MEILLEURES PRATIQUES

PROTÉGER LES DONNÉES DANS LE CENTRE DE DONNÉES
RÉDUIRE LA SURFACE D'ATTAQUE ET PRÉVENIR LES MENACES

Protéger vos actifs numériques stratégiques

Le volume et de la complexité des attaques portées contre les centres de données des entreprises et des administrations ne cessent de s'accroître à un rythme alarmant. Les publications de recherches montrent que ces attaques tendent à viser trois grandes catégories :

- Les cybercriminels, qui attaquent les entreprises commerciales et de détail, comme les magasins, les chaînes de restaurants, les banques, etc.
- Les « hacktivists » qui cherchent à nuire ou causer des dommages aux entreprises auxquels ils s'opposent.
- Les attaques sponsorisées par un État, et qui visent un gouvernement ou des entreprises.

Traditionnellement, les organisations ont répondu à ces attaques en concentrant leur attention sur la détection et la prévention des menaces au niveau du périmètre du réseau et du trafic nord-sud, c'est-à-dire du trafic entrant dans le centre de données et en sortant. Un grand nombre d'administrateurs informatiques estimaient que le trafic est-ouest, entre les systèmes et les applications au sein d'un centre de données, était digne de confiance et ne nécessitait aucune protection.

Cependant, pour un grand nombre de violations ayant fait l'objet de rapports, il apparaît que lorsqu'un attaquant réussit à percer le périmètre du réseau, il est capable de se déplacer latéralement dans le réseau, à l'insu de tous. Il peut ainsi repérer les autres serveurs, accéder aux données confidentielles et les sortir du périmètre réseau dans la mesure où le niveau de sécurité appliqué au périmètre ne s'appliquait pas aux segments internes du centre de données.

Pour sécuriser suffisamment le centre de données, l'accès aux données confidentielles qui y sont stockées doit être régulé à l'aide d'informations d'identification fiables et de règles basées sur les applications, ainsi que par le biais d'outils d'inspection et de prévention des menaces, comme les antivirus, les fonctions de prévention des intrusions (IPS) et les antispywares.

Une architecture de sécurité intégrée et extensible est nécessaire dans l'ensemble de l'organisation pour protéger les informations confidentielles contre tout accès non autorisé et toute fuite de données. Une protection est ainsi nécessaire non seulement au niveau du périmètre, mais également en périphérie du centre de données et au niveau de ses segments internes. Cette approche est connue sous le nom de « modèle Confiance zéro » en matière de sécurité des informations.

Conseil : Identifiez le trafic nord-sud (c'est-à-dire entre le centre de données et les systèmes externes) et le trafic est-ouest (au sein du centre de données), puis recherchez attentivement les faiblesses de sécurité invisibles concernant le trafic est-ouest.

Ce modèle (initialement proposé par le cabinet Forrester® Research) présuppose que le trafic est vecteur de menace jusqu'à preuve du contraire. Au lieu de s'appuyer sur un ensemble d'appareils de sécurité axées sur le périmètre, le cabinet Forrester conseille d'élaborer une architecture réseau comprenant une « passerelle de segmentation » qui combine plusieurs opérations de sécurité et de chiffrement (pare-feu, IPS, NAC, filtrage du contenu, VPN, etc.) au sein d'un périphérique unique haute débit situé au centre du réseau.

Les administrateurs peuvent ainsi segmenter le réseau en différentes zones pour distinguer le trafic vers des informations confidentielles de celui à destination de données moins stratégiques. Il est alors plus difficile pour un attaquant d'accéder durablement à ces les informations ou de les extraire du réseau.

La plate-forme de sécurité nouvelle génération de Palo Alto Networks®, y compris les appareils physiques et virtuels, vous permettent de mettre en œuvre un modèle de sécurité Confiance zéro efficace en vous donnant la possibilité de segmenter votre réseau, vos applications de liste blanche ou de liste noire, l'accès utilisateur et les contenus spécifiques, et de rechercher les menaces dans l'ensemble du trafic.

