Strata : Secure the Entreprise

Firewalls Nouvelle Generation

Les firewalls nouvelle génération Palo Alto Networks donnent la priorité à la prévention et l'intégration d'innovations faciles à déployer. La plateforme de sécurité Palo Alto Networks vous protège contre les menaces connues et inconnues grâce à un contrôle granulaire des applications, des utilisateurs et des contenus et une intelligence cloud partagée de détection des menaces.

Les 3 missions clés du Firewall Nouvelle Génération :

- Permettre à vos utilisateurs d'**accéder aux données et aux applications** selon les exigences de l'entreprise
- Vous **prémunir des menaces connues et inconnues**, y compris dans le trafic chiffré
- Vous **protéger des attaques par vol d'identifiants**

Les 3 technologies clés du Firewall Nouvelle Génération :

APP-ID	USER-ID	CONTENT-ID
Technologie de classification des applications	Technologie de classification des utilisateurs	Technologie de classification des contenus
App-ID ™ est une technologie de classification du trafic brevetée. Elle détermine l'identité d'une application indépendamment du port, du protocole, du cryptage SSH / SSL ou de toute autre tactique d'évasion que l'application peut utiliser	User-ID ™ permet d'identifier l'utilisateur par son identité, indépendamment de son adresse IP, grâce à plusieurs technologies combinant un mapping avec les annuaires ou le monitoring du trafic d'authentification	Content-ID ™ permet une analyse complète de tout le contenu du trafic autorisé comprenant les malwares, tous les types d'exploit, les catégories Web, et les fichiers par catégorie ou type de contenu. L'ensemble sera utilisé comme critère de contrôle

Gamme

Firewall Matériels (Débit avec App-ID | Sessions Max)

PA-7080		PA-7050		PA-5280		PA-5260		PA-5250		PA-5220	
700 Gbps	80/320M	420Gbps	48/192M	64Gbps	64M	64Gbps	32M	40Gbps	8M	20Gbps	4M
PA-3260		**PA-3250**		**PA-3220**		**PA-850**		**PA-820**		**PA-220(R)**	
10Gbps	3M	6.6 Gbps	2M	5Gbps	1M	2Gbps	197K	1.6Gbps	130K	580Mbps	64k

Distribué en France par MIEL

www.miel.fr/palo-alto-networks-next-gen-firewall

Panorama : administration centralisée

Panorama permet une administration centralisée de tous les firewalls, incluant le firewall as-a-service Prisma Access, tout en donnant une vue du trafic et des menaces à l'échelle globale du réseau

Appliance Virtuelle sur VMware ESXi. 25/100/1000 unités	Appliance Matérielle sur site M100/M200/M600	En environnement cloud public

LES SOUSCRIPTIONS

Les souscriptions de sécurité de l'offre Strata sont nativement Intégrées aux Firewalls Nouvelle Génération pour exploiter toutes les technologies d'identification et appliquer automatiquement une sécurité pilotée par l'analytique.

THREAT PREVENTION	URL FILTERING	WILDFIRE
Threat Prevention fournit des signatures qui bloquent les exploits de vulnérabilité client et serveur connus, les malwares, virus trojan... ainsi que les canaux de commande et contrôle.	URL filtering catégorise dynamiquement le trafic Web pour contrôler la navigation des utilisateurs, le type d'accès de n'importe quelle application et la politique de déchiffrement	WildFire ® est un service cloud collaboratif d'analyse sandboxing et de prévention des malwares qui détecte et bloque automatiquement les attaques inconnues sur le réseau, le endpoint et le cloud

DNS SECURITY	SD-WAN	GLOBALPROTECT
DNS Security fait une analyse prédictive de toutes les requêtes DNS pour stopper dynamiquement les attaques utilisant DNS (command & control ou vol de données), et bloquer les domaines malveillants à la volée.	SD-WAN permet au firewall distant d'optimiser dynamiquement la connectivité de plusieurs liens WAN tout en appliquant la sécurité Palo Alto Networks. La gestion est centralisée et peut s'appuyer sur Prisma Access	GlobalProtect ™ assure une connexion VPN IPsec/SSL de tout endpoint en vérifiant l'intégrité du poste et avec le même niveau de visibilité et de contrôle que pour un user interne. Une version agentless permet d'accéder aux applis Web.

Les 13 Fonctions Incontournables du Firewall Nouvelle Génération

- **Identification** des utilisateurs et **autorisations d'accès** adaptées
- **Prévention** des vols et détournements d'identifiants
- **Exécution sécurisée** des applications et contrôle de leurs fonctions
- **Simplification** de la gestion des règles et politiques
- **Sécurisation du trafic** même chiffré
- **Blocage des menaces avancées** pour neutraliser les cyberattaques
- **Protection des collaborateurs mobiles**
- **Sécurisation d'environnements cloud** en mutation permanente
- **Stratégie Zero-Trust**
- **Homogénéité des politiques** sur site, dans le cloud sur les réseaux distants et mobiles
- **Blocage des attaques DNS**
- **Automatisation** des tâches de routine pour se recentrer sur les menaces prioritaires
- **Déploiement simplifié** des innovations en sécurité