Série VM

Principales fonctionnalités des pare-feu nouvelle génération de la série VM :

RECONNAISSANCE DE TOUTES LES APPLICATIONS, SUR TOUS LES PORTS, À TOUT MOMENT AVEC APP-ID™.

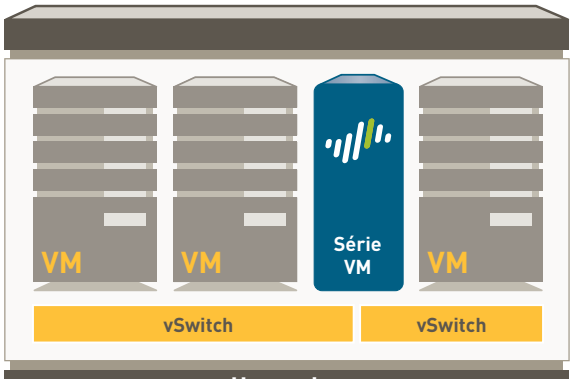
- Identification de l'application, indépendamment du port, du chiffrement (SSL ou SSH) ou de la technique d'évasion.
- Utilisation de l'application et non du port comme base de toutes les décisions stratégiques d'activation sécurisée : autoriser, refuser, planifier, inspecter ou prioriser le trafic.
- Classification des applications non identifiées pour des contrôles stratégiques, l'analyse des menaces, la création d'une App-ID personnalisée ou la capture de paquets pour un examen plus approfondi.

EXTENSION DES STRATÉGIES D'UTILISATION SÉCURISÉE DES APPLICATIONS À TOUS LES UTILISATEURS INDÉPENDAMMENT DE LEUR EMPLACEMENT GÉOGRAPHIQUE AVEC USER-ID™ ET GLOBALPROTECT™.

- Intégration sans agent à Active Directory, LDAP, eDirectory Citrix et Microsoft Terminal Services.
- Intégration à NAC, sans fil et autres référentiels utilisateurs non standard avec une API XML.
- Déploiement de stratégies cohérentes aux utilisateurs des plateformes Microsoft Windows, Mac OS X, Linux, Android ou iOS, quel que soit l'endroit où ils se trouvent.

PROTECTION CONTRE TOUTES LES MENACES - CONNUES ET INCONNUES - AVEC CONTENT-ID™ ET WILDFIRE™.

- Blocage d'une grande variété de menaces connues, notamment l'exploitation de vulnérabilités, les logiciels malveillants et les logiciels espions, sur tous les ports, indépendamment des techniques d'évasion utilisées.
- Limitation des transferts non autorisés de fichiers et de données sensibles. Contrôle de la navigation Web sans lien avec l'activité professionnelle.
- Identification des logiciels malveillants inconnus, analyse de plus de 100 comportements malveillants et livraison automatique d'une protection dans la prochaine mise à jour.



Pare-feu virtuel de la série VM

Les pare-feu de la série VM de Palo Alto Networks™ étendent l'utilisation sécurisée des applications aux environnements virtuels en apportant une réponse efficace aux problèmes de sécurité que soulève la virtualisation : application des politiques de sécurité aux machines virtuelles avec des adresses dynamiques et intégration à des systèmes d'orchestration grâce à une puissante interface de gestion XML.

La série VM propose trois modèles hautement performants : VM-100, VM-200 et VM-300, tous utilisant une architecture logicielle à une seule passe afin de minimiser les temps d'attente dans les environnements de data centers. Les plans de gestion et de données sont séparés pour qu'un processeur dédié puisse leur être affecté et ainsi garantir un accès permanent aux fonctionnalités de gestion, quel que soit le volume du trafic. Les modèles de la série VM sont équipés du système d'exploitation orienté sécurité PAN-OS™ qui permet aux entreprises d'activer des applications en toute sécurité au moyen d'App-ID, User-ID, Content-ID, GlobalProtect et WildFire.