Approche progressive de la protection des données dans le centre de données

Que vous ayez récemment commencé à mettre en œuvre des produits Palo Alto Networks ou que vous les administriez depuis des années, tirez-en le meilleur parti en révisant vos meilleures pratiques afin d'utiliser l'approche Confiance zéro pour sécuriser vos données dans le centre de données.

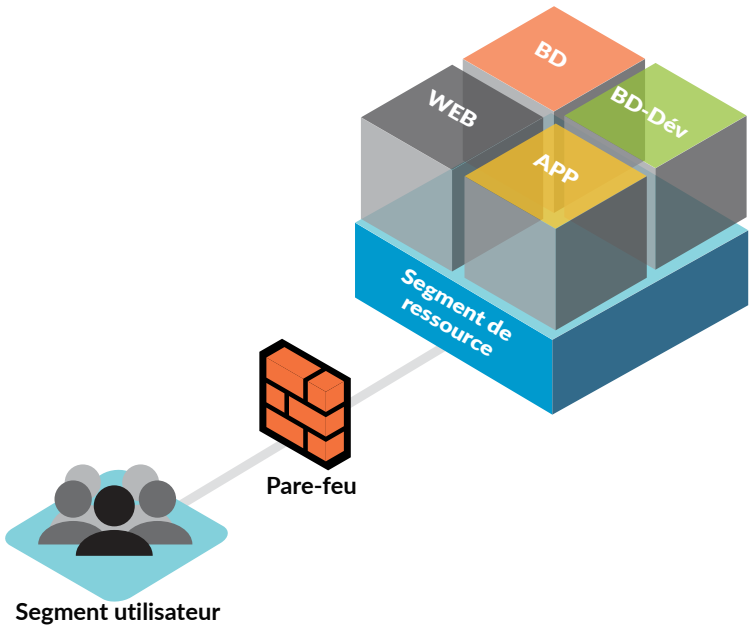
Comme pour n'importe quelle technologie, une mise en œuvre complète passe généralement par une approche progressive. Le déploiement est ainsi opéré en plusieurs phases soigneusement planifiées pour une transition des plus transparentes et perturbant le moins possible les utilisateurs.

Dans l'optique d'une telle transition, nous vous recommandons d'appliquer en trois phases nos meilleures pratiques concernant le centre de données, chacune s'appuyant sur les recommandations de la précédente. Au terme de la mise en œuvre de votre centre de données, il est essentiel de parvenir à une visibilité granulaire et à un examen complet du trafic nord-sud et est-ouest afin d'y prévenir toute menace.

PHASE 1 : PLANIFICATION DU DÉPLOIEMENT DU CENTRE DE DONNEES

Lorsque vous remplacez pour la première fois un pare-feu hérité par un nouveau système ou mettez en œuvre un pare-feu de centre de données, une planification minutieuse s'impose dans la mesure où ces deux options permettent d'élaborer de toutes pièces une toute nouvelle architecture réseau (de type Confiance zéro).

Tout d'abord, procédez à un inventaire précis des environnements physiques et logiques du centre de données, et à leur évaluation. Identifiez et documentez les différents systèmes en place, notamment les serveurs, les routeurs, les commutateurs, et les autres infrastructures réseau et de sécurité. Cette évaluation vous permettra d'identifier et de caractériser l'ensemble du trafic de données, que ce soit entre le centre de données et les systèmes externes (y compris d'autres centres de données de votre organisation), ou entre les systèmes du centre de données.



Conseil : Vous pouvez exploiter quatre leviers pour protéger les ressources de votre centre de données : contrôler les accès, rechercher les abus dans les modèles d'utilisation des données, supprimer les données dont l'organisation n'a plus besoin et chiffrer les données pour les rendre plus difficilement exploitables en cas de vol.
(Source : Forrester Research)

Prévoyez de déployer les technologies de base suivantes dans votre plateforme Palo Alto Networks. Elles vous aideront en effet à cerner le trafic transitant dans votre centre de données, à comprendre en quoi il consiste, et à identifier les données ciblées et les auteurs des tentatives d'accès. Une telle connaissance du trafic est indispensable pour protéger efficacement vos données stratégiques.

