Vue d'ensemble du pare-feu nouvelle génération Palo Alto Networks

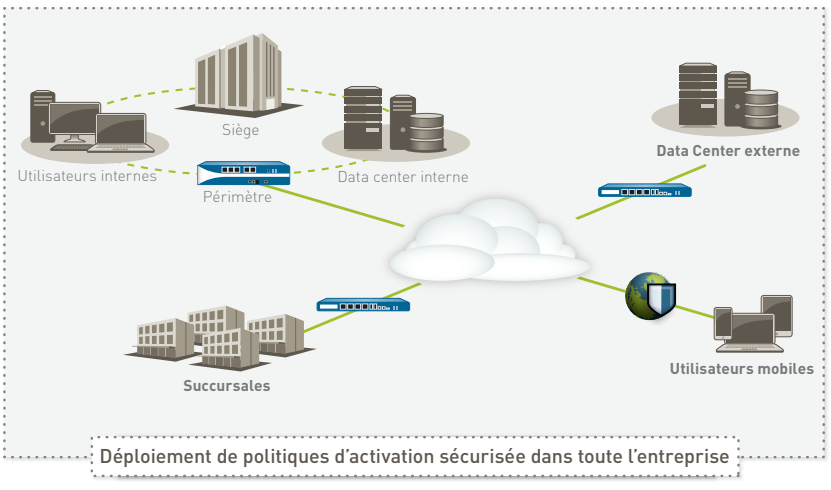
L'évolution du paysage des applications et des menaces, du comportement des utilisateurs et de l'infrastructure réseau a peu à peu érodé la sécurité qu'offraient les pare-feu traditionnels fondés sur les ports. Pour effectuer leur travail, les utilisateurs doivent désormais accéder à tous types d'applications via une grande variété de dispositifs. Parallèlement, le développement des data centers, la virtualisation, la mobilité et les initiatives basées sur le cloud vous obligent à repenser la façon d'autoriser l'accès aux applications sans mettre en péril votre réseau.

La solution classique consiste à bloquer le trafic de l'ensemble des applications en utilisant conjointement au pare-feu un nombre sans cesse croissant de technologies spécialisées risquant de nuire à votre activité ; ou au contraire d'autoriser toutes les applications, compromis tout aussi inacceptable en raison de l'accroissement des risques de sécurité et commerciaux que cela implique. Bien que garantissant un niveau de blocage élevé des applications, votre pare-feu traditionnel basé sur les ports, n'offre aucune alternative satisfaisante à ces deux approches. Pour atteindre un équilibre entre un accès complètement ouvert et un blocage total, vous devez mettre en œuvre une utilisation sécurisée des applications en basant vos politiques de sécurité sur des éléments pertinents, tels que l'identification de l'application, des utilisateurs et du type de contenu.

Conditions essentielles à une activation sécurisée des applications :

