Palo Alto Networks
Leader Mondial de la cybersécurité

Les technologies de Palo Alto Networks permettent à 70 000 entreprises clientes de protéger des milliards de personnes dans le monde entier.

La plateforme de Palo Alto Networks simplifie la problématique de la sécurité, adresse le réseau, le endpoint et le cloud. Elle met l'automatisation et l'innovation au cœur de son offre.

Sa stratégie s'appuie sur 3 piliers :

Secure the Entreprise

STRATA BY PALO ALTO NETWORKS

- Contrôle et visibilité complète
- Intégration étroite
- Performance

Secure the Cloud

PRISMA BY PALO ALTO NETWORKS

L'offre de sécurité Cloud la plus complète du marché

- Sécurité aux accès Clouds
- CASB/DLP
- Gouvernance/conformité

Secure the Future

CORTEX BY PALO ALTO NETWORKS

- Détection des attaques les plus sophistiquées
- Investigation
- Automatisation
- Réponse
- Collaboration

- **Strata** S'appuie sur le meilleur firewall nouvelle génération du marché auquel s'intègrent des innovations constantes sous forme de souscription.
- **Prisma** gère tous les scenarii de sécurisation du cloud. De l'accès vers le cloud où que soit l'utilisateur jusqu'au contrôle de l'accès aux ressources dans tous les clouds.
- **Cortex** présente une suite de produits pour la sécurité opérationnelle, avec une offre de prévention, automatisation, détection et réponse. Cortex agit sur le réseau, les endpoints et le cloud.

Secure the Entreprise

STRATA BY PALO ALTO NETWORKS

Firewall Next Generation
- Threat Prevention
- URL Filtering
- WildFire
- DNS Security
- SD-WAN
- GlobalProtect
- Sécurité IoT

Panorama

Secure the Cloud

PRISMA BY PALO ALTO NETWORKS

Prisma Cloud

Prisma Access (SASE)

Prisma SaaS

VM-Series

Secure the Future

CORTEX BY PALO ALTO NETWORKS

Cortex Data Lake

Cortex XDR
- Prevent (Endpoint)
- Pro (Endpoint)
- Pro (Network)

Cortex XSOAR

Autofocus

STRATA
BY PALO ALTO NETWORKS

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, associé à une intelligence cloud partagée de détection des menaces.

La nouvelle version logicielle PAN-OS 10.0 embarque en plus des modèles de Machine Learning pour aider à prévenir les attaques inconnues et permettre ainsi d'avoir les signatures sans délais.

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 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	Technologie de classification des utilisateurs 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	Technologie de classification des contenus 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

De plus, PAN-OS 10.0 introduit les CN-Series, une version en conteneur du Machine Learning Powered NGFW, conçus spécifiquement pour les environnements Kubernetes.

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

Strata : Secure the Entreprise

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	SÉCURITÉ IOT
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.	Sécurité IoT permet la découverte, la classification et le profilage de tous les devices connectés, en se basant sur les logs provenant des NGFW Palo Alto Networks. Grâce au Machine Learning, il identifie les vulnérabilités, évalue les risques associés, et recommande les mesures de sécurité adaptées.

