Série PA-4000

Principales fonctionnalités des pare-feu nouvelle génération de la série PA-4000 :

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.

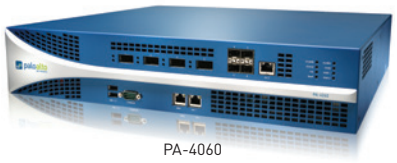
EXTENSION DES STRATÉGIES D'UTILISATION SÉCURISÉE DES APPLICATIONS À TOUS LES UTILISATEURS INDÉPENDAMMENT DE LEUR EMPLACEMENT GÉOGRAPHIQUE AVEC USER-ID™ ET GLOBALPROTECT™.

- Intégration sans agent à Active Directory, LDAP, eDirectory Citrix et Microsoft Terminal Services.
- Intégration à NAC, 802.1X 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

paloalto NETWORKS
the network security company™


PA-4060


PA-4050


PA-4020

Les pare-feu de la série PA-4000 de Palo Alto Networks™ sont composés de trois plateformes hautes performances, PA-4060, PA-4050 et PA-4020, toutes destinées aux déploiements de passerelles Internet et data centers haute vitesse. Le pare-feu A-4000 offre un débit pouvant atteindre 10 Gbits/s avec une mémoire et un processeur dédiés pour les principales fonctionnalités de mise en réseau, sécurité, prévention et gestion des menaces.

Le panneau arrière haute vitesse comporte un plan de contrôle et un plan de données séparés afin de garantir un accès permanent aux fonctionnalités de gestion, quel que soit le volume du trafic. Le pare-feu nouvelle génération PA-4000 utilise le système d'exploitation orienté sécurité PAN-OS™ moyen d'App-ID, User-ID, Content-ID, GlobalProtect et WildFire.

CAPACITÉS ET PERFORMANCES[1]	PA-4060	PA-4050	PA-4020
Débit pare-feu (compatible App-ID)	10 Gbits/s	10 Gbits/s	2 Gbits/s
Débit prévention des menaces	5 Gbits/s	5 Gbits/s	2 Gbits/s
Débit VPN IPsec	2 Gbits/s	2 Gbits/s	1 bits/s
Nouvelles sessions par seconde	60 000	60 000	60 000
Nombre maximum de sessions	2 000 000	2 000 000	500 000
Interfaces tunnel/tunnels VPN IPsec	4 000	4 000	2 000
Utilisateurs simultanés de GlobalProtect (SSL VPN)	10 000	10 000	5 000
Sessions de déchiffrement SSL	23 000	23 000	7 500
Certificats SSL entrants	300	300	25
Routeurs virtuels	125	125	20
Systèmes virtuels (base/max2)	25/125	25/125	10/20
Zones de sécurité	500	500	80
Nombre maximum de politiques	20 000	20 000	10 000

[1] Les capacités et performances sont mesurées en conditions de test idéales au moyen de PAN-OS 5.0.

[2] L'ajout de systèmes virtuels au nombre de base nécessite l'achat d'une licence séparée.

Pour une description complète de l'ensemble des fonctionnalités du pare-feu nouvelle génération PA-4000, rendez-vous à l'adresse www.paloaltonetworks.com/literature.

CARACTÉRISTIQUES MATÉRIELLES

ENTRÉE/SORTIE

- PA-4060 : (4) XFP 10 gigabit, (4) SFP Gigabit
- PA-4050, PA-4020 : (16) 10/100/1000, (8) SFP gigabit

ENTRÉE/SORTIE GESTION

- (2) haute disponibilité 10/100/1000, (1) gestion hors-bande 10/100/1000, (1) port console DB9

CAPACITÉ DE STOCKAGE

- Disque dur 160 Go

ALIMENTATION (CONSO MOY. / MAX.)

- Alimentation CA redondante 400W (175W/200W)

BTU/H MAX.

- 682

TENSION D'ENTRÉE (FRÉQUENCE D'ENTRÉE)

- 100-240VCA (50-60Hz)

CONSOMMATION DE COURANT MAX.

- 2,5A@100VACc

TEMPS MOYEN ENTRE DÉFAILLANCES (MTBF)

- 7,18 ans

COURANT D'APPEL MAX.

- 50A@230VCA ; 30A@120VCA

EN RACK (DIMENSIONS)

- 2U, rack standard 19" (8,89 cm (H) x 41,91 cm (P) x 44,45 cm (L))

POIDS (BOÎTIER SEUL/AVEC L'EMBALLAGE)

- 14,97 kg/18,14 kg

SÉCURITÉ

- UL, CUL, CB

EMI (POTENTIEL D'INTERFÉRENCE ÉLECTROMAGNÉTIQUE)

- FCC classe A, CE classe A, VCCI classe A, TUV

CERTIFICATIONS

- Norme FIPS 140 de niveau 2, certification Critères Communs EAL2, ICSA, UCAPL

ENVIRONNEMENT

- Température de fonctionnement : 32 à 122 °F, 0 à 50 °C
- Température de non fonctionnement : -4 à 158 °F, -20 à 70 °C

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) : 20 000/20 000 (PA-4060, PA-4050), 10 000/10 000 (PA-4020)
- Transfert stratégique
- Protocole PPPoE (Point-to-Point Protocol over Ethernet)
- Trames Jumbo : Taille de trame max. : 9 210 octets
- Adressage multicast : PIM-SM, PIM-SSM, IGMP v1, v2 et v3

HAUTE DISPONIBILITÉ

- Modes : Actif/Actif, Actif/Passif
- 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. : 4 096 (PA-4060, PA-4050), 2 048 (PA-4020)
- Interfaces agrégées (802.3ad)

NAT/PAT

- Règles NAT max. : 4 000 (PA-4060, PA-4050), 1 000 (PA-4020)
- Règles NAT max. (DIPP) : 250 (PA-4060, PA-4050), 200 (PA-4020)
- Pool de ports et d'adresses IP dynamiques : 254
- Pool d'adresses IP dynamiques : 16,234
- 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) : 8 (PA-4060, PA-4050), 4 (PA-4020)
- NAT64

VIRTUAL WIRE

- Virtual Wire max. : 2,048 (PA-4060, PA-4050), 1,024 (PA-4020)
- Types d'interface affectés à Virtual Wire : interfaces physiques et sous-interfaces

TRANSFERT L2

- Dimensions de la table ARP/équipement : 20 000 (PA-4060, PA-4050), 10 000 (PA-4020)
- Dimensions de la table MAC/équipement : 20 000 (PA-4060, PA-4050), 10 000 (PA-4020)
- Dimensions de la table de voisinage IPv6 : 5 000 (PA-4060, PA-4050), 2 000 (PA-4020)

SÉCURITÉ

PARE-FEU

- Contrôle stratégique des applications, des utilisateurs et du contenu
- Protection contre les paquets fragmentés
- Protection contre les analyses avec 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 uniques
- 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 bit, 192 bit, 256 bit)
- 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 le stockage des 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) : 12

SSL VPN/ACCÈS DISTANT (GLOBALPROTECT)

- Passerelle GlobalProtect
- Portail GlobalProtect
- Transport : IPSec ou alternativement SSL
- Authentification : LDAP, SecurID ou base de données locale
- OS 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, CLI ou gestion centrale (Panorama)
- Interface utilisateur multilingue
- Syslog et SNMP v2/v3
- 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 un complément d'information sur l'ensemble des fonctionnalités du pare-feu nouvelle génération PA-4000, 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