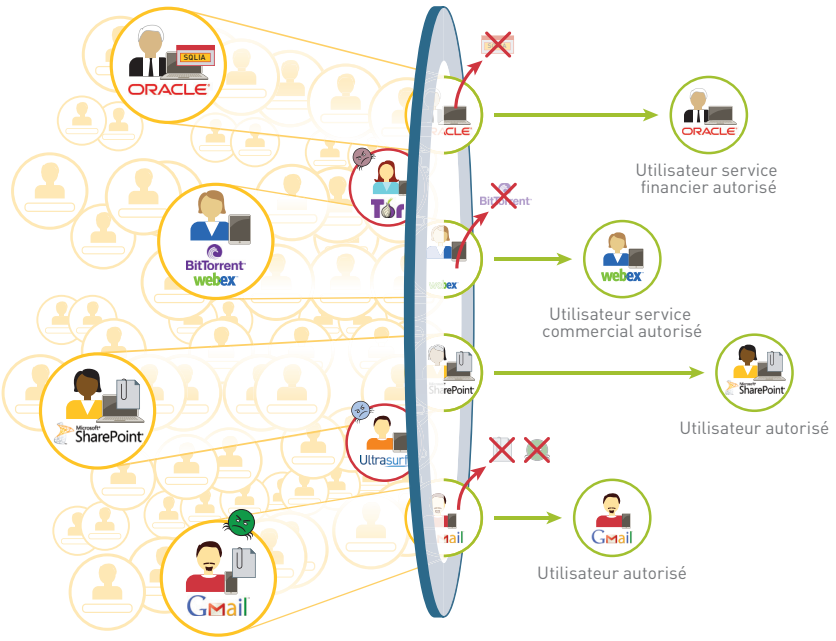
- **Identifier des applications, et non des ports.** Classification du trafic dès qu'il atteint le pare-feu pour déterminer l'identité de l'application, indépendamment du protocole, du chiffrement ou de la technique d'évasion. Utilisation par la suite de cette identité comme base de toutes les politiques de sécurité.
- **Identifier des utilisateurs, et non des adresses IP.** Utilisation des informations de groupes et d'utilisateurs stockées dans les annuaires d'entreprise et autres magasins d'utilisateurs pour déployer des politiques d'utilisation cohérentes pour tous les utilisateurs, indépendamment de leur emplacement ou de leur équipement.
- **Bloquer toutes les menaces - connues et inconnues.** Protection contre les vulnérabilités, les logiciels malveillants, les logiciels espions et les URL à haut risque connus tout en assurant une protection contre les logiciels malveillants jusqu'à là inconnus et hautement ciblés.
- **Simplifier la gestion des politiques.** Utilisation sûre et sécurisée des applications et réduction des contraintes administratives grâce à des outils graphiques, à un éditeur de politiques unifié, à des modèles et à un regroupement des équipements.

Les politiques d'utilisation sécurisée des applications permettent d'atteindre un niveau accru de sécurité, indépendamment du lieu de déploiement. En périphérie, vous pouvez réduire les risques en bloquant une grande variété d'applications indésirables et en détectant d'éventuelles menaces, connues ou inconnues, dans les applications autorisées.



paloalto NETWORKS
the network security company™

CONTRÔLE TOTAL DES APPLICATIONS, DES UTILISATEURS ET DU CONTENU



Au niveau du data center (physique ou virtuel), l'activation sécurisée des applications consiste à s'assurer que seules les applications du data center sont accessibles aux utilisateurs autorisés afin de protéger le contenu et répondre au défi posé par la nature dynamique d'une infrastructure virtuelle. Les utilisateurs distants et les filiales de votre entreprise sont protégés par les mêmes politiques de sécurité que celles déployées au siège, garantissant par là-même une cohérence stratégique.

Une activation sécurisée des applications pour renforcer le pouvoir de l'entreprise

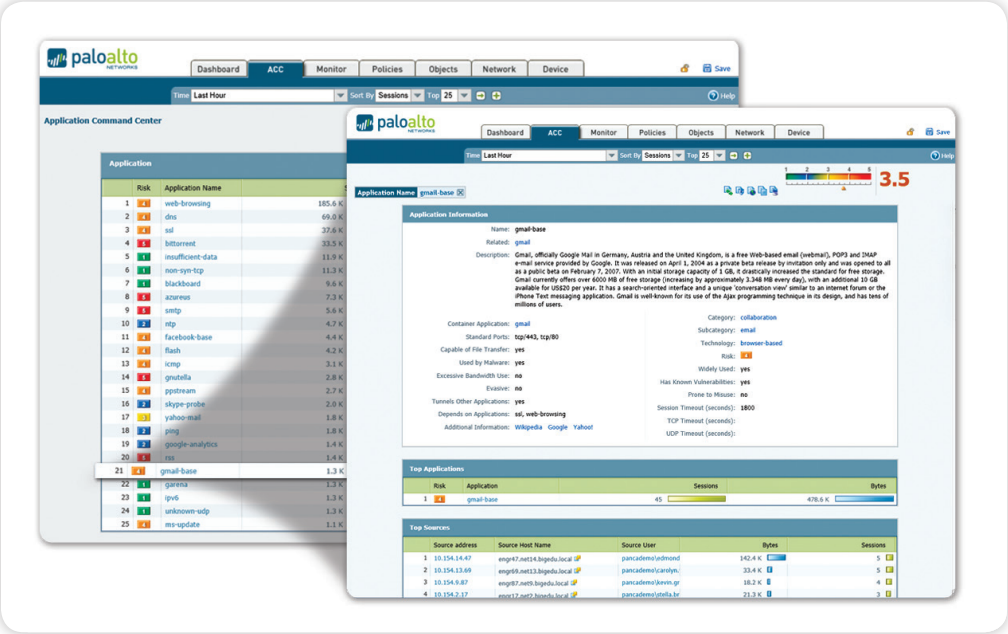
En permettant l'activation sécurisée des applications, les pare-feu nouvelle génération de Palo Alto Networks vous aident à gérer les risques associés au nombre croissant d'applications franchissant votre réseau. En autorisant l'accès aux applications à des utilisateurs ou groupes d'utilisateurs locaux, nomades ou distants et en protégeant le trafic contre les menaces connues et inconnues, vous pouvez renforcer votre sécurité tout en développant votre activité.