CAPACITÉS GÉNÉRALES[1]	VM-300	VM-200	VM-100
Nombre maximum de sessions	250 000	100 000	50 000
Interfaces tunnel/tunnels VPN IPsec	2 000	500	25
Utilisateurs simultanés de GlobalProtect (SSL VPN)	500	200	25
Sessions de déchiffrement SSL	1 024	1 024	1 024
Certificats SSL entrants	25	25	25
Routeurs virtuels	3	3	3
Zones de sécurité	40	20	10
Nombre maximum de politiques	2 500	1 000	250
Objets d'adresse	5 000	2 500	2 500
PERFORMANCES			
Débit pare-feu (compatible App-ID)	1 Gbits/s		
Débit prévention des menaces	600 Gbits/s		
Débit VPN IPsec	250 Gbits/s		
Nouvelles sessions par seconde	8 000		

[1] Les capacités et performances sont mesurées en conditions de test idéales avec PAN-OS 5.0 et 8 cœurs de processeur.

paloalto NETWORKS
the network security company™

VIRTUALISATION	VM-300	VM-200	VM-100
HyperVisor	VMware ESXi 4.1 et ESXi 5.0		
Pilote réseau	VMXNet3		
Cœurs de processeur	2, 4 ou 8		
Mémoire (minimum)	4 Go		
Capacité du lecteur de disque (min./max.)	40 G /2 To		

MISE EN RÉSEAU

MODES D'INTERFACE :

- L2, L3, Tap, Virtual Wire (mode transparent)

ROUTAGE

- Modes de routage : OSPF, RIP, BGP, statique
- Dimensions de la table de routage (entrées par équipement/par routeur virtuel) : 1000/1000
- Transfert stratégique
- Adressage multicast : PIM-SM, PIM-SSM, IGMP v1, v2 et v3

HAUTE DISPONIBILITÉ

- Modes : Actif/Passif sans synchronisation de sessions
- Détection de défaillances : surveillance des chemins d'accès et des interfaces

ATTRIBUTION D'ADRESSES

- Attribution d'adresses aux dispositifs : client DHCP/PPPoE/statique
- Attribution d'adresses aux utilisateurs : serveur DHCP/relais DHCP/statique

IPV6

- L2, L3, Tap, Virtual Wire (mode transparent)
- Fonctionnalités : App-ID, User-ID, Content-ID, WildFire et déchiffrement SSL

VLAN

- Etiquettes VLAN 802.1q par équipement/par interface 4 094/4 094
- Interfaces max. : 1 024 (VM-300), 288 (VM-200), 100 (VM-100)

NAT/PAT

- Règles NAT max. : 1 000 (VM-300), 1 000 (VM-200), 125 (VM-100)
- Règles NAT max. (DIPP) : 200 (VM-300), 200 (VM-200), 125 (VM-100)
- Pool de ports et d'adresses IP dynamiques : 254
- Pool d'adresses IP dynamiques : 32,000
- Modes NAT : 1:1 NAT, n:n NAT, m:n NAT
- Dépassement d'abonnement DIPP (une seule adresse IP de destination par adresse IP et port sources) : 2
- NAT64

VIRTUAL WIRE

- Virtual Wire max. : 500 (VM-300), 100 (VM-200), 40 (VM-100)
- Types d'interface affectés à Virtual Wire : interfaces physiques et sous-interfaces

TRANSFERT L2

- Dimensions de la table ARP/dispositif : 1 000 (VM-300), 500 (VM-200), 500 (VM-100)
- Dimensions de la table MAC/dispositif : 1 000 (VM-300), 500 (VM-200), 500 (VM-100)
- Dimensions de la table de voisinage IPv6 : 1 000 (VM-300), 500 (VM-200), 500 (VM-100)

SÉCURITÉ

PARE-FEU

- Contrôle stratégique des applications, des utilisateurs et du contenu
- Protection contre les paquets fragmentés
- Protection contre les analyses de reconnaissance
- Protection contre le déni de service (DoS)/déni de service distribué (DDoS)
- Déchiffrement : SSL (entrant et sortant), SSH

