Palo Alto Networks

La plateforme de sécurité de l'entreprise

La cyber criminalité connait une profonde métamorphose. L'ampleur et la sophistication des attaques ont atteint un niveau tel qu'elles sont aujourd'hui une préoccupation majeure pour les entreprises et les gouvernements. La consumérisation numérique, le cloud, la transformation digitale ou la mobilité sont devenus simultanément des usages fondamentaux et des vecteurs d'attaques toujours plus ciblées, complexes et lucratives. Comment briser la chaîne de frappe d'une cyber attaque sans freiner ces usages et l'activité de l'entreprise ?

paloalto NETWORKS®

Briser la chaîne de frappe des cyber attaques

Ne plus bloquer les applications mais **valider leur utilisation en toute sécurité**, ne plus simplement détecter les cyberattaques mais **bloquer leur déclenchement** : telle est la vision de Palo Alto Networks depuis 2005. Pour atteindre un tel but, une nouvelle approche était nécessaire. Une approche qui repense la cybersecurité et qui rompt avec l'infrastructure traditionnelle.

1. Augmenter la capacité à voir tout le trafic réseau
2. Etablir un contrôle positif des applications et des utilisateurs
3. Bloquer automatiquement toutes les cyber attaques connues
4. Etablir un système automatisé de fourniture immédiate de défense dès qu'une cyber attaque inconnue est détectée.

MIEL

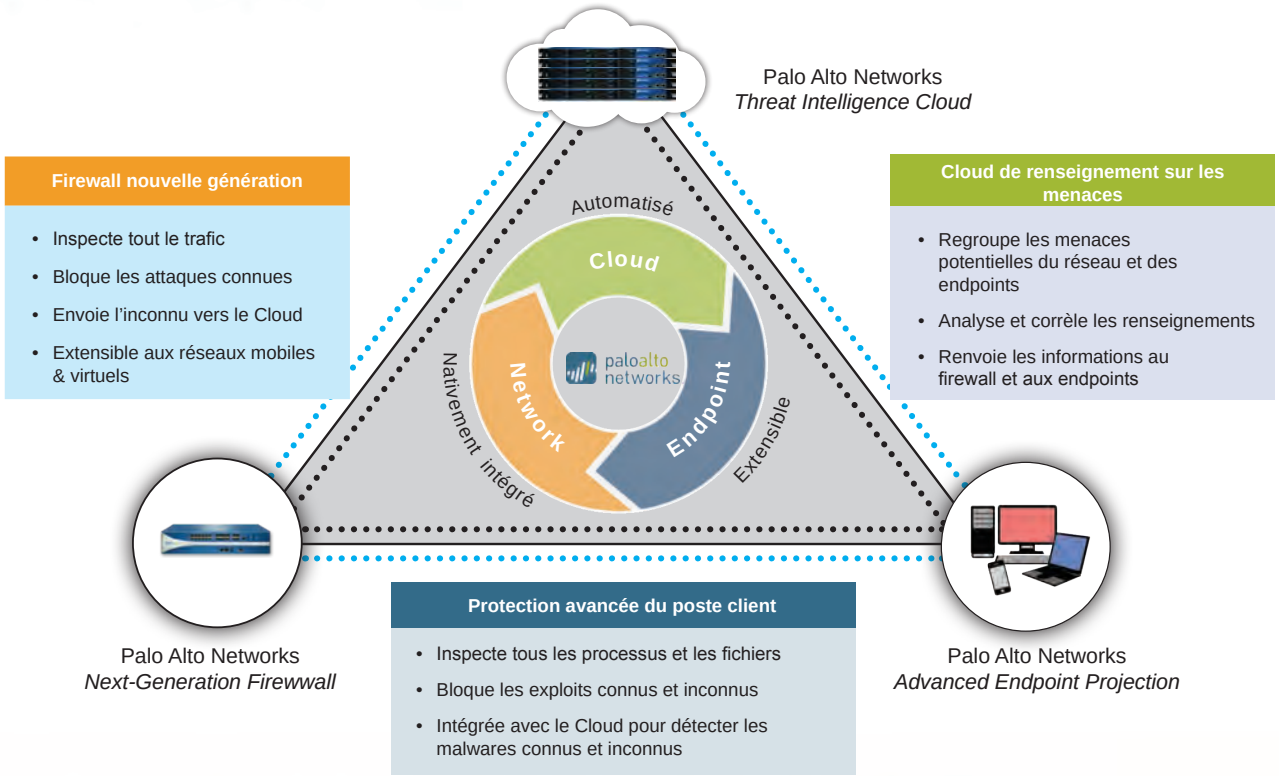
Distribution. Formation. Assistance. Appelez le 01 60 19 34 52

