Innovations Palo Alto Networks

ZERO TRUST NETWORK SECURITY

Palo Alto Networks a frappé un grand coup en annonçant une série d'innovations majeures afin d'adopter une vraie posture Zero Trust dans leur stratégie de sécurité réseau quels que soient les cas d'usage ou la taille de l'entreprise.

Nouvelles Plateformes NGFW «ML-Powered»

Cloud identity Engine

Sécurité Internet réinventée

CASB intégré

Nouvelles Plateformes NGFW alimentées par Machine Learning

Deux nouveaux modèles de firewal nouvelle génération ont été introduits de manière à couvrir tous les types d'accès. La série PA-400 va permettre d'adresser une gamme de sites étendue, du bureau distant au site principal des entreprises de taille moyenne. Le PA-5450 va cibler les campus les plus larges aux gros datacenters.

Cloud Identity Engine

Il s'agit du premier moteur cloud qui permet aux entreprises de facilement authentifier et autoriser leurs utilisateurs dans tous les réseaux de l'entreprise, les clouds et les applications, indépendamment du lieu où leur identité est stockée.

Sécurité Internet améliorée

La nouvelle souscription de filtrage URL avancé offre pour la première fois une prévention des attaques web zero-day grâce aux fonctions en ligne de *Machine Learning*. Les fonctions étendues de sécurité DNS protègent d'attaques DNS émergentes qu'aucun autre éditeur n'est en mesure de contrer.

CASB Intégré

Les firewalls possèdent maintenant un CASB (Cloud Access Security Broker) intégré qui permet d'étendre proactivement la sécurisation des accès à toutes les applications SaaS, y compris celles jamais vues auparavant.

MIEL

Distribué en France par MIEL

01 60 19 34 52 - https://www.miel.fr/palo-alto-networks

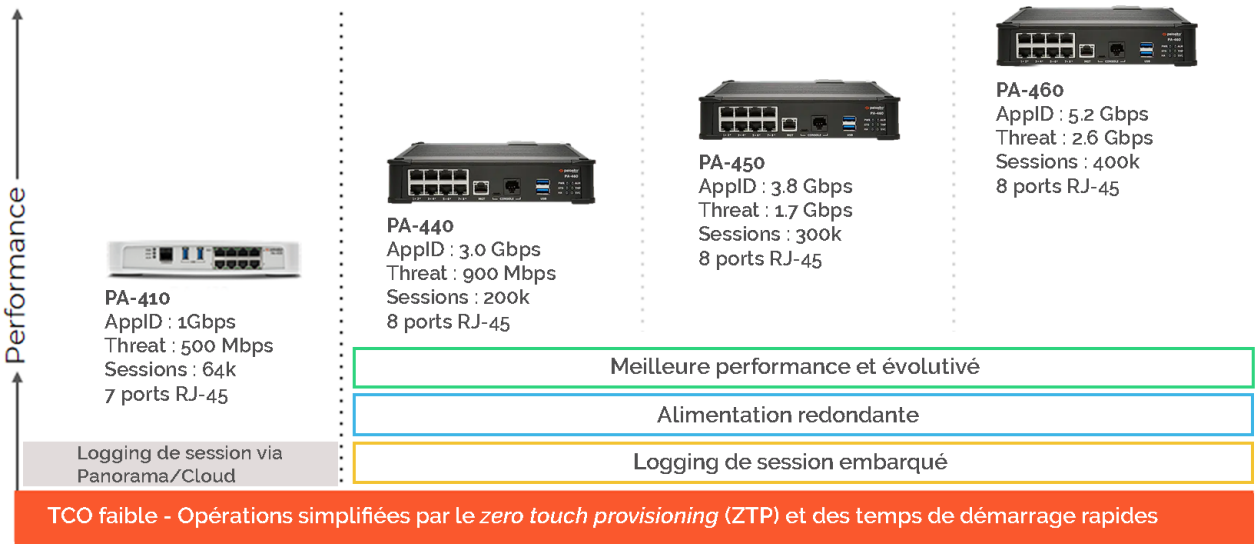
Nouveau matériel : PA-400 series

Petite appliance. Grande performance.