- **Classification systématique de toutes les applications, sur tous les ports.** Une reconnaissance précise du trafic est au cœur de tout pare-feu, le résultat constituant la base de la stratégie de sécurité. Aujourd'hui, les applications abusent facilement des pare-feu fondés sur les ports à l'aide de techniques telles que le saut de ports, l'utilisation de SSL et de SSH, l'attaque furtive sur le port 80 ou l'utilisation de ports non standard. App-ID résout le problème de visibilité réduite qui affecte la classification du trafic et handicape les pare-feu traditionnels. Grâce à l'application de plusieurs mécanismes de reconnaissance du trafic, le pare-feu détermine l'identité exacte des applications qui transitent par le réseau, indépendamment du port, du chiffrement (SSL ou SSH) ou de la technique d'évasion. Toutes vos décisions stratégiques en matière de sécurité reposent désormais sur l'identification précise des applications qui traversent votre réseau. Les applications non identifiées, qui ne représentent qu'un faible pourcentage du trafic mais constituent un risque potentiel élevé, sont automatiquement classifiées et font l'objet d'une gestion systématique avec notamment des inspections et des contrôles stratégiques, l'analyse des menaces, la création d'une App-ID personnalisée ou la capture de paquets pour le développement d'une App-ID Palo Alto Networks.

- **Intégration des utilisateurs et des équipements dans les politiques de sécurité.** La création et la gestion de politiques de sécurité basées sur l'application et l'identité de l'utilisateur, indépendamment de l'emplacement géographique et du dispositif utilisé, garantit une meilleure protection du réseau que la simple identification du port et de l'adresse IP. L'intégration à un large éventail de référentiels d'utilisateurs permet d'identifier les utilisateurs Microsoft Windows, Mac OS X, Linux, Android ou iOS qui accèdent aux applications. Les utilisateurs nomades ou distants sont protégés de manière transparente par le même ensemble de politiques cohérentes que celui mis en œuvre sur le réseau local de l'entreprise. Grâce à la visibilité et au contrôle combinés de l'activité des applications d'un utilisateur, vous pouvez autoriser l'utilisation sécurisée d' Oracle, BitTorrent ou Gmail ou de toute autre application traversant votre réseau, quels que soient l'endroit où se trouve l'utilisateur et son mode d'accès.
- **Bloquer toutes les menaces, connues et inconnues.** La protection des réseaux modernes nécessite de lutter aussi bien contre des vulnérabilités, des logiciels malveillants et des logiciels espions connus que contre des menaces ciblées totalement inconnues. Pour cela, il est nécessaire dans un premier temps de réduire la surface d'attaque de votre réseau en autorisant certaines applications et en refusant toutes les autres, de manière implicite par le bais d'une stratégie du type « refuser tout le reste » ou de stratégies explicites. Une prévention coordonnée des menaces peut alors être appliquée à l'ensemble du trafic autorisé pour bloquer en une seule passe les sites à haut risque, les vulnérabilités, les virus, les logiciels espions et les requêtes DNS malveillantes. Les logiciels malveillants personnalisés ou inconnus sont analysés et identifiés en exécutant les fichiers inconnus et en observant directement plus de 100 comportements malveillants dans un environnement de test virtuel. Lorsque de nouveaux logiciels malveillants sont détectés, le pare-feu génère automatiquement une signature du fichier infecté et du trafic associé et vous l'envoie. Le processus d'analyse de prévention des menaces utilise le contexte des applications et des protocoles pour garantir le blocage systématique de toutes les menaces, y compris celles qui tentent de se dissimuler dans des tunnels, dans du contenu compressé ou sur des ports non standard.