Une plateforme de sécurité intégrée : réseau, cloud et endpoint

La solution de Palo Alto Networks se compose de 3 éléments qui corrèlent leurs informations de détection et coordonnent leurs actions de protection :

- Les firewalls nouvelle génération
- Une intelligence dans le cloud, de renseignement sur les menaces
- Une protection avancée du poste client

Avec des partenaires stratégiques comme VMWare, Citrix, Arista ou Splunk, Palo Alto Networks propose **une plateforme de sécurité d'entreprise** qui protège tous les utilisateurs, tous les devices, sur tous les points du réseau et du data center.



Firewall nouvelle génération

- Inspecte tout le trafic
- Bloque les attaques connues
- Envoie l'inconnu vers le Cloud
- Extensible aux réseaux mobiles & virtuels

Cloud de renseignement sur les menaces

- Regroupe les menaces potentielles du réseau et des endpoints
- Analyse et corrèle les renseignements
- Renvoie les informations au firewall et aux endpoints

Palo Alto Networks
Next-Generation Firewall

Protection avancée du poste client

- Inspecte tous les processus et les fichiers
- Bloque les exploits connus et inconnus
- Intégrée avec le Cloud pour détecter les malwares connus et inconnus

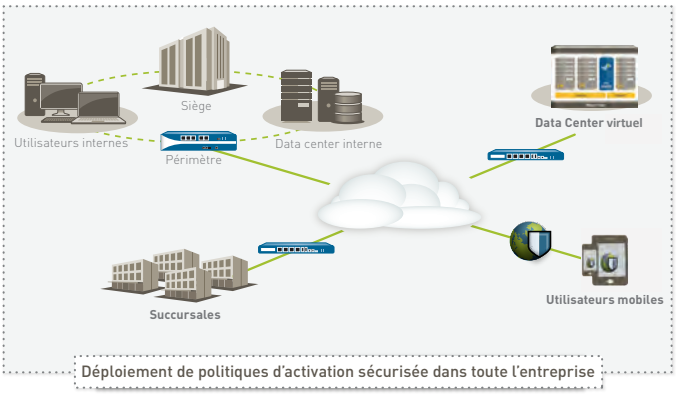
Palo Alto Networks
Advanced Endpoint Projection

Un FIREWALL NOUVELLE GENERATION au cœur du système

Ce fut la première solution proposée par Palo Alto Networks à partir de 2007 avec des critères fondamentaux qui restent aujourd'hui encore uniques dans la sécurité réseau :

- Une visibilité inégalée de toutes les applications en une seule analyse, indépendamment du port, du protocole ou du chiffrement SSL. Le firewall nouvelle génération détermine si le contenu de l'application est malveillant ou autre, et associe le trafic à l'identité de l'utilisateur, indépendamment de son adresse IP, son poste de travail ou son emplacement.
- Des contrôles de sécurité positifs qui valident les vrais utilisateurs et la vraie nature des applications, réduisant considérablement la surface d'attaque et éliminant une exposition inutile à de nombreux risques.
- Une augmentation de l'efficacité de la sécurité en corrélant rapidement les événements dans un système unique à boucle fermée qui automatise les actions et applique un système de management commun à toute l'architecture.

