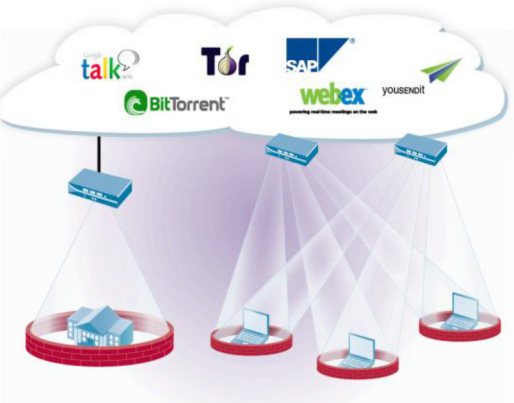
# Des produits encore plus performants.
## Le leader des firewalls nouvelle génération accélère !

Alors que les firewalls Palo Alto Networks sont considérés comme les plus avancés technologiquement, la société américaine a décidé de frapper une fois de plus un grand coup en présentant sa plus grosse mise à jour depuis la création du produit. Palo Alto Networks annonce simultanément un nouveau produit : GlobalProtect, une nouvelle série de plateformes matérielles : PA-5000 et une mise à jour majeure de son OS : PAN-OS4.0

### GLOBAL PROTECT : Contrôle d'intégrité pour tous les utilisateurs




**GlobalProtect** : système destiné à protéger les utilisateurs et les données situés hors du périmètre réseau.
Il est composé de clients embarqués sur les postes et de licences à activer sur les firewalls. Il permet au poste de détecter la passerelle PAN-OS la plus proche et de bénéficier de la visibilité et du contrôle comme n'importe quel utilisateur du réseau.
GlobalProtect requière une licence globale appelée « Portal License » ainsi qu'une licence par passerelle correspondant à chacun des firewalls participant au système collaboratif de sécurité.

**Découverte réseau et connexion automatique**: Dès que le poste dispose d'une connectivité, le client GlobalProtect détecte automatiquement si l'utilisateur est dans le réseau ou hors du réseau, et se connecte automatiquement à la passerelle la plus proche de manière transparente

**Profilage du host** : En plus des critères classiques de reconnaissance, le client remonte des informations sur l'état du poste (niveau de patch, encryption des disques…).

**Supporte** Windows XP, Vista, 7 en version 32- et 64-bit. Supporte Single Sign-on.

**PAN-OS4.0 : 50 nouvelles fonctionnalités pour un OS encore plus performant**

Près de 50 nouvelles fonctionnalités ont été ajoutées à la nouvelle mise à jour PAN OS 4.0. Elles augmentent l'avance de Palo Alto dans les firewalls de nouvelle génération.

| APP-ID | USER-ID | MENACES ET DONNEES | FILTRAGE URL |
|---|---|---|---|
| • App-ID custom possible pour les applications inconnues<br>• Collecte de stat sur les applications et les menaces<br>• Décryption des tunnels SSH<br>• App-ID customs étendues à 6000 | • Support Windows 2003 64-bit; support Terminal Server Windows 2008 32- et 64-bit; Support XenApp 6<br>• Séquence d'authentification multi-annuaires<br>• Masquage des en-têtes " x-forwarded-for"<br>• Authentification portail captif par certificat<br>• Portail captif par port destination | • Détection comportementale de botnets<br>• Détection de virus dans les documents PDF<br>• Drive by download protection: blocage de téléchargement tout en autorisant la navigation<br>• Hold-down time scan détection: blocage d'une source pendant une durée de temps<br>• Attribut de temps pour les signatures IPS et customs<br>• Profil de protection DoS plus granulaire | • Logs et reporting possible sur la page Container, stylesheets, fichier JavaScript…<br>• Log URL étendu à 1023 Byte par URL<br>• Possibilité de Mise à jour manuelle de la DB URL |

| INTERFACE | ADMINISTRATION | PANORAMA | RESEAU |
|---|---|---|---|
| • Gestion des règles en "drag and drop"<br>• Edition des objets en pop-up dans la règle<br>• Création et édition d'objets intégrés dans le contexte de la règle | • Objets sur adresses de nom de domaine<br>• Stockage et formats de logs/événement configurable (y compris CEF pour ArcSight)<br>• Gestion du verrouillage de transaction de config. dans un contexte multi admin<br>• Support de SNMPv3<br>• Reporting étendu des VSYS (scheduler, UAR, summary reports, email forwarding)<br>• PCAP accessible via l'interface web | • Partage de config étendu (rulebases, objets & profiles)<br>• Stockage dynamique de logs via NFS<br>• Haute dispo<br>• UAR (User Activity Report) dispo dans Panorama<br>• Backups de config Exportable<br>• Rapport d'audit de configuration | • Haute dispo Actif/Actif<br>• Support IPv6 L2/L3<br>• Proxy DNS<br>• DoS : limite de sessions par IP source/dest<br>• Règles basées pays<br>• Routage VR à VR<br>• Virtual System comme destination de règle PBF<br>• plusieurs interfaces L3 non taguées possibles sur une seule interface physique<br>• NetConnect SSL-VPN : Notification d'expiration du mot de passe<br>• Support Mac OS |

**SERIE PA-5000 : Classification complète du trafic jusqu'à 20Gbps**

L'innovation matérielle de Palo Alto Networks continue grâce à la série PA-5000. Elle permet de traiter le trafic jusqu'à 20Gbps. Les performances sont inégalées pour la protection du data-center.



| PA-5060 | PA-5050 | PA-5020 |
|---|---|---|
| 20 Gbps FW | 10 Gbps FW | 5 Gbps FW |
| 10 Gbps menaces | 5 Gbps menaces | 2 Gbps menaces |
| 4 Gbps IPSec VPN - 20,000 Users VPN SSL | 4 Gbps IPSec VPN - 10,000 Users VPN SSL | 2 Gbps IPSec VPN - 5,000 Users VPN SSL |
| 4,000,000 sessions | 2,000,000 sessions | 1,000,000 sessions |
| Jusqu'à 225 VSYS | Jusqu'à 125 VSYS | Jusqu'à 20 VSYS |
| (4) SFP+ (10 Gig) I/O- (8) SFP (1 Gig) I/O -(12) 10/100/1000 | (4) SFP+ (10 Gig) I/O - (8) SFP (1 Gig) I/O - (12) 10/100/1000 | (8) SFP (1 Gig) I/O - (12) 10/100/1000 |