Les 14 Fonctions Incontournables du Firewall Nouvelle Génération

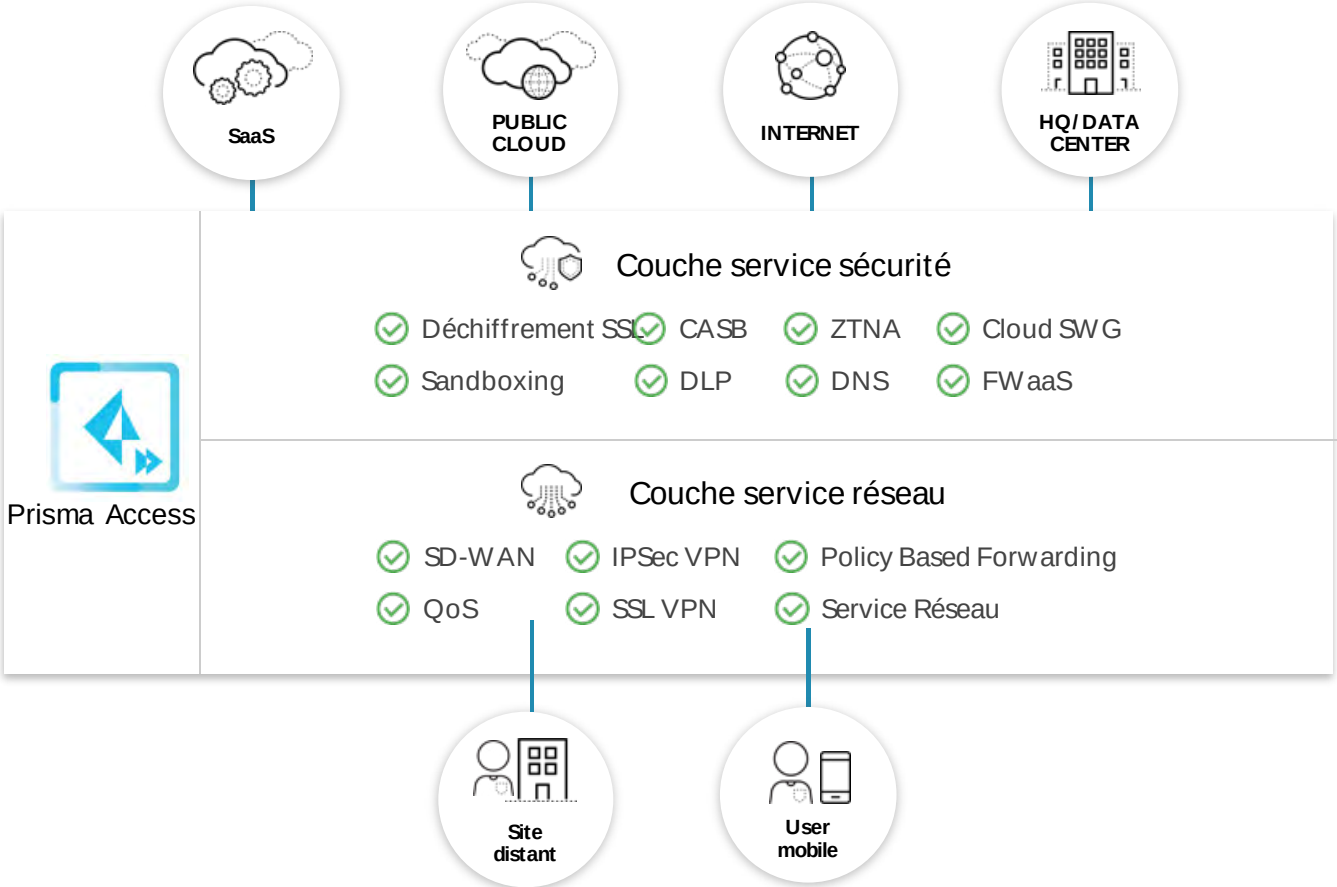
- **Identification** des utilisateurs et **autorisations d'accès** adaptées
- **Prévention** des vols et détournements d'identifiants
- **Exécution sécurisée** des applications et contrôle de leurs fonctions
- **Simplification** de la gestion des règles et politiques
- **Sécurisation du trafic** même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

La suite de produits Prisma représente l'offre de sécurité et de conformité cloud la plus complète du marché. Elle sécurise l'accès vers le cloud, les ressources natives cloud ainsi que les environnements hybrides.

PRISMA ACCESS (SASE)

Prisma Access est une offre cloud de **"Firewall-as-a-service"** qui propose toutes les fonctions et toutes les souscriptions du firewall nouvelle génération Palo Alto Networks, gérées de manière centralisée et unifiée avec les firewalls physiques si l'entreprise en possède. La disponibilité et la montée en charge du service sont gérées et garanties par Palo Alto Networks.

Prisma Access se décline en solutions pour les users nomades quel que soit le site ou le cloud accédé ainsi que pour les sites distants, afin de sécuriser les réseaux distribués et le SD-WAN.



Pour les users nomades, une connexion sécurisée « Always-on » se fait grâce au client GlobalProtect disponible sur **Windows, MacOs, Linux, Android, et iOS.**

VM-SERIES

VM-Series est la forme virtualisée du firewall nouvelle génération. Elle peut être déployée dans tous les environnements cloud privés ou publics. Les firewalls VM-Series peuvent en effet être basés sur les technologies VMware ESX ou NSX, Cisco, KVM, OpenStack, Nutanix, Amazon Web Services, Microsoft Azure, Google Cloud Platform, Oracle Cloud et Alibaba Cloud.