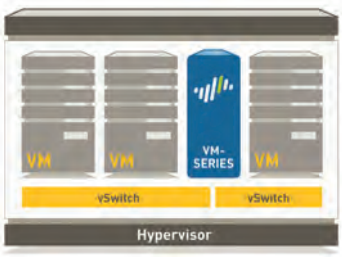
Palo Alto Networks propose une gamme complète d'appliances de sécurité nouvelle génération, depuis le PA-200 conçu pour les sites distants jusqu'au PA-7080, qui est un des chassis modulaires conçu pour les data centers haute performance. L'architecture de toutes les plate-formes est basée sur un moteur de traitement en parallèle et en un seul passage des fonctions de réseau, de sécurité et de protection contre les menaces , tout en décorrélant physiquement les ressources de management. Les performances sont ainsi "prédictibles" et garanties.

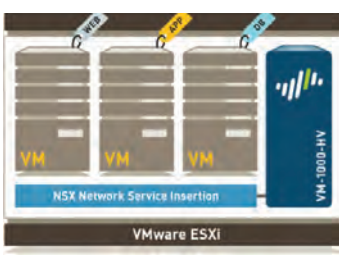


Les fonctionnalités fournies sur les plateformes matérielles sont identiquement disponibles dans les firewalls virtuels VM-Series, permettant la mise en place des mêmes principes et règles de sécurité dans un environnement virtuel. Le trafic entre les VMs et les ressources basées dans le Cloud bénéficient d'un niveau de sécurité inégalé.

Performance et capacités	PA-7080 SYSTEM	PA-705 SYSTEM	PA-5060	PA-5050	PA-5020	PA-3060	PA-3020	PA-3050	PA-500	PA-200
Débit Firewall (App-ID activé)	200 Gbps	120 Gbps	20 Gbps	10 Gbps	5 Gbps	4 Gbps	2 Gbps	4 Gbps	250 Mbps	100 Mbps
Débit Protection contre les menaces	100 Gbps	100 Gbps	10 Gbps	5 Gbps	2 Gbps	2 Gbps	1 Gbps	2 Gbps	100 Mbps	50 Mbps
Débit VPN IPSec	80 Gbps	24 Gbps	4 Gbps	4 Gbps	2 Gbps	500 Mbps	500 Mbps	500 Mbps	50 Mbps	50 Mbps
Nouvelles sessions par seconde	1 200,000	720,000	120,000	120,000	120,000	50,000	50,000	50,000	7,500	1,000
Nbre sessions max.	40 M	24 M	4,000,000	2,000,000	1,000,000	500,000	250,000	500,000	64,000	64,000

Performance et capacités	VM-1000-HV (NSX)	VM-300	VM-200	VM-100
Debit Firewall (App-ID activé)	1 Gbps			
Débit Protection contre les menaces	600 Mbps			
Débit VPN IPSec	250 Mbps			
Nouvelles sessions par seconde	8,000			
Nbre sessions Max	250,000	250,000	100,000	50,000
tunnels VPN IPSec / interfaces tunnel	2,000	2,000	500	25