Les matériels de la nouvelle séries PA-400 de Palo Alto Networks, qui comprend le PA-460, PA-450, PA-440, et PA-410, apportent les fonctions du NGFW Palo Alto Network et ses propriétés de Machine Learning aux sites distants, aux succursales et et aux entreprises de taille moyenne.

- petit format
- débits plus élevés
- meilleure performance
- pas de partie amovible
- design résilient

Avec un design industriel petit format sans partie amovible, sans ventilateur et des alimentations redondantes, ainsi que des options de montage en bureau, en fixation murale ou en rack, la série PA-400 est parfaitement équipée pour tout type de site distant.



Options de bundles de souscriptions

Les services de sécurité de Palo Alto Networks peuvent être regroupés en deux types de bundles différents :

Professional

«Complete security»
sécurité étendue au réseau et au web

TP | WF | DNS | ADV URL

Soucriptions : Threat prevention, Wildfire, DNS Security et Advanced URL Filtering

Enterprise

«All in comprehensive security»
sécurité étendue à tous les vecteurs d'attaque réseau

TP | WF | DNS | ADV URL | SD-WAN | SaaS | IoT

+ SD-WAN, SaaS Security et IoT

Nouveau matériel PA-5450

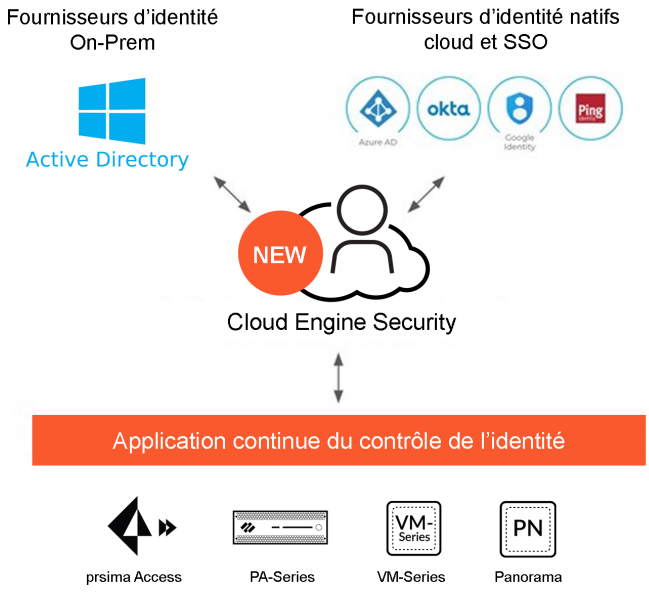
Le nouveau modèle PA-5450 de Palo Alto Networks a été conçu pour les data centers « hyperscale », les fournisseurs d'accès Internet et mobile, et pour la segmentation des campus les plus importants. Son architecture modulaire et évolutive qui combine des cartes réseaux (NC) et des cartes de traitement (DPC) permet d'atteindre jusqu'à 150 Gbps de performance lorsque tous les services de sécurité sont activés.

- architecture modulaire
- capacité évolutive
- performances élevées
- réduction du rapport coût/performance
- design résilient

	Conf MAX (2 NC + 4 DPC)	Conf Mini (1NC+1DPC)
Débit Firewall (http/Appmix)	200/200 Gbps	72/68 Gbps
Débit Threat Prevention	125/150 Gbps	31/37 Gbps
Débit VPN IPSec	95 Gbps	19 Gbps
Nouvelles sessions/secondes	4M	830,000

Cloud Identity Engine

Le moteur d'identité Cloud de Palo Alto Networks va simplifier les contrôles de l'identité dans le but de généraliser le Zero Trust. Quel que soit le format de sécurité réseau utilisé, Cloud Identity va authentifier et autoriser les utilisateurs où que soient la ou les sources de leur identité, sur site, dans le Cloud ou dans un système hybride.