Modèles VM-Series (Débit avec App-ID) :

VM-50 (Lite)		VM-100/VM-200		V300/VM1000-H		VVM-500		VM-700	
200Mbps	64K(50K)	2Gbps	250K	4 Gbps	819K	8Gbps	2M	16 Gbps	10M

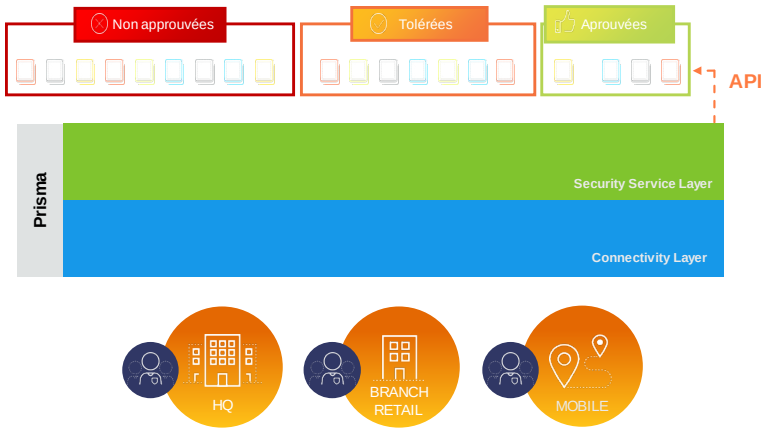
Prisma : Secure The Cloud

PRISMA SAAS

Prisma SaaS est une solution native Cloud de CASB (Cloud Access Security Broker) multimodes protégeant à la fois l'accès aux applications SaaS et leur utilisation :

- Visibilité et contrôle granulaires de tous les usages utilisateurs sur les applications SaaS
- Analyse détaillée de l'utilisation de ces applications liée à la conformité
- Identification des risques et des malwares, prévention des menaces
- Fonctionnalités avancées de DLP (Data Loss Prevention)

Prisma SaaS peut être enrichie par un service DLP avancé pour garantir la gouvernance et la protection complète des données. Ce service aide à réduire les risques d'exfiltration de données et de non conformité par la découverte, le contrôle et la protection des données sensibles.



Les licences Prisma SaaS sont basées sur le nombre d'utilisateurs, indépendamment du nombre d'applications.

PRISMA CLOUD

Prisma Cloud sécurise vos déploiements complexes multi cloud en assurant la visibilité et la sécurité de vos données et workloads sur les cloud publics GCP, AWS et Microsoft Azure. Prisma Cloud a une approche totalement intégrée aux outils de déploiement et de développement pour une sécurité « by-design ». Les licences Prisma Cloud sont basées sur le nombre de Workload à sécuriser.

- Protection des containers, Serverless et hosts
- Vue unifiée de la conformité et de la sécurité
- Encadrement complet des DevSecOps
- Gouvernance et conformité

CORTEX™
BY PALO ALTO NETWORKS

Identifier et répondre aux attaques les plus sophistiquées, combler les failles de sécurité nécessitent toujours plus de produits à gérer, plus de sources de données à corréler et plus d'actions répétitives.

Face à une telle quantité d'évènements à gérer et de solutions à synchroniser, les équipes de sécurité opérationnelles n'ont pas d'autre choix que d'avoir recours à l'automatisation, appuyée par de l'intelligence artificielle, pour accélérer la détection, l'investigation et la réponse.

L'approche de Palo Alto Networks, appuyée par la suite de produits Cortex, a la réponse la plus cohérente et la plus pertinente du marché dans ce domaine.

RÉINVENTER LA SECURITE OPÉRATIONNELLE

Prévenir tout ce qui peut être prévenu

CORTEX XDR

Détecter et investiguer rapidement tout ce qui ne peut être prévenu

CORTEX XDR

Automatiser la réponse et progresser à chaque incident

CORTEX XSOAR

Cortex est LA PLATEFORME DE SÉCURITE OPÉRATIONNELLE.

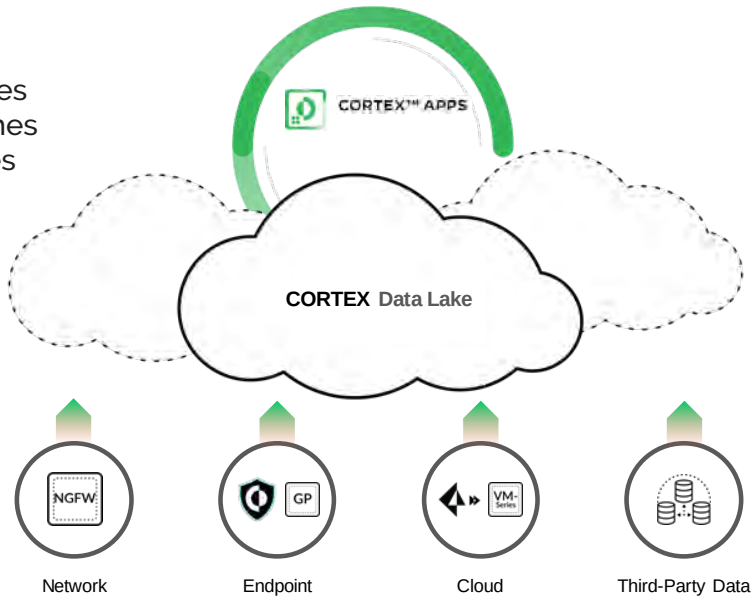
Elle est composée de 3 éléments clés :