- User-ID™ vérifie l'identité de l'utilisateur, et plus seulement les adresses IP, à l'aide d'annuaires d'entreprises, d'offres de services de terminal ou de Microsoft® Exchange. User-ID fournit des informations contextuelles détaillées sur les utilisateurs qui accèdent au réseau.
- App-ID™ reconnaît et classe de façon native des milliers d'applications, notamment des applications Web. App-ID vous aide à identifier les applications utilisées, à savoir si certaines utilisent des ports par défaut ou personnalisés, et à détecter les applications inconnues et non autorisées présentes sur le réseau.
- Content-ID™ permet aux clients d'appliquer des politiques afin d'inspecter et de contrôler le contenu transitant sur le réseau. Content-ID combine un moteur de prévention des menaces en temps réel, une base de données complète d'URL et des éléments d'identification des applications pour limiter les transferts de données et de fichiers non autorisés.
- Il lui est alors possible de détecter et de bloquer une large gamme d'exploitations, de logiciels malveillants et de connexions Web (HTTP et DNS) dangereuses ou non autorisées.
- Content-ID, disponible dans le cadre d'un abonnement Threat Prevention, vous permet de contrôler les contenus non approuvés, de limiter les transferts de fichiers et de données stratégiques non autorisés, notamment des numéros de cartes de crédit ou de sécurité sociale, et de protéger votre organisation contre les logiciels malveillants et les exploitations connus ou nouveaux, par le biais de politiques.

Type de politique	Description
Sécurité	Détermine si une session doit être bloquée ou autorisée en fonction des attributs du trafic comme la zone de sécurité source et de destination, l'adresse IP source et de destination, l'application, l'utilisateur et le service.
NAT	Indique au pare-feu les paquets devant être traduits et la manière dont la traduction doit être effectuée. Le pare-feu prend en charge la traduction de l'adresse source et/ou du port et la traduction de l'adresse de destination et/ou du port.
QoS	Identifie le trafic nécessitant un traitement QoS (traitement préférentiel ou à bande passante limitée) à l'aide d'un ou plusieurs paramètres définis et de leur affectation à une classe.
Transfert basé sur une politique	Identifie le trafic qui doit utiliser une autre interface de sortie que celle qui serait normalement utilisée en fonction de la table de routage.
Décryptage	Identifie le trafic crypté à des fins de visibilité, contrôle et sécurité granulaire.
Contrôle prioritaire sur l'application	Identifie les sessions que vous ne souhaitez pas voir traitées par le moteur App-ID, qui est une inspection de la Couche 7.
Portail captif	Identifie le trafic qui nécessite l'identification de l'utilisateur. La politique de portail captif est uniquement déclenchée si d'autres mécanismes User-ID n'ont pas identifié d'utilisateur à associer à l'adresse IP source.
Protection DoS	Identifie les attaques de déni de service (DoS) et prend des mesures de protection en cas de correspondance des règles.
Protection de zone	Fournit à des zones réseau spécifiques d'un même réseau une protection supplémentaire contre les attaques, notamment les techniques d'évasion et le respect des seuils de trafic.

Conseil : Installez la plateforme devant n'importe quel périphérique de protection hérité afin qu'elle examine le trafic réseau qui le traverse et vous fournisse la visibilité qui vous fait défaut.

Conseil : Le décryptage peut être effectué sur des interfaces de câble virtuel (VWire), de Couche 2, ou de Couche 3, ou en mode TAP. Pour bénéficier d'une meilleure vision du trafic dans le centre de données, veillez à le décrypter au maximum.

Conseil : La plateforme de sécurité nouvelle génération de Palo Alto Networks peut fonctionner dans plusieurs déploiements simultanément, car ces derniers se font au niveau de l'interface.