Une grande souplesse de déploiement et de gestion

La fonctionnalité d'activation sécurisée des applications est disponible aussi bien sur les plateformes matérielles dédiées que sur les machines virtuelles. Si vous déployez plusieurs pare-feu Palo Alto Networks, matériels ou virtuels, vous pouvez utiliser la solution de gestion centralisée Panorama pour avoir une meilleure visibilité des modèles de trafic, déployer des politiques, générer des rapports et diffuser des mises à jour de contenu depuis un emplacement central.



Visibilité des applications : Affichez la cartographie des applications dans un format clair et lisible. Ajoutez et supprimez des filtres pour en savoir plus sur l'application, ses fonctions et leurs utilisateurs

Activation sécurisée des applications : une approche globale

Une utilisation sûre des applications passe par une approche globale de la sécurisation de votre réseau et du développement de votre activité qui commence par une parfaitement connaissance des applications qui résident sur votre réseau, des utilisateurs (indépendamment de leur emplacement ou de leur plateforme) et le cas échéant, du contenu. Grâce à une meilleure connaissance de l'activité du réseau, vous pourrez créer des politiques de sécurité plus pertinentes et plus cohérentes avec votre activité basées sur les applications, les utilisateurs et le contenu. L'emplacement des utilisateurs, la plateforme utilisée et le lieu de déploiement de la politique – périphérie, data center physique ou virtuel, filiale ou utilisateur distant - n'ont pas ou peu d'incidence sur la façon dont la stratégie est créée. Vous pouvez désormais autoriser en toute sécurité tout type d'application, d'utilisateur et de contenu.

Une connaissance approfondie pour des stratégies de sécurité plus strictes

Les pratiques d'excellence en matière de sécurité stipulent qu'une meilleure connaissance des éléments qui transitent sur votre réseau favorise la mise en œuvre de politiques de sécurité plus strictes. Par exemple, le fait de savoir précisément quelles applications traversent votre réseau permet aux administrateurs d'autoriser les applications dont votre entreprise a besoin, tout en bloquant les applications indésirables. L'identification conjointe de l'utilisateur et de son adresse IP permet une meilleure affectation des politiques de sécurité.

