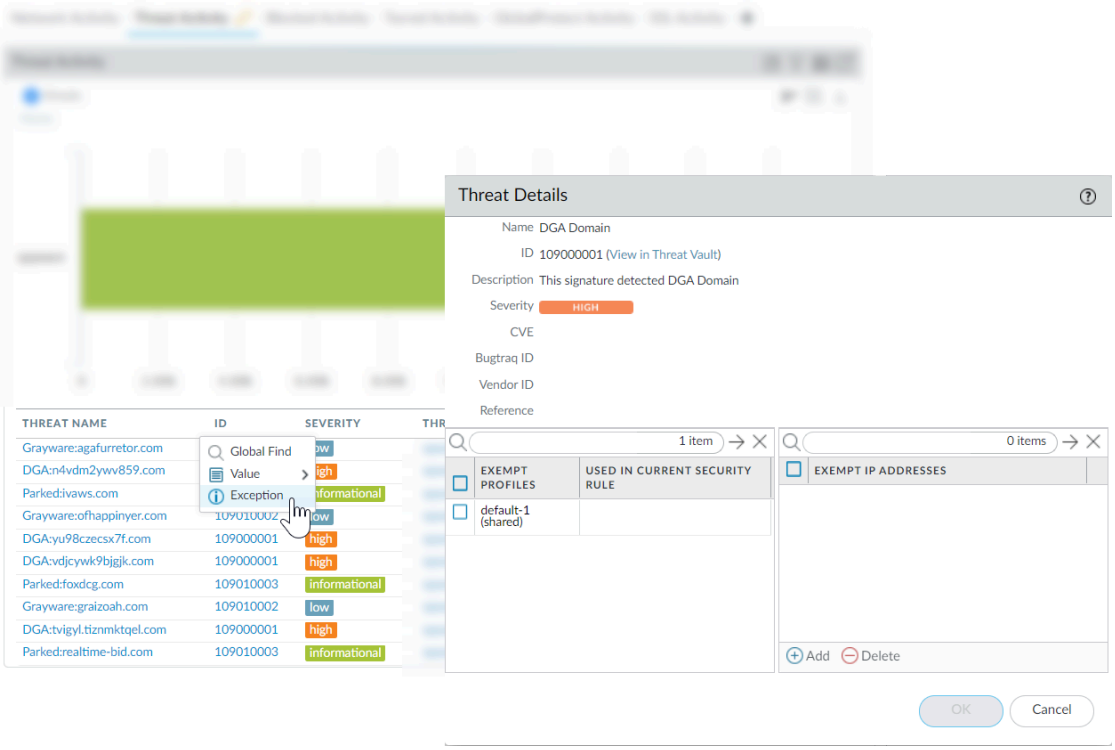
- Pour voir chaque événement de menace détecté par le pare-feu en fonction des signatures de menaces, sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menaces)**. Vous pouvez trouver l'ID d'une entrée de menace répertoriée dans la colonne ID ou

sélectionner l'entrée de journal pour afficher les détails du journal, y compris l'ID de menace.

- Pour afficher un aperçu des principales menaces sur le réseau, sélectionnez **ACC** > **Threat Activity (Activité de menace ACC)** et jetez un coup d'œil au widget Activité de la menace. La colonne ID affiche l'ID de menace pour chaque menace affichée.
- Pour afficher les détails des menaces que vous pouvez configurer en tant qu'exceptions de menace (le pare-feu applique la menace différemment de l'action par défaut définie pour la signature de menace), sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware/Vulnerability Protection (Protection contre les vulnérabilités Antispyware)**. **Ajoutez** ou modifiez un profil et cliquez sur l'onglet **Exceptions** pour afficher les exceptions configurées. Si aucune exception n'est configurée, vous pouvez filtrer les signatures de menaces ou sélectionner **Afficher toutes les signatures**.