La visibilité et le contrôle des applications et des utilisateurs fournis par App-ID et User-ID, combiné à l'examen des contenus réalisé par Content-ID, permettent aux services informatiques de prendre des décisions basées sur les risques qui protègent l'organisation contre les menaces, et sécurise les systèmes et les applications nécessaires au bon fonctionnement de l'entreprise.

Le tableau ci-dessous récapitule les différents types de politique pris en charge par la plateforme de sécurité nouvelle génération de Palo Alto Networks. Déterminez les fonctionnalités et les règles de politique que vous allez mettre en œuvre et dans quel ordre. Pour cela, hiérarchisez leur objectif par rapport aux priorités du centre de données de votre organisation, comme la durée de fonctionnement du système, la consommation de la bande passante ou les réglementations en matière de sécurité des données.

Guide de l'administrateur :

- Activation d'une politique basée sur l'utilisateur et le groupe
- Présentation d'App-ID
- Déploiements VM-Series
- Configuration des interfaces et des zones

PHASE 2 : VISIBILITÉ COMPLÈTE SUR LE TRAFIC DU CENTRE DE DONNÉES

Cette étape a pour objectif d'identifier et de valider toutes les communications applicatives entrant dans le centre de données et en sortant. Lorsque vous installez la plateforme de sécurité nouvelle génération pour la première fois, nous vous recommandons de commencer par la déployer en mode TAP.

Ce modepermet de surveiller passivement et sans heurt le trafic réseau, mais sans prévenir ni bloquer de connexions. Il est ainsi possible de surveiller le trafic nord-sud et est-ouest dans le centre de données et d'en établir un profil en fonction des applications, des menaces et de l'utilisation du trafic, sans interrompre le trafic de production. L'examen du trafic et des journaux des menaces générés en mode TAP permet également de vérifier les applications, les utilisateurs et les menaces qui ont été identifiés lors de l'analyse préalable des documents et des configurations existantes.

La collecte et l'analyse du trafic réseau peuvent vous aider à établir rapidement le profil de l'environnement et à détecter les menaces en temps réel. À partir de ces données, vous pouvez rapidement générer des rapports personnalisés et dresser une analyse du cycle de vie de sécurité comprenant les éléments suivants :

- Identification des applications
- Nombre de sessions et volume de bande passante associée consommée avec chaque application
- Adresses source et de destination
- Portée complète des menaces inconnues observées
- Pourcentage de logiciels malveillants détectés par la plateforme et non par les solutions antivirus tierces
- Menaces persistantes avancées et logiciels malveillants de type « zero-day » identifiés par Palo Alto Networks WildFire
- Vecteurs de menaces au niveau des applications et les types de fichiers malveillants
- Comportements utilisateur dangereux

Une fois les données du trafic réseau du centre de données collectées et analysées, vous pouvez créer des alertes pour les menaces les plus courantes. Vous pourrez ainsi analyser votre environnement de façon plus approfondie grâce à des fonctionnalités de création de rapports et de détermination des tendances visant à valider le trafic. Vous pourrez alors entamer le processus plus complet et complexe de développement de politiques.

Lorsque suffisamment de données auront été collectées, reconfigurez la plateforme en mode VWire ou Couche 2 (L2) / Couche 3 (L3) pour commence à intervenir sur le trafic indésirable et à risque.

VWire permet d'appliquer différentes politiques pour gérer le trafic provenant de plusieurs réseaux internes, et pour le segmenter et le classer en différentes zones. Sur une base logique, cette configuration isole l'environnement de ressources stratégiques des autres systèmes moins critiques. En mode VWire, la plateforme est installée de façon transparente sur un segment de réseau en reliant deux ports entre eux. L'installation et la configuration sont ainsi simplifiées et ne nécessitent aucune modification des appareils réseau adjacents. Les commutateurs de distribution et/ou centraux du centre de données sont configurés de façon à acheminer uniquement le

Conseil : Pour évaluer le trafic sans procéder à un fastidieux examen manuel des journaux, élaborez des rapports personnalisés comme ceux couvrant les principales applications et règles de sécurité, et le trafic répondant à la règle de sécurité de collection de type « tout autoriser ». Ces rapports fournissent une référence historique des données qui vous permet, ainsi qu'à votre équipe, de dresser constamment le profil du trafic entrant dans votre centre de données et en sortant.