- **Cortex XDR** pour la détection et la réponse qui étend la détection et la réponse au-delà du endpoint.
- **Cortex XSOAR** pour l'orchestration, l'automatisation et la réponse de sécurité.
- **Cortex Data Lake** qui collecte, transforme et intègre les données des solutions Palo Alto Networks dans le réseau, le endpoint et le cloud.

CORTEX DATA LAKE

Les firewalls nouvelle génération, Prisma Access et les endpoints sont configurés pour envoyer des logs riches et corrélés vers Cortex Data Lake pour être exploitées par des services de machine learning et des applications de sécurité.

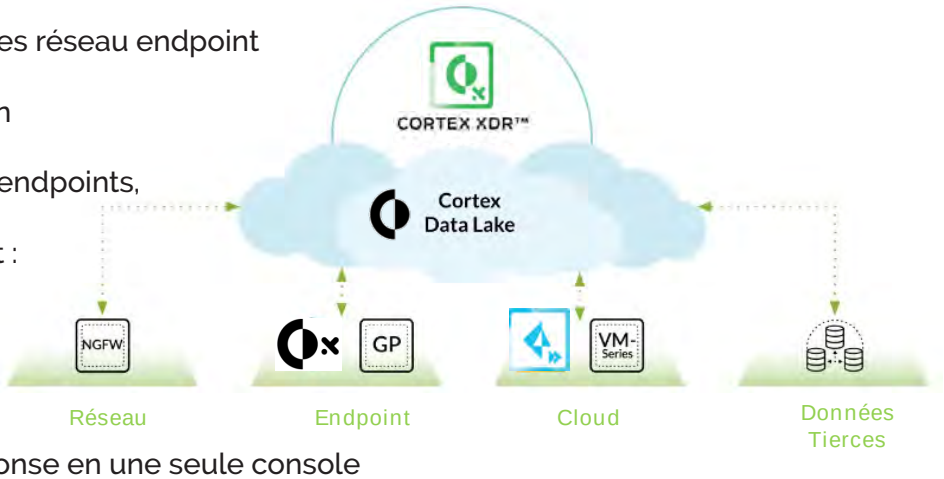
Cortex Data Lake est élastique, illimité et peut être configuré pour recevoir des données d'éditeurs tiers.



Cortex : Secure The Future

CORTEX XDR

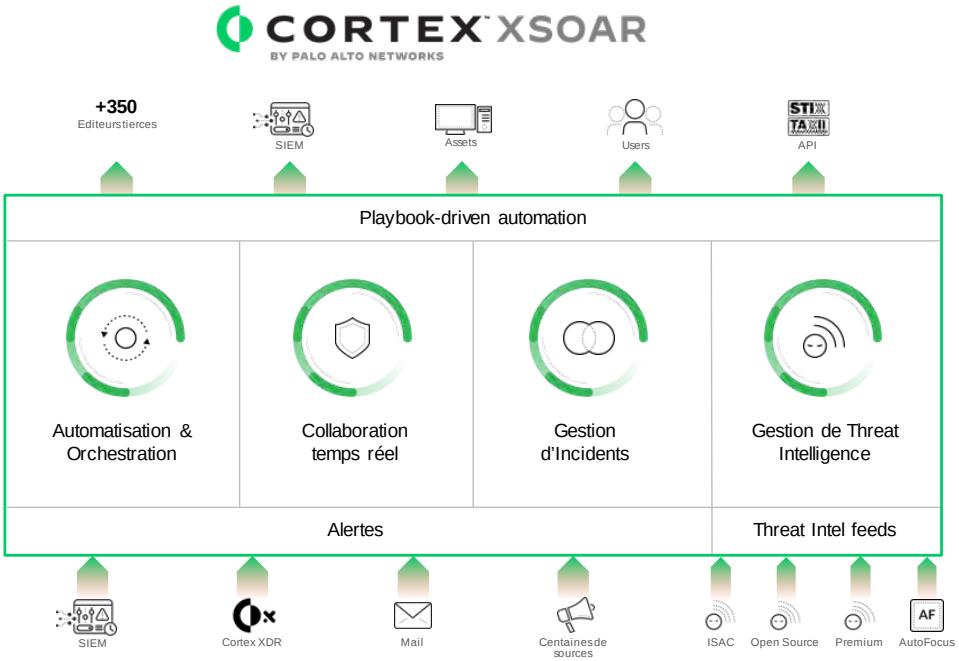
- Intégration de toutes les données réseau endpoint et cloud
- Découverte des menaces par un Machine Learning continu
- Réponse coordonnée entre les endpoints, le réseau et le cloud
- Protection avancée du endpoint : Prévention, détection et réponse
- Investigation 8x plus rapide
- Sécurisation des devices USB
- Management unifiié du reporting, du triage et de la réponse en une seule console
- Nativement Intégré à Cortex XSOAR