Zero Trust pour un monde "cloud-first"
Vérification facile et continue de l'identité du user avant toute autorisation d'accès grâce à des integrations instantanées aux Fournisseurs d'identité

Identité unifiée dans l'infrastructure
Synchronise les données de user, de groupe et d'authentification entre tous les produits de la plateforme firewall

Prévention des attaques basées sur les identifiants
Déploiement globale du MFA pour toutes les applications et tous les users, indépendamment de l'app ou du fournisseur

Protection des investissements
Transition fluide du On Prem vers le cloud – identité, firewall ou apps- avec un effort minimal

Sécurité internet réinventée

Le *Machine Learning* en ligne a été étendu aux souscriptions de filtrage URL. La souscription Advanced Url Filtering va être beaucoup plus efficace dans la capture des nouvelles menaces en temps réel. Les fonctions de sécurité DNS ont été étendues pour bloquer des types d'attaques DNS que les éditeurs de sécurité ne parviennent pas à bloquer.

Nouvelles fonctions avec Advanced URL Filtering

- URLs et domaines malveillants encore jamais détectés
- Lien à usage unique
- Liens à très courte durée de vie (i.e. malvertizing)
- Dissimulation de contenu malveillant par "cloaking"
- URLs malveillants cachés dans des domaines ou sites web compromis
- URLs de C2 ne servant pas de conter u ouvertement malveillant

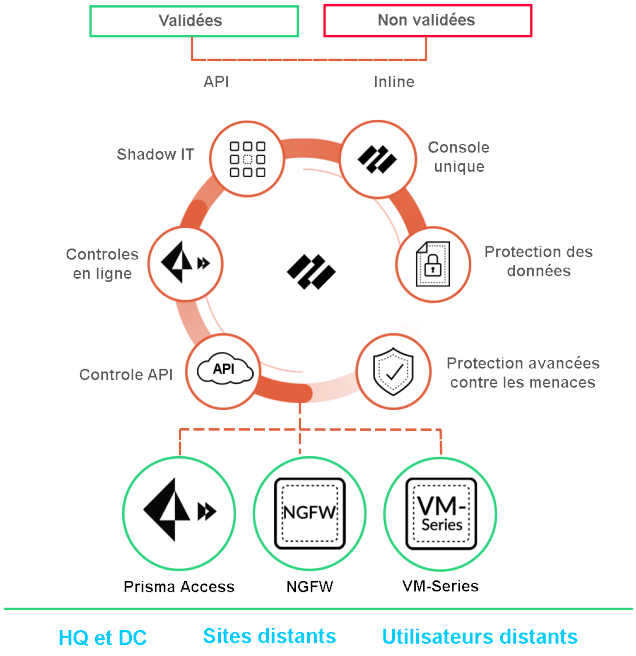
Protection DNS

Protections existantes	Nouvelles Protections	
Known malicious domains	Fast-flux domains	Dangling DNS attacks
High-risk domains	DNS rebinding attacks	NSNX denial of service
DGA domains	Dictionary DGA	Prediction detection of new domains
DNS tunneling		Ultra-slow DNS tunneling

CASB intégré

La souscription de CASB intégré (appelée SaaS Security) permet de répondre simplement à tous les scénarios de sécurisation des applications, des utilisateurs et des données SaaS.

Directement intégré aux firewalls ou à Prisma Access, la découverte et le contrôle en ligne automatiques des applications vont se combiner à une couverture très large des applications SaaS légitimes de l'entreprise (via API) pour se protéger des fuites de données et des menaces, que les données soient stockées dans le cloud ou en transit.



Distribué en France par MIEL
Appelez le 01 60 19 34 52