Conseil : Le classement des règles est essentiel pour garantir des critères de correspondance optimaux. Étant donné qu'une politique est évaluée de haut en bas, la politique la plus spécifique doit précéder les plus générales. Une règle de niveau inférieur n'est pas évaluée si une règle qui la précède répond aux critères de correspondance.

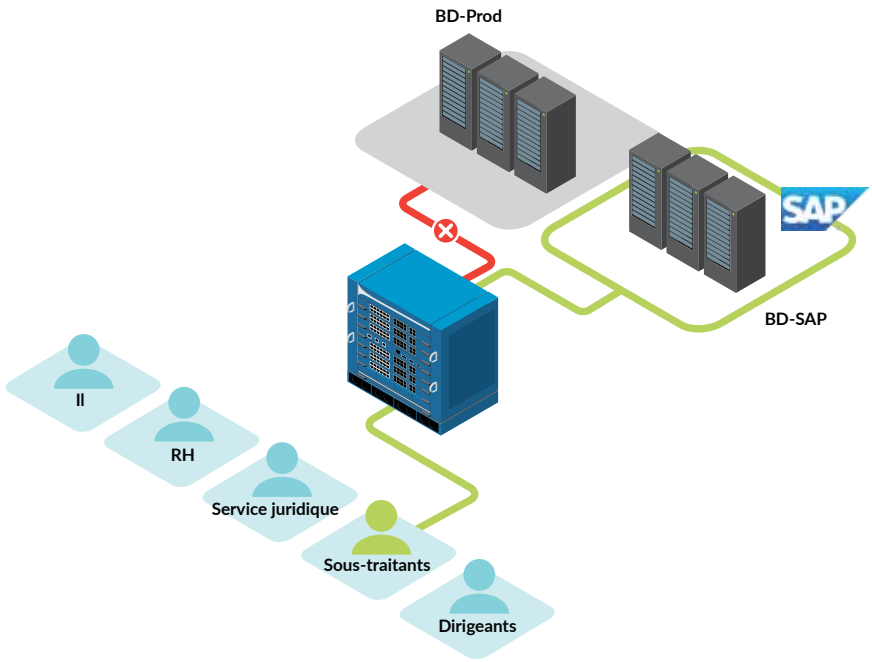
trafic de données stratégiques pertinent à la plateforme (via des VLAN). L'environnement peut ainsi gérer ses VLAN et l'adressage IP. Le mode VWire réachemine l'ensemble du trafic via la plateforme pour permettre le développement initial de politiques et surveiller le trafic entrant dans l'environnement et en sortant.

Utilisez les informations collectées pour développer une politique de sécurité initiale qui décrit les accès autorisés, notamment les sources, les réseaux de destination, les applications et les groupes d'utilisateurs approuvés. Créez ensuite des règles de sécurité pour les communications entrant dans le centre de données et en sortant sur la base de regroupements d'applications connues similaires, notamment de base de données, Web, Microsoft, de gestion et d'infrastructure.

Vous pourrez ainsi développer un large cadre de politique de sécurité qui vous aidera à classer les applications approuvées. Appliquez des profils de protection contre les menaces à toutes les règles pour bénéficier d'une meilleure visibilité sur la sécurité. Vous serez ainsi mieux armé pour bloquer les exploitations, les logiciels malveillants et le trafic de commande et contrôle sans altérer les communications professionnelles.

Pour ne bloquer aucune communication vitale lorsque vous développez et testez votre politique de centre de données, appliquez à la fin de la pyramide de règles de sécurité une règle de collecteur de type « tout autoriser » qui autorise explicitement toutes les communications qui ne sont pas encore rattachées à une règle.