Produit	Cortex XDR Prevent (Endpoint)	Cortex XDR Pro per Endpoint	Cortex XDR Pro Network per TB
Protection du Endpoint	X	X	-
Contrôle des devices	X	X	-
Gestion des incidents	Alertes Endpoint	Toutes les sources	Toutes les sources
Contrôle périphérique	X	X	-
Analytique	-	X	X
Threat Intelligence externe	Optionnelle	Optionnelle	X
Réponse Intégrée	Endpoint	Endpoint+Réseau	

CORTEX XSOAR

Cortex™ XSOAR est une plateforme d'orchestration, d'automatisation et de réponse de sécurité (SOAR) qui permet aux équipes de sécurité opérationnelles de piloter de manière unifiée la gestion d'incident, l'automatisation, la collaboration temps réel et la gestion des sources de Threat Intelligence tout au long du cycle de tout incident. La réponse est cordonnée avec + de 350 éditeurs différents de sécurité.



AUTOFOCUS

Est un portail qui offre un service de Threat Intelligence qui prend en compte les données de WildFire et les corrèle avec les informations de menaces de sources tierces. L'objectif est d'avoir une analyse contextuelle des attaques dont on est l'objet et de prioriser la réponse.

SLR :
SECURITY LIFECCYCLE REVIEW

MONTREZ LA PUISSANCE DE LA PLATEFORME PALO ALTO NETWORKS

Le **SLR (Security Lifecycle Review)** est un outil destiné à offrir une visibilité sur les applications, les risques et les menaces, obtenue sous la forme d'un rapport généré sur la base d'informations recueillies par le firewall nouvelle génération grâce à une mise en place non intrusive.

Le SLR est une évaluation sur mesure des risques comprenant l'exposition réelle aux menaces, le comportement utilisateur, l'utilisation des applications, pour comprendre les risques "cyber" de l'entreprise.

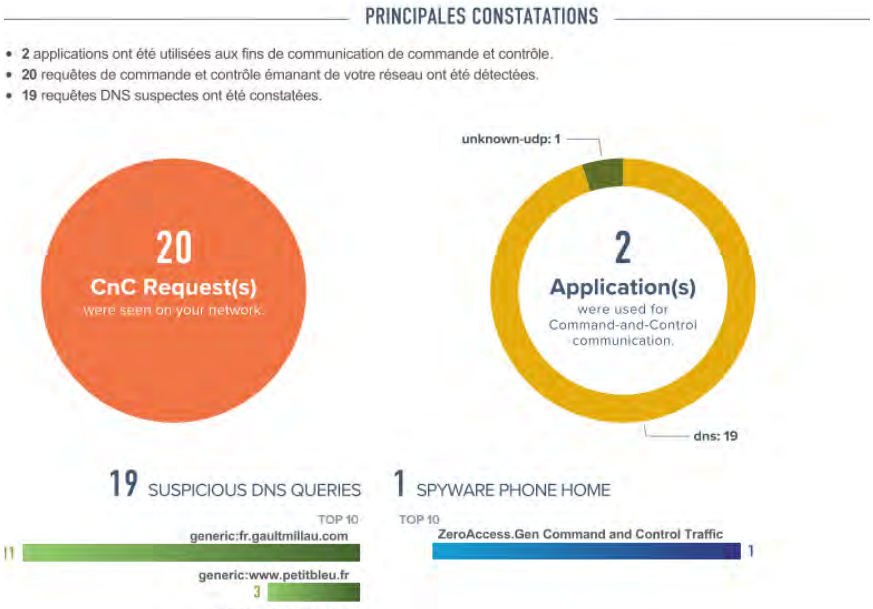
Le SLR est généré par l'intermédiaire d'un partenaire en récupérant un fichier de logs.