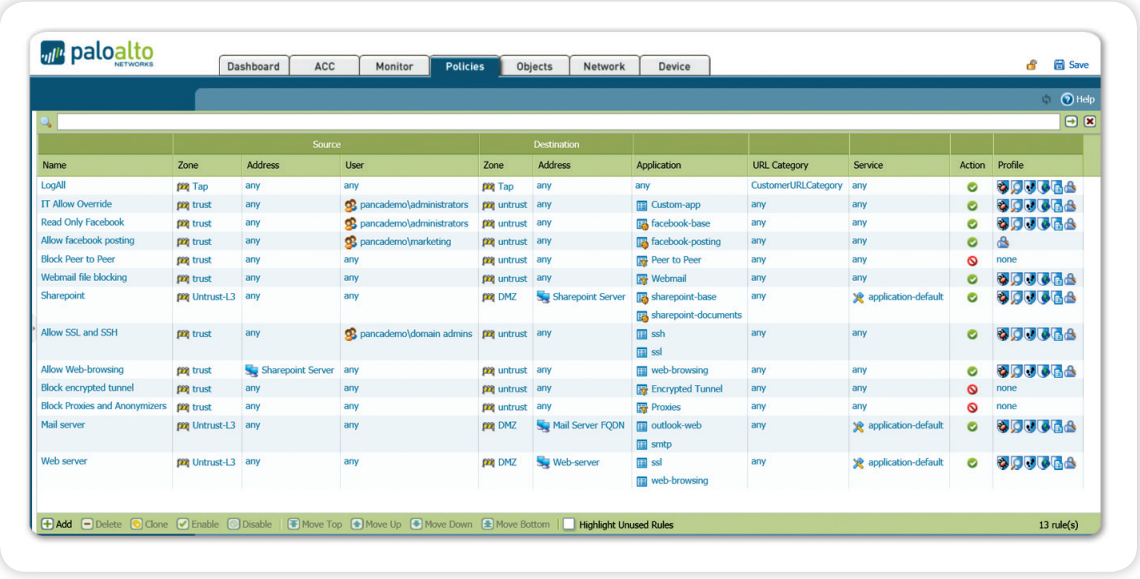
- Grâce à de puissants outils graphiques, les administrateurs bénéficient d'une meilleure visibilité de l'activité des applications et de leur impact sur la sécurité et peuvent ainsi prendre des décisions stratégiques mieux informées. Les applications sont continuellement analysées et les synthèses graphiques consultables dans une interface Web conviviale sont mises à jour à mesure que l'état des applications change.
- D'un simple clic, vous pouvez facilement afficher une description des applications nouvelles ou inconnues, ainsi que leurs caractéristiques comportementales, et savoir qui les utilise.
- Une visibilité supplémentaire des catégories d'URL, des menaces et des modèles de données offre une analyse complète et globale de l'activité du réseau.
- Les applications inconnues, qui représentent un faible pourcentage du trafic mais constituent un risque potentiel élevé, sont analysée pour déterminer s'il s'agit d'applications internes, telles que des applications commerciales qui n'ont pas encore été identifiées ou de menaces.

Utilisation sécurisée des applications et réduction des risques

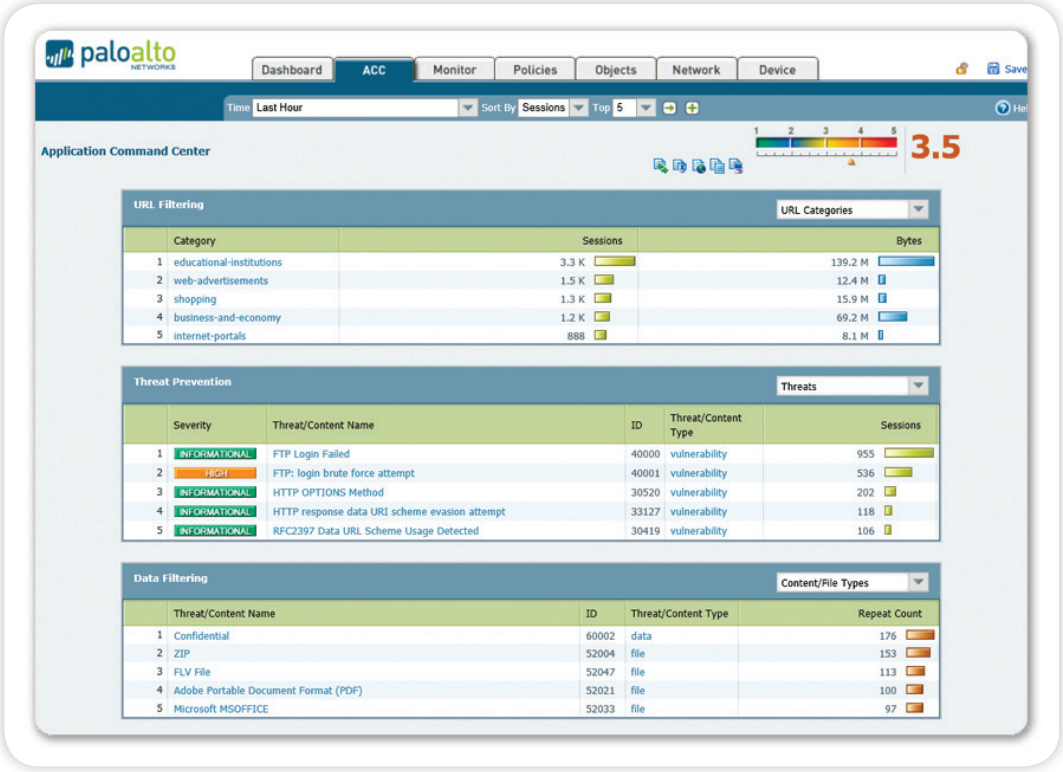
L'activation sécurisée des applications repose sur des critères de décisions stratégiques tels que les applications et leurs fonctionnalités, les utilisateurs, les groupes et le contenu pour atteindre un point d'équilibre entre le blocage total de toutes les applications, solution néfaste à votre activité et l'alternative très risquée d'autoriser toutes les applications.