Examinez ensuite plus particulièrement les applications qui n'utilisent pas de port ou de protocole non standard, ou les applications inconnues. Celles-ci ne doivent être autorisées qu'après validation par le propriétaire du système. Les règles d'applications validées doivent être ajoutées avant la règle de collection dans la hiérarchie pour une action sécurisée et un développement logique des règles.



Avant la fin de cette phase, la politique de sécurité inclut normalement l'ensemble des applications, ports, protocoles, réseaux source et de destination identifiés et approuvés, et les utilisateurs et groupes d'utilisateurs autorisés à y accéder. L'intégralité du trafic approuvé est alors identifiée par une application grâce à une politique de sécurité spécifique.

Seul le trafic non approuvé déclenchera la règle de collection. Vous pourrez alors l'examiner, le valider et créer une autre règle pour l'autoriser plus spécialement. Enfin, pour appliquer une protection active, abandonnez le système d'alerte simple au profit d'un blocage actif des menaces connues. Pour cela, ajoutez des profils de sécurité à votre ensemble de règles.

Remplacez la règle de collection par une nouvelle règle de type « tout refuser » au bas de la liste des politiques, qui soit configurée pour bloquer et consigner le trafic refusé. L'abandon d'une approche basée sur des listes noires au profit d'une approche s'appuyant sur des listes blanches permet au système de refuser le trafic qui n'a pas été explicitement autorisé tout en optimisant la visibilité et la prévention des menaces. À ce stade, vous pouvez abandonner la plateforme de sécurité héritée.

Conseil : le classement des règles est essentiel pour garantir des critères de correspondance optimaux. Étant donné qu'une politique est évaluée de haut en bas, la politique la plus spécifique doit précéder les plus générales. Une règle de niveau inférieur n'est pas évaluée si une règle qui la précède répond aux critères de correspondance.

Conseil : comme différents niveaux d'encodagepeuvent être employés comme technique d'évasion, utilisez l'encodage sur plusieurs niveaux pour que les fichiers non identifiés dans lesquels les menaces n'ont pas été recherchées ne traversent pas le pare-feu dans le but d'atteindre votre centre de données.

Guide de l'administrateur :

- Surveillance
- Composants d'une règle de sécurité
- Comment configurer un appareil Palo Alto Networks pour le mode TAP
- Configuration des profils et politiques de sécurité
- Décryptage
- Déploiements de câble virtuel
- Génération de rapports personnalisés

PHASE 3 : SÉCURITÉ AVANCÉE DU CENTRE DE DONNÉES

Après avoir configuré votre plateforme de sécurité de base, vous pouvez commencer à générer d'autres rapports spécifiques, à affiner des règles de politique et à mettre en œuvre des fonctionnalités de prévention supplémentaires. Vous pouvez, par exemple, appliquer des profils de sécurité stricts, WildFire™, l'environnement cloud d'analyse des logiciels malveillants, GlobalProtect™, le service de sécurité de la main-d'œuvre mobile et Traps™, le service de protection avancée des terminaux.

Activez le transfert de fichiers vers WildFire pour vous assurer que les fichiers inconnus, et plus particulièrement les types de fichiers utilisés dans le cadre professionnel comme les fichiers Microsoft Office et Adobe® Acrobat®, ne contiennent aucune menace persistante avancée (APT) ni aucun logiciel malveillant de type « zero-day ». WildFire analyse les fichiers inconnus, puis génère des protections contre les logiciels malveillants, le trafic de commande et contrôle, et les URL malveillantes quand un fichier est supposé malveillant.

WildFire exécute le contenu suspect dans plusieurs versions de l'application cible située au sein de systèmes d'exploitation virtualisés. Par ailleurs, il identifie des centaines de comportements associés à des logiciels malveillants comme des modifications de l'hôte, un trafic réseau suspect et des techniques d'évasion anti-analyse. À l'instar des protections des applications, ces comportements sont également accompagnés d'un rapport qui peut ensuite être utilisé pour identifier de façon positive les systèmes infectés.

