GUIDE DES LICENCES PRODUITS

EXCLUSIVE NETWORKS

paloalto NETWORKS

Produit/Solution	Type	Description	Licence	Pré-requis / Informations complémentaires
STRATA				
Firewall nouvelle-génération	Matériel/ Châssis	Inspection du contenu du trafic réseau, pour détecter et bloquer les menaces connues et inconnues, selon l'approche single-pass.	Plateforme de base en version matérielle. Dans les architectures à haute disponibilité (HA), les équipes doivent disposer de licences identiques. Des licences en pack destinés à ce type d'architecture sont proposées à prix réduit. Abonnements associés : Threat Prevention, URL Filtering, Wildfire, Global Protect et DNS Security Service.	Disponible en versions matérielle et virtuelle. Dimensions basées sur les performances/la bande passante requise. Estimations possibles à partir du nombre d'utilisateurs, des sessions simultanées, du déchiffrement SSL, etc.
App-ID	PAN-OS	Identification automatique des applications à l'aide de multiples mécanismes.	Inclus dans le Firewall nouvelle-génération.	Inclus par défaut dans le système d'exploitation de la plateforme.
User-ID	PAN-OS	Définition de stratégies spécifiques permettant d'activer en toute sécurité des applications (sortantes ou entrantes) en fonction des utilisateurs ou groupes d'utilisateurs.	Inclus dans le Firewall nouvelle-génération.	Inclus par défaut dans le système d'exploitation de la plateforme.
Content-ID	PAN-OS	Inspection et filtrage du contenu du trafic traversant le firewall nouvelle-génération. Réduction des risques associés aux transferts non-autorisés de données et de fichiers. Blocage de fichiers par type. Possibilité de définir quelles applications sont autorisées à transférer des fichiers. Blocage des transferts de fichiers entrants ou sortants indésirables et filtrage des données afin de contrôler le transfert d'informations sensibles (numéros de carte de crédit, sécurité sociale, etc.).	Inclus dans le Firewall nouvelle-génération.	Inclus par défaut dans le système d'exploitation de la plateforme.
Threat Prevention (Prévention des cyber menaces)	Abonnement	Protection contre les cyber menaces et exploits grâce à la fonctionnalité IPS (Intrusion Prevention System). Blocage des activités C&C grâce au module anti-spyware. Blocage des transferts de fichiers malveillants grâce à la protection anti-malware.	Associé au Firewall nouvelle-génération. Licence indépendante.	- -
URL Filtering (Filtrage des adresses URL)	Abonnement	Accès sécurisé au web. Accès bloqué aux sites malveillants et sites de phishing.	Associé au Firewall nouvelle-génération. Licence indépendante.	- -
DNS Security Service (Service de sécurité DSN)	Abonnement	Analyse prédictive, pour stopper les attaques utilisant le DNS pour se connecter aux serveurs C&C ou pour exfiltrer des informations. L'intégration étroite avec le Firewall nouvelle-génération permet d'offrir une protection automatisée. Les outils tiers complémentaires ne sont plus nécessaires. Les menaces cachées dans le trafic DNS sont rapidement identifiées grâce aux renseignements partagés sur les menaces et au machine learning. Cette protection cloud est mise à jour automatiquement : les entreprises disposent ainsi d'un nouveau point de contrôle critique permettant de bloquer les attaques DNS.	Associé au Firewall nouvelle-génération. Licence indépendante.	Ce service bloque les nouveaux domaines malveillants grâce au machine learning. Neutralise le DNS Tunelling. Se substitue à des outils tiers isolés et accélère les mise à jour relatives aux cyber menaces, via le recours au cloud. Abonnement à Threat Prevention et version PAN-OS 9.0 du Firewall nouvelle-génération nécessaires.
Global Protect	Accès à distance sécurisé - VPN	Protection de n'importe quel utilisateur/périphérique, où qu'il soit, grâce à la fonctionnalité VPN.	Fonctions d'accès à distance VPN SSL pour Windows et Mac incluses dans la version standard. Fonctionnalités disponibles avec la licence Global Protection : VPN SSL pour iOS, android, Linux, Chromebooks, Windows 10 UWP ; VPN SSL sans client et contrôles HIP (Host Identity Protocol).	Accès distant sécurisé « always-on ». Firewall nouvelle-génération requis.
Wildfire	Abonnement	Le plus grand service cloud d'analyse de logiciels malveillants au monde : détection et prévention des cybermenaces inconnues. En cas de détection d'une cybermenace inconnue auprès d'un client, une mise à jour est automatiquement générée pour protéger l'ensemble des clients de la plateforme, en seulement cinq minutes.	Mode Cloud : Licence par abonnement pour le firewall nouvelle-génération. Mode Installation locale : modèle hardware simple. Inclus dans la version standard du service TMS (Traps Management Service).	Partage global des menaces : une menace détectée sur un client bénéficie à tous les utilisateurs de Wildfire. Firewall nouvelle-génération et/ou TMS requis.
SD-WAN	Abonnement	La technologie SD-WAN sert à répartir le trafic sur des réseaux étendus (WAN). Elle permet de déterminer automatiquement l'itinéraire le plus efficace entre les différents sites distants.	Associé au firewall nouvelle génération. Licence indépedante.	PAN OS 9.1
Panorama	Gestion	Gestion et surveillance des Firewalls nouvelle-génération, de manière centralisée. Définition des configurations, des politiques, des mises à jour et des rapports à partir d'une console unique, pour l'ensemble de l'environnement informatique.	Licences basées sur le nombre de firewalls gérées. 3 options de licence : 25, 100 ou + de 1000 firewalls nouvelle-génération. Options de mise à niveau disponibles : 25>100, 100>+1.000 Disponible en versions matérielle (appliance) et virtuelle (MV).	Firewall nouvelle-génération requis.