En périphérie, notamment au niveau des filiales et des utilisateurs nomades ou distants, les politiques d'activation des applications sont principalement axées sur l'identification du trafic, puis sur l'autorisation sélective de celui-ci en fonction de l'identité de l'utilisateur et pour finir sur son analyse pour la détection des menaces potentielles. Quelques exemples de politiques :

- Limiter l'utilisation des messageries Web et instantanées à quelques variantes ; identifier les applications qui utilisent SSL, inspecter le trafic pour détecter d'éventuelles exploitations de vulnérabilités et charger les fichiers inconnus dans WildFire pour les analyser et créer des signatures.
- Autoriser les sites Web et les applications multimédias de diffusion vidéo tout en mettant en œuvre des stratégies de qualité de service et de prévention des logiciels malveillants afin de limiter l'impact sur les applications VoIP et protéger le réseau.
- Contrôler le trafic Facebook en bloquant l'accès aux jeux et aux modules sociaux et en autorisant la publication de messages Facebook uniquement à des fins de marketing. Analyser le trafic Facebook afin de détecter les logiciels malveillants et l'exploitation de failles.
- Contrôler la navigation sur le Web en autorisant et en analysant le trafic vers des sites Web associés aux activités de l'entreprise, tout en bloquant l'accès aux sites n'ayant aucun lien manifeste avec l'activité de l'entreprise. Les pages de blocage personnalisées peuvent guider l'accès aux autres sites.
- Mettre en œuvre une politique de sécurité cohérente en déployant de manière transparente les mêmes politiques à tous les utilisateurs, locaux, nomades ou distants, via GlobalProtect.
- Utiliser une stratégie implicite du type « refuser tout le reste » ou bloquer explicitement les applications indésirables, telles que le partage de fichiers P2P et les services de type circumventor ou refuser le trafic en provenance de pays spécifiques afin de réduire le trafic représentant un risque de sécurité et commercial.



Éditeur de stratégies unifié : Une interface simple permet de creer et deployer rapidement des strategies qui controlent les applications, les utilisateurs et le contenu.



Visibilité du contenu et des menaces : Affichez l'activité de transfert de données/fichiers, de menaces et d'URL dans un format clair et facile à lire. Ajoutez et supprimez des filtres pour en savoir plus sur des éléments individuels.

Au niveau du data center (qu'il soit physique, virtuel ou une combinaison des deux), la mise en œuvre de l'activation sécurisée des applications repose sur la validation des applications, la recherche d'applications douteuses et la protection des données.