QUE FAIT LE SLR ?

- Identification et usage des applications
- Identification et usage des applications SaaS
- Comportement des utilisateurs
- Rapport sur les risques et les menaces

SLR : DANS QUEL CAS ?

- Construire un cas d'usage Palo Alto Networks pour les architectes, les managers et les décisionnaires.
- Montrer comment restaurer la visibilité et le contrôle sur les applications, les utilisateurs et le contenu
- Prouver la nécessité d'une telle solution dans le réseau
- Gérer le cycle d'évaluation et mettre un cadre autour de l'évaluation/POC

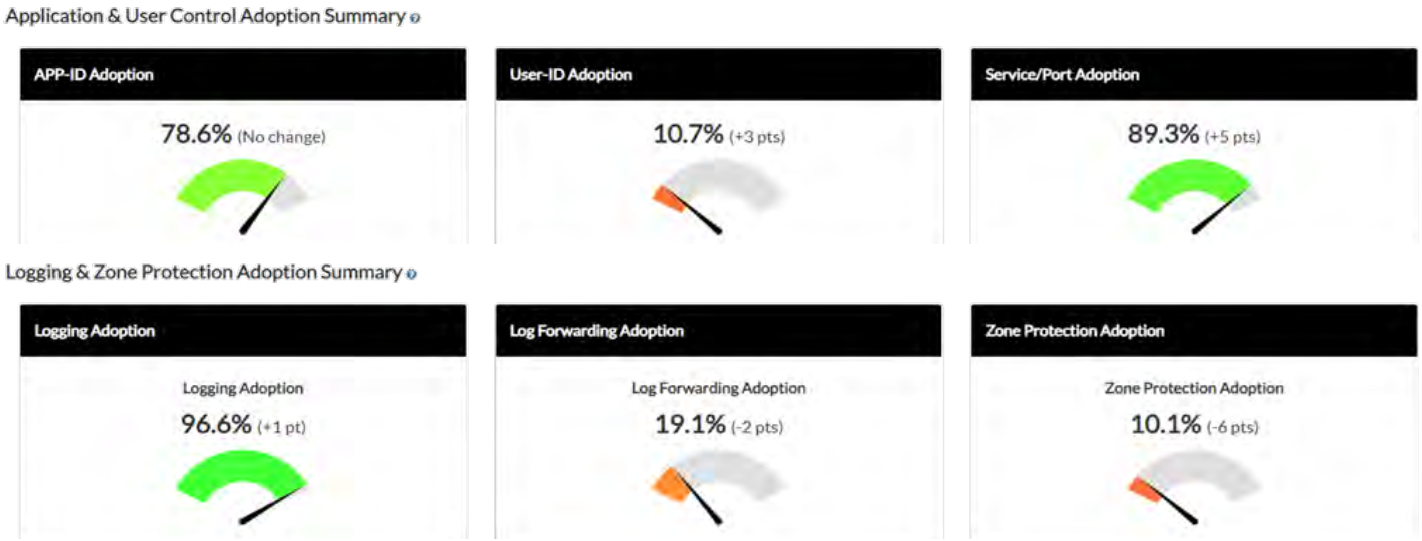


BPA :
BEST PRACTICE ASSESSMENT

ÉVALUEZ VOTRE PLATEFORME PALO ALTO NETWORKS

Que vous soyez un expert des firewalls nouvelle génération de Palo Alto Networks ou un tout nouvel utilisateur, la plus grande question reste de savoir si vos firewalls sont correctement configurés et protègent complètement le réseau. Le BPA évalue les configurations, identifie les risques et fournit des recommandations aux utilisateurs des firewalls Palo Alto Networks et de Panorama pour résoudre les problèmes de sécurité et faire évoluer l'architecture lorsque c'est nécessaire.

Le BPA va comparer les configurations d'un firewall ou d'un parc de firewalls avec les bonnes pratiques et produit un guide indiquant celles qui sont suivies, celles qui ne le sont pas, tout en fournissant des recommandations détaillées par fonction. Le BPA va résumer l'adoption des bonnes pratiques, le niveau de compatibilité des règles, des objets, des zones avec une observation de son évolution dans le temps.



Le BPA a 2 composantes :

- Une carte « thermique » de niveau d'adoption des règles (Security Capability Adoption Heatmap)
- Le rapport BPA

QUE FAIT LE BPA ?