2020-04

GUIDE DES LICENCES PRODUITS

EXCLUSIVE NETWORKS

paloalto NETWORKS

Produit/Solution	Type	Description	Licence	Pré-requis / Informations complémentaires
PRISMA				
Firewall nouvelle génération virtualisé	VM-Series	Ce Firewall virtualisé fournit toutes les fonctionnalités du Firewall nouvelle-génération en version virtuelle, pour une utilisation en environnements cloud privés et publics.	Plateforme de base en version virtuelle. Pour les architectures HA (haute disponibilité), chaque équipe doit disposer de sa propre licence. Trois packs disponibles : Basique : machine virtuelle et accompagnement. Bundle 1 : machine virtuelle, licence TP et accompagnement. Bundle 2 : machine virtuelle, licences TP, URLF, WF, GP, DNS et accompagnement.	Ce Firewall virtualisé peut être déployé en environnement cloud public (AWS, Azure, GCP, Alibaba, Oracle Cloud) et en cloud privé (VMWare ESX, NSX, KVM, OpenStack, Hyper-V, Nutanix, Cisco ACI). Utilisation possible dans le cadre d'un Enterprise License Agreement (ELA).
Prisma Access	Sécurité distribuée en entreprise	Prévention des cyberattaques en succursales. Protection des déploiements SDWAN et des utilisateurs mobiles grâce au Firewall nouvelle-génération (SaaS). Déploiement et exécution automatisés des services de sécurité.	Sites distants : Licences basées sur le débit (minimum 200 Mo) Utilisateurs : Licences par nombre d'utilisateurs (200 utilisateurs)	Solution SaaS ; pas de déploiement HW. Offre Opex. Panorama et Cortex Data Lake requis.
Prisma Cloud	Sécurité/ conformité Cloud	Monitoring continu des services sur l'infrastructure cloud publique. Contrôle continu de la conformité réglementaire. Monitoring continu de la sécurité, validation de la conformité et des rapports, protection complète du stockage, simplification des opérations de sécurité et validation réglementaire continue de l'infrastructure cloud. Découverte et classification des données présentes dans les conteneurs et évaluation de l'exposition des données sensibles, sur la base de différentes règles définies.	Licences basées sur le nombre de charges de travail (workloads) à protéger.	Fonctionnalités de remédiation automatique pour les données exposées. Possibilité de mise en quarantaine des logiciels malveillants. Service SaaS.
Prisma SaaS	Sécurité/ conformité en SaaS	Etablissement d'une connexion directe aux applications SaaS pour la classification des données, la prévention des fuites de données et la détection des menaces. Les clients sont ainsi en mesure de sécuriser leurs applications professionnelles SaaS.	Licences basées sur le nombre d'utilisateurs. La licence actuelle couvre toutes les applications à protéger.	Mode service 100% sans agent ni proxy. Cette solution communique directement avec les applications SaaS et examine les données, quel que soit l'appareil ou l'emplacement d'où elles proviennent. Pas de connexion et donc pas d'incidence sur la latence ou la bande passante des applications. Solution CASB, en SaaS. 250 utilisateurs minimum.
CORTEX				