- Isoler le référentiel des numéros de cartes bancaires Oracle dans une zone sécurisée ; contrôler l'accès aux services financiers en forçant le trafic à transiter par les ports standard et en inspectant le trafic pour y rechercher des failles dans les applications.
- Autoriser uniquement le service informatique à accéder au data center via un ensemble donné d'applications de gestion à distance (par exemple, SSH, RDP, Telnet) via leurs ports standard.
- Limiter l'utilisation de Microsoft SharePoint Administration à la seule équipe d'administration et autoriser l'accès aux documents Microsoft SharePoint à tous les autres utilisateurs.

Protection des applications utilisées

L'activation sécurisée des applications consiste à autoriser l'accès à certaines applications, puis à appliquer des politiques spécifiques pour bloquer les vulnérabilités, les logiciels malveillants et les logiciels espions, connus ou inconnus, et à contrôler les transferts de fichiers ou de données et la navigation sur le Web. Les techniques d'évasion courantes, telles que la mise sous tunnel et le saut de ports, sont esquivées en exécutant les politiques de prévention des menaces en fonction des informations fournies par les décodeurs de protocoles d'App-ID. En revanche, les solutions UTM adoptent une approche cloisonnée de la prévention des menaces où chaque fonctionnalité, pare-feu, système de prévention d'intrusion, antivirus et filtrage d'URL analyse le trafic sans aucun partage de contexte, ce qui les rend plus vulnérables aux comportements d'évasion.

- **Bloquer les menaces connues : système de prévention d'intrusion et logiciel antivirus/ anti-espions réseau.** Un format de signature uniforme et un moteur d'analyse basé sur le flux vous permettent de protéger votre réseau contre une vaste gamme de menaces. Les fonctions de prévention des intrusions (IPS) empêchent les failles de sécurité au niveau du réseau et de l'application, les dépassements de mémoire tampon, les attaques par refus de service et les attaques

par analyse des ports. La protection par antivirus et anti-espions bloque des millions de logiciels malveillants, y compris les virus PDF et les programmes malveillants dissimulés dans les fichiers compressés ou dans le trafic Web (HTTP/HTTPS compressé). Le déchiffrement SSL stratégique appliqué à toutes les applications, sur tous les ports, vous protège contre les logiciels malveillants qui circulent via les applications chiffrées en SSL.

- **Bloquer les logiciels malveillants ciblés et inconnus : Wildfire™.** Les logiciels malveillants inconnus ou ciblés sont identifiés et analysés par WildFire, qui exécute et observe directement les fichiers inconnus dans un environnement de test virtuel basé sur le cloud. WildFire surveille le comportement de plus de 100 logiciels malveillants et communique immédiatement les résultats à l'administrateur sous forme d'alerte. Un abonnement - en option - à WildFire offre des fonctions de protection, de journal de log et de génération de rapports avancées. Avec WildFire, vous êtes protégé dans l'heure qui suit la détection d'un nouveau logiciel malveillant, sa propagation étant avortée avant qu'il n'ait le moindre impact sur votre activité. En tant qu'abonné, vous avez également accès aux fonctions de journal de log et de génération de rapports intégrées de WildFire, ainsi qu'à une API permettant l'envoi d'échantillons au cloud WildFire pour être analysés.
- **Identifier les hôtes infectés par des zombies.** App-ID classifie toutes les applications, sur tous les ports, y compris tout trafic inconnu, ce qui permet souvent de détecter des anomalies ou des menaces sur votre réseau. Le rapport comportemental de réseau de zombies met en corrélation le trafic inconnu, les requêtes d'URL ou DNS suspectes et toute une gamme de comportements anormaux du réseau afin d'identifier les équipements susceptibles d'être infectés par des logiciels malveillants. Les résultats sont affichés sous la forme d'une liste d'hôtes potentiellement infectés qui peuvent être étudiés en tant que membres possibles d'un réseau de zombies.
- **Limiter les transferts non autorisés de fichiers et de données.** Des fonctionnalités de filtrage de données permettent à vos administrateurs de mettre en œuvre des stratégies pour réduire les risques liés aux transferts non autorisés de fichiers et de données. Les transferts de fichiers peuvent être contrôlés par l'analyse du contenu (par opposition au seul examen de l'extension de fichier), afin d'autoriser ou non le transfert. Les fichiers exécutables, qui se trouvent habituellement dans les téléchargements automatiques, peuvent être bloqués, protégeant par là-même votre réseau contre toute propagation de logiciels malveillants non détectés. Enfin, les fonctions de filtrage des données peuvent détecter et contrôler le flux de modèles de données confidentielles (numéros de carte de crédit ou de sécurité sociale et modèles personnalisés).
- **Contrôler la navigation sur le Web.** Un moteur de filtrage des URL, totalement intégré et personnalisable, permet à vos administrateurs d'appliquer des politiques de navigation Web extrêmement précises parallèlement aux stratégies de contrôle et de visibilité des applications, protégeant ainsi votre entreprise contre un spectre étendu de risques en termes de loi, de réglementation et de productivité. De plus, les catégories d'URL peuvent être utilisées dans les politiques afin de fournir une plus grande précision du contrôle du déchiffrement SSL, de la qualité de service ou de tout autre élément de base des règles.