STEP 3 | Survolez un **Threat Name (Nom de menace)** ou l'**ID** de la menace pour ouvrir la liste déroulante et cliquez sur **Exception (Exception)** pour examiner les détails de la menace et la manière dont le pare-feu est configuré pour appliquer la menace.

Par exemple, renseignez-vous sur l'une des principales menaces répertoriées sur l'ACC :



STEP 4 | Examiner les derniers **Threat Details (Détails de la Menace)** pour la menace et lancez une recherche dans l'Archivage sécurisé des menaces en fonction de l'ID de menace.

- Les détails sur les menaces affichées incluent les dernières informations dans l'Archivage sécurisé des menaces sur la menace, les ressources que vous pouvez utiliser pour en savoir plus sur la menace et les CVEs associés à la menace.
- Sélectionnez **View in Threat Vault (Afficher dans l'Archivage sécurisé des menaces)** pour ouvrir une recherche d'Archivage sécurisé des menaces dans une nouvelle fenêtre et

rechercher les dernières informations que la base de données des menaces de Palo Alto Networks détient pour cette signature de menace.

STEP 5 | Vérifier si une signature de menace est configurée comme une exception à votre politique de sécurité.

- Si la colonne **Used in current security rule (Utilisé dans la règle de sécurité actuelle)** est vide, le pare-feu applique la menace en fonction de l'action de signature par défaut recommandée (par exemple, blocage ou alerte).
- Une coche dans la colonne **Used in current security rule (Utilisé dans la règle de sécurité actuelle)** indique qu'une règle de politique de sécurité est configurée pour appliquer une action autre que la valeur par défaut pour la menace (par exemple, autoriser), en fonction des paramètres liés **Exempt Profiles (Profils exemptés)**.

*La **colonne Utilisé dans la règle de sécurité** n'indique pas si la règle de politique de sécurité est activée, uniquement si la règle de politique de sécurité est configurée avec l'exception de menace. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** pour vérifier si une règle de stratégie de sécurité indiquée est activée.*

STEP 6 | **Ajouter** une adresse IP sur laquelle filtrer l'exception de menace ou afficher les **Exempt IP Addresses (Adresses IP d'exemption)** existantes.

Configurez une adresse IP d'exemption pour appliquer une exception de menace uniquement lorsque la session associée a une adresse IP source ou de destination correspondante ; Pour toutes les autres sessions, la menace est appliquée en fonction de l'action de signature par défaut.

Créer des rapports personnalisés en fonction des catégories de menaces

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Licence Advanced Threat Prevention (pour une prise en charge améliorée des fonctionnalités) ou Threat Prevention

Vous pouvez créer des rapports personnalisés sur le pare-feu pour générer (à la demande) ou planifier (chaque nuit) des rapports en fonction des attributs ou des éléments d'information clés que vous souhaitez récupérer et analyser.

- Créez des rapports personnalisés basés sur les catégories de menaces pour recevoir des informations sur les types spécifiques de menaces détectées par le pare-feu.
  1. Sélectionnez **Monitor (Surveiller)** > **Manage Custom (Gestion personnalisée)** des rapports pour ajouter un nouveau rapport personnalisé ou modifier un rapport existant.
  2. Choisissez la **base de données** à utiliser comme source pour le rapport personnalisé. Dans ce cas, sélectionnez **Menace** dans l'un des deux types de sources de base de données, dans les bases de données récapitulatives et dans les journaux détaillés. Les données de la base de données de synthèse sont condensées pour permettre un temps de réponse plus rapide lors de la génération de rapports. Les journaux détaillés prennent plus de temps à générer, mais fournissent un ensemble détaillé et détaillé de données pour chaque entrée de journal.
  3. Dans le Constructeur de requêtes, ajoutez un filtre de rapport avec l'attribut **Threat Category (Catégorie de menace)** et dans le champ Valeur, sélectionnez une catégorie de menace sur laquelle baser votre rapport.
  4. Pour tester les paramètres de rapport, sélectionnez **Run Now (Lancer l'exécution)**.
  5. Cliquez sur **OK** pour enregistrer le rapport.