Cortex XDR Prevent	Protection avancée des postes de travail	Solution de protection des postes de travail. Elle empêche l'exécution de fichiers malveillants, qu'ils soient apparentés à des campagnes connues ou à des attaques encore inédites. Les administrateurs peuvent effectuer des analyses périodiques pour identifier les menaces latentes et se conformer aux exigences réglementaires. Les informations fournies par les postes de travail permettent de contextualiser les cyber incidents pour mieux réagir.	Licences basées sur le nombre d'appareils protégés (minimum 200). Wildfire inclus. *Pack Firewall nouvelle-génération+Traps disponible, pour une protection intégrée des appareils et du réseau. Ce pack est disponible pour 50, 100, 150 ou 200-500 appareils, avec les firewalls nouvelle-génération suivants : PA-220, PA-820, PA-820, PA-850 et plateformes virtuelles.	Techniques de prévention multiples : blocage des logiciels malveillants connus et exploits 0-day. Console de gestion SaaS : Traps Management Service (TMS). Permet de protéger les postes de travail, serveurs et appareils mobiles. Agent compatible avec les systèmes d'exploitation Windows (de XP SP3 à W10), Linux, Android et Mac OS (pas iOS).
Cortex Data Lake (alias Logging Service)	Collecteur de logs via le cloud	Possibilité de stocker les journaux de manière centralisée, sur le cloud.	Licence basée sur le nombre de téraoctets bruts. 1 ou 3 ans. Pour déterminer les dimensions, vous pouvez utiliser le Cortex Sizing Calculator : https://apps.paloaltonetworks.com/logging-service-calculator.	Collecteur conçu pour les architectures d'envergure. Gestion des logs simplifiée. Collecte sécurisée des données logs du réseau, des appareils et du cloud. Utilisation efficace de ces informations pour la prévention des attaques. Firewall nouvelle-génération et/ou TMS requis. Minimum 1 To. Panorama nécessaire pour les logs des firewalls.
Cortex XDR Pro	Réponse aux cyber incidents	Visibilité complète sur le trafic réseau, sur le comportement des utilisateurs et sur l'activité des postes de travail. Simplification de la recherche de menaces, grâce à la corrélation des événements provenant de différentes plateformes de Palo Alto Networks. Analyse facile de chaque menace détectée.	Licence basée sur le nombre de téraoctets bruts. 1 ou 3 ans.	Actions de réponse immédiate et élaboration de règles de comportement permettant de détecter et répondre aux activités malveillantes. Collecte des événements Traps. Nécessite un minimum de 30 jours de rétention des logs. Cortex Data Lake requis. Minimum 1 To.
Cortex XSOAR	Orchestration	Orchestration des solutions présentées chez le client à des fins d'automatisation.	Licence basée sur le nombre d'utilisateurs. 1 ou 3 ans.	Application de scénarios prédéfinis afin d'automatiser des tâches de réponse à incident.
Cortex Platform (alias Application Framework)	Solution API évolutive	Déploiement d'applications à partir d'un écosystème ouvert : les clients sont en mesure d'intégrer des applications à la plateforme de sécurisation de Palo Alto Networks.	Framework gratuit et open-source.	Cette solution permet de déployer rapidement de nouvelles fonctions et technologies de sécurité, tout en assurant leur parfaite intégration.

2020-04