WILDFIRE

- Identification et analyse des fichiers ciblés et inconnus pour rechercher plus de 100 comportements malveillants
- Création et livraison automatique d'une protection contre les nouveaux logiciels malveillants via la mise à jour des signatures
- Livraison des mises à jour des signatures en moins d'1 heure, fonctionnalités de journal de log/génération de rapports intégrées ; accès à l'API WildFire pour soumettre jusqu'à 100 échantillons et 1 000 requêtes par jour (abonnement requis)

FILTRAGE DES FICHIERS ET DES DONNÉES

- Transfert de fichiers : contrôle bidirectionnel sur plus de 60 types de fichiers
- Transfert de données : contrôle bidirectionnel sur les transferts non autorisés de numéros de cartes de crédit et de numéros de sécurité sociale
- Protection par téléchargements automatiques

INTÉGRATION DE L'UTILISATEUR (USER-ID)

- Microsoft Active Directory, Novell eDirectory, Sun One et autres annuaires LDAP
- Microsoft Windows Server 2003/2008/2008r2, Microsoft Exchange Server 2003/2007/2010
- Microsoft Terminal Services, Citrix XenApp
- API XML pour faciliter l'intégration aux référentiels utilisateurs non standard

VPN IPSEC (SITE À SITE)

- Protocole Key Exchange : clé manuelle, IKE v1
- Chiffrement : 3DES, AES (128 bits, 192 bits, 256 bits)
- Authentification : MD5, SHA-1, SHA-256, SHA-384, SHA-512
- Création d'un tunnel VPN dynamique (GlobalProtect)

PRÉVENTION DES MENACES (ABONNEMENT REQUIS)

- Protection contre l'exploitation des vulnérabilités du système d'exploitation et des applications
- Protection par flux contre les virus (notamment ceux incorporés aux fichiers HTML, Javascript, PDF et compressés), les logiciels espions et les vers informatiques

FILTRAGE DES URL (ABONNEMENT REQUIS)

- Catégories d'URL prédéfinies et personnalisées
- Mémoire cache du dispositif pour les dernières URL visitées
- Catégorie d'URL intégrée aux critères des stratégies de sécurité
- Informations sur les durées de navigation

QUALITÉ DE SERVICE (QOS)

- Priorisation du trafic en fonction de l'application, de l'utilisateur, de la source, de la destination, de l'interface, du tunnel VPN IPSec, etc.
- 8 classes de trafic avec des paramètres de bande passante maximum et prioritaire garantis
- Surveillance en temps réel de la bande passante
- Marquage Diffserv stratégique
- Interfaces physiques prises en charge pour la qualité de service (QoS) : 6 (VM-300, VM-200), 4 (VM-100)

SSL VPN/ACCÈS DISTANT (GLOBALPROTECT)

- Passerelle GlobalProtect
- Portail GlobalProtect
- Transport : IPSec ou alternativement SSL
- Authentification : LDAP, SecurID ou base de données locale
- SE client : Mac OS X 10.6, 10.7 (32/64 bits), 10.8 (32/64 bits), Windows XP, Windows Vista (32/64 bits), Windows 7 (32/64 bits)
- Prise en charge de clients tiers : Apple iOS, Android 4.0 et versions ultérieures, VPNC IPSec pour Linux

OUTILS DE GESTION, DE GÉNÉRATION DE RAPPORTS ET DE VISIBILITÉ

- Interface Web intégrée, interface de ligne de commande ou gestion centralisée (Panorama)
- Interface utilisateur multilingue
- Syslog, Netflow v9 et SNMP v2/v3
- Interface API REST basée sur XML
- Synthèse graphique des applications, catégories d'URL, menaces et données (ACC)
- Consultation, filtrage et export des journaux de trafic, menaces, WildFire, URL et de filtrage des données
- Génération de rapports entièrement personnalisables

Pour une description complète de l'ensemble des fonctionnalités des pare-feu nouvelle génération de la série VM, rendez-vous à l'adresse www.paloaltonetworks.com/literature.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Accueil : +1.408.573.4000
Ventes : +1.866.320.4788
Assistance : +1.866.898.9087

www.paloaltonetworks.com