- Evaluation des configurations
- Vérification des bonnes pratiques
- Identification des risques
- Recommandations

LE BPA : DANS QUEL CAS ?

- Pour aider à implémenter les bonnes pratiques dans une architecture
- Lorsque les responsables IT et sécurité manquent de connaissances sur ce qu'il se passe sur leurs réseaux
- Lorsque les clients investissent dans Palo Alto Networks mais n'utilisent pas pleinement ses possibilités
- Lorsque la stratégie de sécurité n'est pas assez orientée prévention

Le BPA se génère sur le portail partenaire (www.paloaltonetworks.com/partners)
ou le portail « Customer Success » (www.customersuccess.paloaltonetworks.com).
Il faut charger le fichier « tech support » présent dans les produits.

EXPEDITION

MIGREZ INTELLIGEMMENT ET RAPIDEMENT VERS UNE CONFIGURATION PALO ALTO NETWORKS

Expedition est un outil open-source qui va permettre d'accélérer la migration de configuration de firewalls traditionnels vers les technologies de firewall nouvelle génération Palo Alto Networks, donnant ainsi accès aux meilleurs processus et aux meilleures pratiques de protections contre les menaces.

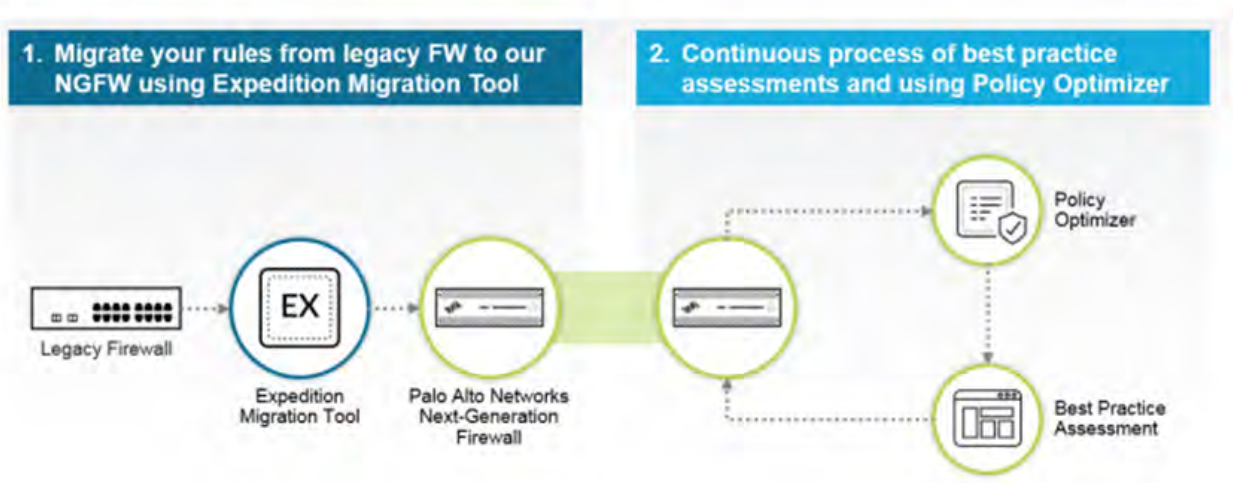
Expedition transpose facilement les règles de sécurité à la couche 3/4 des firewalls tiers vers des règles à la couche 7, améliorant ainsi la protection. Expedition aide à l'implémentation de ces règles à travers les technologies App-ID™, User-ID™ et Content-ID™ de Palo Alto Networks.

Expedition permet d'importer automatiquement les configurations des firewalls

- Cisco
- Fortinet
- Check Point
- Forcepoint
- Juniper
- IBM XG.

Les configurations d'autres types de firewalls peuvent être migrés par l'intermédiaire d'Expedition avec l'aide de scripts.

Expedition va automatiquement mettre à jour vos règles existantes. Il va également utiliser l'analytique pour générer et implémenter de nouvelles règles et des recommandations de configuration. L'objectif sera d'améliorer les contrôles de sécurité tout en optimisant les processus.



UTD :
ULTIMATE TEST DRIVE

METTEZ VOUS AUX COMMANDES DE LA PLATEFORME PALO ALTO NETWORKS

Les UTD (Ultimate Test Drive) sont des sessions sous forme d'ateliers techniques qui vous permettent de prendre en main la plateforme Palo Alto Networks à travers des cas d'usage scénarisés avec pour objectif de démontrer toute la valeur de la plateforme de sécurité Palo Alto Networks.