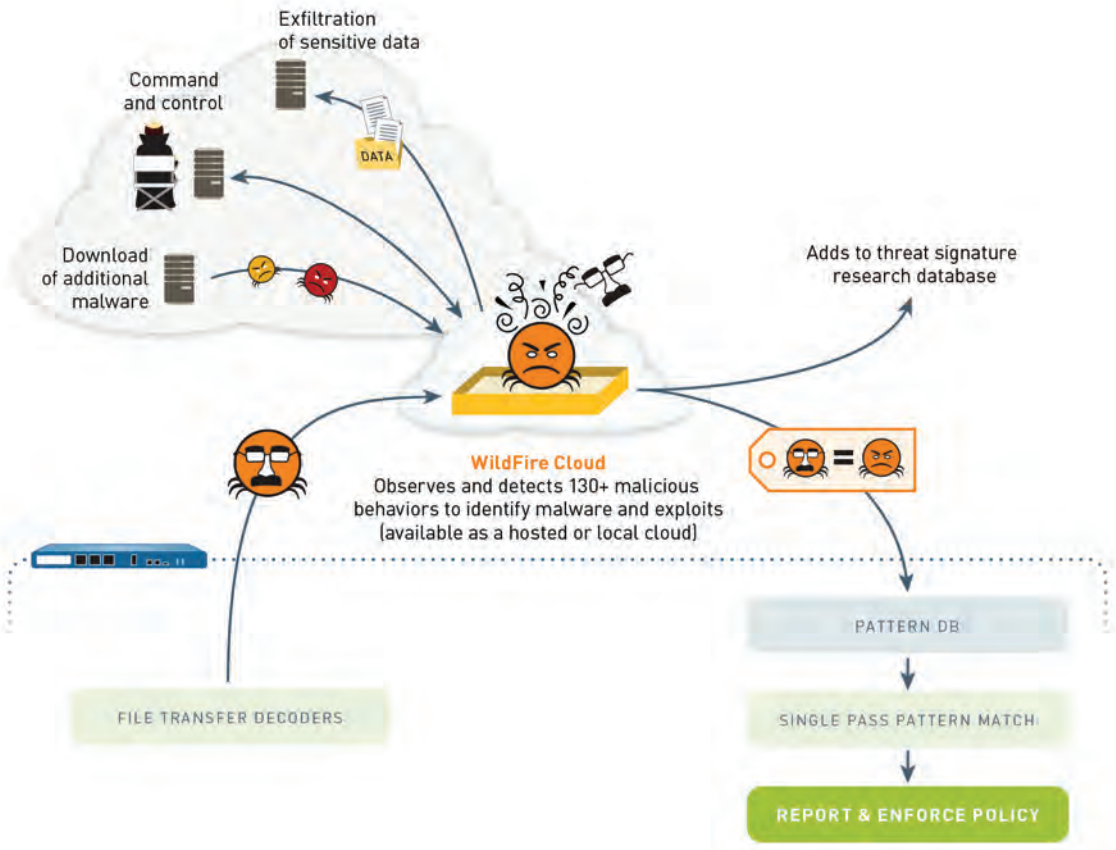


Intelligence Cloud : base de re

Le concept de "Cloud de renseignements sur les menaces" est une base de données collaborative qui consiste à s'appuyer sur les millions d'informations provenant de millers de solutions Palo Alto Networks déployées de par le monde pour identifier automatiquement des menaces inconnues et envoyer aussitôt les protections contre la nouvelle menace détéctée à la communauté.
Par ailleurs, cette base de données permet d'accélèrer les temps de réponse aux incidents et les investigations grâce à des fonctions de reporting en profondeur pour une remédiation rapide.

Plateforme WILDFIRE™ : identification des malwares

WildFire identifie les logiciels malveillants inconnus, les exploits zero day et les menaces persistantes avancées (APT) grâce à une analyse dynamique dans l' environnement cloud. Il **diffuse automatiquement des protections**, presque en temps réel, pour réagir rapidement aux cyber-attaques. WildFire repose sur le firewall nouvelle génération qui classifie l'ensemble du trafic en natif, y compris les menaces et les applications, ainsi que sur les informations des postes clients .



