



Communiqué de presse  
Paris, le 8 juin 2009

## **PALO ALTO NETWORKS PLACE LA BARRE PLUS HAUTE DANS LA VISIBILITE ET LE CONTROLE DES APPLICATIONS AVEC LA DERNIERE VERSION DE SON FIREWALL DE NOUVELLE GENERATION**

***PAN-OS 3.0 : ajout de la QoS permettant la gestion de la bande passante en Multi-Gigabit et l'intégration des clients distants VPN SSL***

---

**Palo Alto Networks™, le leader des pare-feux de nouvelle génération, annonce aujourd'hui PAN-OS 3.0, la dernière version de son Operating Système déjà primé par de nombreuses récompenses dans le milieu des pare-feux. PAN-OS 3.0 comprend de nouvelles fonctionnalités importantes, comme la QoS et l'intégration des clients VPN SSL. Ces nouvelles fonctionnalités permettent en outre aux entreprises d'utiliser de nouvelles applications tout en gérant les risques inhérents à l'utilisation de ces applications.**

---

Les entreprises utilisent un éventail d'applications Internet, de plus en plus large pour des raisons culturelles ou professionnelles, dans le but d'être toujours plus présentes auprès de leurs clients, d'augmenter leur chiffre d'affaire... Les techniques de sécurisation d'accès à Internet continuent de filtrer sur un mode obsolète « *Bloque ou autorise* », sans permettre de granularité, ni d'intelligence pour reconnaître ces nouvelles applications. Selon le cabinet Gartner, *"d'ici à 2012, les entreprises qui utilisent les filtres 'bloquer ou ignorer' pour contrôler l'accès à Internet, s'exposent à une augmentation des coûts liés aux incidents de sécurité de 2 à 4 fois supérieurs, par rapport aux entreprises qui utilisent des stratégies basées sur 'comprendre et contrôler'... Les éditeurs de solutions de sécurité basées sur une approche de 'tout bloquer', devront développer des solutions permettant plus de granularité dans le contrôle."*<sup>1</sup>

PAN-OS 3.0 apporte de la gestion de trafic directement sur le pare-feu, garantissant de la bande passante aux applications critiques pour l'activité de l'entreprise. Les fonctions principales du pare-feu Palo Alto offrent une visibilité et un contrôle granulaire uniques des applications, ce qui apporte aux entreprises un large éventail de contrôles tels que : autoriser, refuser, autoriser pour certains utilisateurs ou fonctions, détecter les menaces et aujourd'hui gérer le trafic. Les administrateurs sont maintenant capables de gérer la bande passante consommée par les applications, ainsi que les priorités, directement à partir de la politique du pare-feu, plutôt que de supprimer les applications sans avoir de visibilité ni de contrôle. D'après le dernier rapport 'Application Usage

and Risk' (avril 2009), sur un échantillon de plus de 900 000 utilisateurs, plus de la moitié de la bande passante est utilisée par 28% des applications, dont la plupart sont non-professionnelles.<sup>2</sup>

*« A l'université Paul Cézanne Aix-Marseille III, nous ne bloquons pas les applications utilisées en interne par les chercheurs et les étudiants, mais nous devons nous assurer que celles-ci sont sûres »* déclare Dr. Alain BOCH, Chef d'exploitation du centre informatique interuniversitaire de St Jérôme. *« Palo Alto Networks nous apporte une très grande visibilité sur les applications et nous garantit qu'elles sont sans danger pour notre environnement. Cette granularité dans la reconnaissance des applications est vraiment un plus. Nous sommes particulièrement intéressés par les nouvelles fonctionnalités de la V3.00, notamment par la gestion de la bande passante. Ceci nous permettra de garantir toujours une disponibilité de la bande passante à nos applications les plus critiques, tout en simplifiant notre architecture réseau. »*

Répondant aux attentes des clients, PAN-OS 3.0 offre également des fonctionnalités du VPN SSL, permettant d'étendre le réseau tout en conservant le même niveau de sécurité et de visibilité, par le contrôle des utilisateurs, des applications et du contenu. Auparavant les entreprises avaient le choix entre un VPN ouvert mais non sécurisé, solution simple à faible coût, ou un portail extranet avec un haut niveau de sécurité, solution chère et complexe.

L'ajout de ces nouvelles fonctionnalités, tout en conservant des performances élevées, a été possible grâce à l'architecture 'Single Pass Parallel Processing' (SP3) de Palo Alto Networks— combinant une analyse des paquets en un seul passage avec du matériel dédié à des fonctions spécifiques. La fonction de QoS dans le PAN-OS 3.0 permet aux entreprises de gérer et 'prioriser' le trafic par application avec des performances en multi-gigabit, grâce à l'intégration des fonctions logicielles sur du matériel dédié. De la même manière, les nouvelles fonctionnalités du VPN SSL de PAN-OS 3.0 bénéficie du contrôle et de la visibilité des applications, couplé à du matériel dédié au traitement SSL.

*« Les applications ne sont pas des menaces, mais elles peuvent véhiculer un risque »* déclare Olivier BOUSQUET, Responsable Commercial France Palo Alto Networks. *« En tant que spécialiste du pare-feu, Palo Alto Networks utilise un modèle de sécurité qui offre aux entreprises la souplesse dont elles ont besoin pour adopter de nouvelles applications, tout en gérant le risque inhérent. Et ce en allant beaucoup plus loin que les modèles classiques, qui se contentent de détecter et supprimer les nouvelles applications ».*

#### **Prix et disponibilité**

Les nouvelles fonctionnalités de PAN-OS 3.0, le VPN SSL et la QoS, sont gratuites pour les clients sous contrat de maintenance. PAN-OS 3.0 sera disponible au téléchargement courant juin.

#### **À propos de Palo Alto Networks**

Palo Alto Networks est le leader des firewalls de nouvelle génération, permettant d'offrir une visibilité et une politique granulaire du contrôle des applications et du contenu sans précédent – par utilisateur et non juste par adresse IP – et non au détriment des performances (plus de 10Gbps).

Basés sur sa technologie brevetée App-ID, les firewalls de Palo Alto Networks identifient et contrôlent les applications avec précision – sans tenir compte du port, du protocole, de tactique

évasive ou du chiffrement SSL – et scannent le contenu pour arrêter les menaces et prévenir les pertes de données. Les entreprises peuvent aujourd’hui utiliser sans contrainte le Web 2.0 en maintenant une visibilité et un contrôle complets et en réduisant de manière significative le coût total de possession au travers d’un équipement consolidé.

Pour plus d’informations : [www.paloaltonetworks.com](http://www.paloaltonetworks.com)

**Note 1** – Gartner, Inc., “Predicts 2009: Infrastructure Protection Isn’t a Monolithic Function,” John Pescatore, et al, 19 Décembre 2008.

**Note 2** – “Application Usage and Risk Report,” Palo Alto Networks, 20 Avril 2009.

Palo Alto Networks, le logo Palo Alto Networks et App-ID sont des marques déposées de Palo Alto Networks, Inc. aux Etats Unis. Toutes les autres marques et noms commerciaux utilisées ou mentionnées dans ce document appartiennent à leurs propriétaires respectifs.

#### **CONTACT PRESSE:**

#### **SCENARII**

Laurence Dutrey / Majida Guettaoui

Tél. : 01 58 88 39 59 / 39 04

ldutrey@itgspr.fr / mguettaoui@itgspr.fr