Si certains de vos actifs communiquent en externe dans une capacité ou une autre, configurez des profils de filtrage des URL pour les règles applicables afin de bénéficier d'un niveau de sécurité supplémentaire. Ainsi, vos actifs ne pourront plus communiquer avec des URL malveillantes et très risquées.

Activez GlobalProtect sur les téléphones et ordinateurs portables professionnels des utilisateurs afin de les identifier autrement qu'avec leur adresse IP quand ils tentent d'accéder à distance aux ressources stratégiques de l'entreprise. Étendez également les protections de sécurité sur votre plateforme quand ces appareils sont déconnectés du réseau, et vérifiez que leur connexion au centre de données est sécurisée.

GlobalProtect est une source User-ID™ qui renforce la portée de la plateforme de sécurité, quel que soit l'endroit où se trouvent les utilisateurs. Ce service s'assure également que l'accès aux ressources stratégiques stockées dans votre centre de données est en permanence conforme à la politique de sécurité en place.

Déployez une protection avancée des terminaux Traps sur tous les serveurs Windows et dans l'infrastructure de bureau virtuelle (VDI) exécutés dans votre centre de données afin de bénéficier d'un niveau de protection supplémentaire contre les exploitations. Traps est un agent qui prévient les exploitations de vulnérabilité de type « zero-day » et les attaques par des logiciels malveillants sans signature. Il empêche ainsi la violation des ressources de votre centre de données.

L'agent Traps s'introduit dans chaque processus à son démarrage et se concentre sur les principales techniques qu'un attaquant doit lier pour opérer une attaque. Si le processus tente d'exécuter l'une des principales techniques d'attaque, Traps bloque immédiatement cette dernière, termine le processus et avertit l'administrateur qu'une attaque a été déjouée.

Conseil : Configurez votre plateforme pour importer toutes les cinq minutes les mises à jour de sécurité depuis WildFire.

Conseil : Utilisez la fonctionnalité de listes dynamiques externes pour déjouer les attaquants en important les adresses IP source de pirates récurrents qui apparaissent dans vos journaux des menaces au cours d'une période, puis bloquez-les pendant 24 heures ou plus.

Guide de l'administrateur :

- Déploiements de réseaux privés virtuels
- Filtrage des URL
- Activation du transfert WildFire de base
- Utilisation d'une liste dynamique externe dans une politique

Notre engagement envers nos clients

Palo Alto Networks s'attache à assurer la réussite des déploiements de ses clients et fournit à cet effet une assistance complète via nos services client mondiaux. Un échec n'est effectivement pas concevable. Nos offres d'assistance et nos programmes de formation ont été conçus pour limiter les problèmes de déploiement que vous pourriez avoir.

- Services d'assurance de systèmes de Palo Alto Networks
- Programmes d'assistance client de Palo Alto Networks
- Services de conseil de Palo Alto Networks
- Services d'enseignement de Palo Alto Networks

Rejoignez la communauté LIVE de Palo Alto Networks pour prendre part à des discussions entre utilisateurs, et consulter des tutoriels et des articles de la base de connaissances.

- Guide de l'administrateur PAN-OS Version 7.1 – Panorama
- Guide de l'administrateur PAN-OS Version 7.0 – Panorama
- Guide de l'administrateur PAN-OS Version 6.1 – Panorama

fuel
PALO ALTO NETWORKS
USER GROUP

Rejoignez la communauté Fuel User Group de Palo Alto Networks pour échanger avec des professionnels du monde entier qui consentent à présenter leurs meilleures pratiques et renseignements commerciaux durement gagnés. Vous pouvez également obtenir des réponses à vos problématiques de sécurité auprès d'experts en la matière au cours d'événements en ligne comme des webinaires et des sessions de questions/réponses, ou encore de discussions individualisées.

paloalto NETWORKS

4401 Great America Parkway Santa Clara, CA 95054

Accueil téléphonique : +1.408.753.4000
Service commercial : +1.866.320.4788
Assistance : +1.866.898.9087

www.paloaltonetworks.com