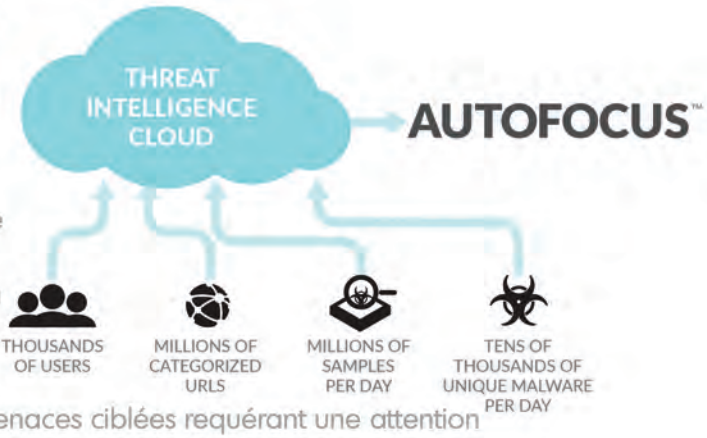
WildFire apprend et renseigne en combinant la visibilité unique des firewalls nouvelle génération déployés et un environnement d'analyse des logiciels malveillants dans le Cloud.

nseignements sur les menaces

AUTOFOCUS™ : Priorité, Contexte, Action

La diversité et le volume des attaques ciblées sont tels que les méthodes d'analyse inondent les équipes sécurité d'alertes et d'informations qui les empêchent de répondre et de comprendre les attaques les plus critiques.

Le service de renseignement **AutoFocus™**, par une analyse synthétique des attaques ciblées, transforme ces renseignements en un plan d'action précis pour contrer ces menaces :



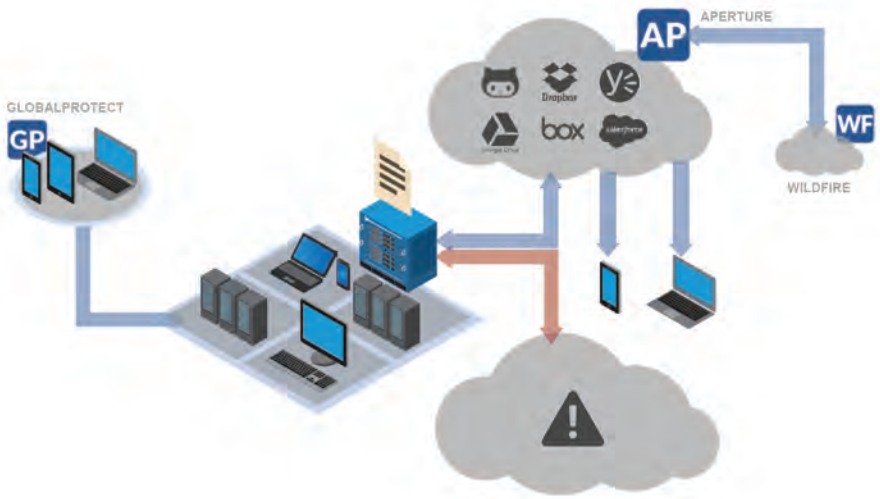
- Il établit une priorité parmi les alertes pour les menaces ciblées requérant une attention immédiate
- Il fournit les informations contextuelles sur les attaques, adversaires, campagnes et les secteurs ciblés
- Il répond proactivement aux menaces et bloque les attaques futures

APERTURE : Sécurisez l'utilisation de vos applications SaaS

L'utilisation indifférenciée des applications SaaS validées par l'entreprise et de celles qui ne sont pas contrôlées créé un fossé dans la visibilité de la sécurité. De nouveaux risques de propagation des menaces, de fuites d'informations et de non-conformité font leur apparition.

Aperture™ fournit une **visibilité** complète des utilisateurs, répertoires et activité fichiers à l'intérieur même des applications SaaS et une analyse détaillée de leur usage pour prévenir les risques liés aux données et à la conformité.

Encore plus important, il fournit une **règle de contrôle contextuelle** de l'utilisation des applications SaaS, et une mise en quarantaine des utilisateurs ou données en violation. L'intégration d''Aperture dans WildFire empêche par ailleurs les applications SaaS d'être un nouveau mode de propagation des malwares.