Une gestion et une analyse permanentes

Les pratiques recommandées en matière de sécurité stipulent que les administrateurs doivent trouver un point d'équilibre entre une gestion proactive du pare-feu - qu'il y ait un ou plusieurs centaines de dispositifs - et se montrer réactif, enquêter, analyser et signaler les incidents concernant la sécurité.

- **Gestion :** chaque plateforme Palo Alto Networks peut être gérée individuellement via une interface de ligne de commande (CLI) ou une interface Web complète. Pour les déploiements à grande échelle, Panorama peut être déployé sous licence comme solution de gestion centralisée permettant un contrôle global central avec néanmoins une certaine souplesse pour les stratégies locales, en utilisant des fonctionnalités telles que les modèles et les stratégies partagées. La prise en charge d'outils normalisés tels que les API REST ou SNMP permet l'intégration d'outils de gestion tiers. Les interfaces Web du boîtier et de Panorama sont identiques afin de faciliter le passage de l'une à l'autre. Vos administrateurs peuvent à tout moment utiliser l'une ou l'autre des interfaces pour effectuer des modifications, sans se préoccuper d'éventuels problèmes de synchronisation. La gestion basée sur les rôles est prise en charge sur l'ensemble des supports de gestion pour permettre l'affectation de fonctions et fonctionnalités à des utilisateurs donnés.
- **Création de rapports :** des rapports prédéfinis peuvent être utilisés tels quels, personnalisés ou regroupés dans un seul rapport afin de s'adapter aux exigences particulières. Tous les rapports peuvent être exportés au format CSV ou PDF et exécutés puis envoyés par courrier électronique en fonction d'un planning défini.
- **Journal de log :** le filtrage des journaux en temps réel facilite l'examen rigoureux et rapide de chaque session franchissant votre réseau. Les résultats du filtrage des journaux peuvent être exportés vers un fichier CSV ou envoyés à un serveur syslog pour un archivage hors connexion ou une analyse plus approfondie.

Des plateformes matérielles ou virtuelles dédiées

Palo Alto Networks offre une gamme complète de plateformes matérielles dédiées : de la plateforme PA-200 conçue pour les bureaux distants des entreprises, à la plateforme PA-5060 conçue pour les data centers à haut débit. L'architecture de la plateforme s'appuie sur un moteur logiciel à une seule passe et utilise un traitement spécifique à certaines fonctions pour la mise en réseau, la sécurité, la prévention et la gestion des menaces afin d'offrir les performances attendues. Les fonctionnalités de pare-feu disponibles sur les plateformes matérielles sont également disponibles sur les pare-feu virtuels de la série VM, vous permettant ainsi de sécuriser vos environnements informatiques virtuels ou de type cloud à l'aide des mêmes stratégies que celles appliquées à vos pare-feu de périmètre ou de bureaux distants.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Accueil : +1.408.573.4000
Ventes : +1.866.320.4788
Assistance : +1.866.898.9087

www.paloaltonetworks.com