Les ateliers peuvent se faire en ligne ou sous forme de workshop sur site et donnent accès dans tous les cas à des labs virtuels.

LES DIFFÉRENTS UTD

SECURE ACCESS SERVICE EDGE (SASE) AVEC PRISMA ACCESS	• CYBERSECURITY PORTFOLIO	NEXT-GENERATION FIREWALL
• Protéger les sites distants et les users mobiles où qu'ils soient. • Assurer la connectivité et la sécurité pour toutes les applications grâce au Firewall as-a-service (FWaaS). • S'adapter aux changements d'environnement grâce à une infrastructure cloud qui converge les fonctions de réseau et de sécurité.	• Protéger les utilisateurs des attaques ransomwares avec les modules de protection contre les malwares • Prévenir des menaces inconnues avec le Machine-Learning Powered NGFW • Sécuriser les déploiements Cloud avec l'offre Prisma • Automatiser, détecter et répondre avec Cortex	• Etablir des règles pour sécuriser l'utilisation d'appli et en bloquer d'autres • Activer l'analyse sandbox des malwares inconnus avec WildFire® • Configurez des règles de déchiffrement et d'inspection du flux SSL • Sécuriser les devices mobiles avec GlobalProtect
NETWORK SECURITY MANAGEMENT (PANORAMA)	**VIRTUALIZED DATA CENTER**	**CLOUD-DELIVERED SECURITY SERVICES**
• Centraliser des déploiements de règles globales et locales • Utiliser des templates Pour faciliter la configuration réseau et device • Gestion de la hiérarchie logique de groupes pour une meilleure gestion • Importer facilement des configurations existantes dans Panorama	• Avoir une visibilité complète des applications dans le DC • Contrôler le trafic entre les VM par applications pour limiter l'exposition • Prévenir la propagation des attaques connues et inconnues dans le DC • Adapter dynamiquement les règles aux changements dans le DC	• Aller au délà des IPS traditionnels pour empêcher toute menace connue sur l'ensemble du traffic en un seul passage • S'appuyer sur l'analyse prédictive pour bloquer les attaques DNS • Rapidement identifier et protéger tous les devices OT et IoT non gérés grâce au Machine Learning
VM-SERIES SUR AMAZON WEB SERVICES (AWS)	**VM-SERIES SUR MICROSOFT AZURE**	**VM-SERIES SUR GOOGLE CLOUD PLATFORM**
• Implémenter des règles pour sécuriser les applications dans le VPC Amazon® • Comprendre les différentes VM-Series pour les cas d'usage AWS • Protéger le déploiement AWS en bloquant une attaque brute-force proactivement	• Déployer des VM Series dans Azure • Autoriser les applications et prévenir les menaces dans Azure • Publier des métriques PanOS grâce à l'intégration des VM-series dans Azure • Rediriger le trafic des VM pour la tolérance de panne	• Déployer des VM-Series dans GCP • Améliorer la sécurité native de GCP par une protection contre les attaques avancées • Utiliser Policy Optimizer pour passer des règles basées port vers des règles applicatives • Adapter dynamiquement les règles de sécurité dans GCP grâce aux VM-Series et aux DAG (Dynamic Address Groups)

MIEL ACADEMY :
FORMATIONS PALO ALTO NETWORKS

Miel est un centre de formation ATP pour Palo Alto Networks depuis près de 10 ans.
Nos formateurs ont tous une très solide expérience avant-vente et après-vente afin de délivrer la formation la plus pertinente possible.

Nos sessions inter-entreprises se déroulent à Paris, à Bièvres (91) et ponctuellement en région. Nous proposons aussi des sessions sur-mesure en « intra » pour un minimum de 3 participants.

Il est également possible de suivre des formations virtuelles avec formateurs, en ligne, pour toutes les dates sur Paris et Bièvres.

Les formations disponibles sont les suivantes :

PAN-EDU-210
Firewalls 9.X : Essentials - Configuration et Management
5 jours - PCNSA / PCNSE

PAN-EDU-214
Firewalls 9.X : Configuration avancée de la prévention des menaces
4 jours

PAN-EDU-260
Cortex XDR 2 : Prevention, Analysis and Response
3 jours

PAN-EDU-330
Firewalls 9.X: Troubleshooting avancé des firewalls. 3 jours - PCNSE

PAN-EDU-220
Panorama 9 : Administration
2 jours - PCNSE

PAN-EDU-318
Prisma Access SASE Security Design and Operation - 3 jours

La Plateforme Palo Alto Networks