Protection a

En associant ses fonctions de connexions VPN et ses fonctions de sécurité nouvelle génération à une vérification d'integrité des postes, Palo Alto Networks fournit avec GlobalProtect une solution unique de protection des connexions mobiles. Le poste client est, lui, protégé de manière révolutionnaire, en prévenant l'exploitation des vulnérabilités logicielles grâce au blocage du nombre fini des techniques d'exploitation qu'un attaquant doit combiner pour livrer un malware, protégeant ainsi le poste indépendamment de la vulnérabilité : c'est la solution Traps.

GLOBALPROTECT™ propage les règles de sécurité

GlobalProtect est une solution de connexion VPN SSL IPSec capable de fournir la sécurité du firewall nouvelle génération et ses protections contre les menaces, à n'importe quel utilisateur quel que soit son emplacement :

- Connexion automatique, visibilité et application des règles en continu à l'extérieur comme à l'intérieur du périmètre physique de l'entreprise
- Règles de contrôle granulaire basées sur les applications, les utilisateurs et un profil d'intégrité (OS, Patch, protections…)
- Adossement aux fonctions des firewalls Palo Alto Networks pour fournir performance et protection indépendamment de la position de l'utilisateur final

vancée du poste client

TRAPS™ stoppe les attaques modernes sur le terminal

Malgré une pléthore de produits de sécurité du poste client disponibles sur le marché, les appareils des utilisateurs restent le maillon faible des infrastructures et sont infectés à un rythme alarmant. Les méthodes traditionnelles de protection des postes clients ne peuvent tout simplement plus faire face à un tel volume et une telle rapidité d'évolution. Au lieu de chercher à identifier les millions d'attaques individuelles elles-mêmes, ou à détecter des comportements malveillants parfois indétectables, Traps se concentre sur les techniques de base que chaque attaquant doit combiner pour exécuter son attaque. Avec cette approche, Traps peut contrecarrer une attaque avant même que la moindre activité malveillante ne s'exécute.

Fonctionnalités Traps :

- Prévention de tous les exploits, y compris ceux qui utilisent des vulnérabilités zero-day
- Prévention de tous les exécutables malveillants sans connaissance préalable de ces derniers
- Investigation et analyse détaillées des attaques subies et bloquées
- Déploiement et installation simples et transparents
- Intégration étroite avec le réseau et WildFire

Afin d'assurer une protection avancée du poste, Traps va combiner :

- l'application d'une politique de restriction des accès aux fichiers en fonction de l'utlisateur, du média ou du type de fichier
- l'inspection des fichiers par WildFire pour bloquer l'accès à des fichiers déjà présents et reconnus comme malwares connus ou inconnus
- Le blocage des techniques combinées d'exploitations des vulnérabilités pour livrer un malware

Commencez par auditer votre sécurité

Le SLR (Security Lifecycle Review) montre quels sont les applications, les applications SaaS, le trafic URL, le type de contenu et les menaces connues et inconnues qui traversent le réseau.

Le SLR est généré depuis les logs collectés par l'appliance Palo Alto Networks déployée sur le réseau.

Ce rapport PDF est un snapshot de l'activité des collaborateurs sur 7 jours et permet un audit de sécurité du réseau. Il est édité par le partenaire (Editeur/distri/ESN).

Miel, premier centre de formation sur les solutions Palo Alto Networks

appelez le 01 60 19 16 27

PAN-EDU-201/205
Formation de 5 jours :
Bundle Essentials 1 et 2 : Administration et gestion avancée des firewalls

Possiblilité de suivre séparemment la formation PAN-EDU-201 sur 3 jours (administration des firewalls) et la formation PAN-EDU-205 sur 2 jours (formation avancée).

PAN-EDU-311
Formation de 3 jours
Troubleshooting avancé des firewalls

PAN-EDU-221
Formation de 2 jours sur l'Administration de Panorama

PAN-EDU-231
Formation de 2 jours sur la gestion avancée des menaces

Retrouvez les dates des prochaines sessions sur :
www.miel.fr/formation

Téléchargez ce document en PDF

http://www.miel.fr/info/gammepan

paloalto NETWORKS®