Palo Alto Networks classé parmi les visionnaires dans le Magic Quadrant des pare-feu de réseau d'entreprise

Sunnyvale, Californie, 22 mars 2010 - Palo Alto Networks™, spécialiste de la sécurité des réseaux, a été placé par Gartner, Inc. dans le quadrant des visionnaires de son classement Magic Quadrant des pare-feu de réseau d'entreprise.[1]

Selon le rapport, « Gartner a constaté en 2009 que les pressions exercées par le marché accéléraient la demande de pare-feu de nouvelle génération capables de détecter et de bloquer des attaques sophistiquées, et d'appliquer des règles de sécurité granulaires au niveau applicatif (plutôt que des ports et des protocoles). »[2]

« Le passage rapide des applications s'exécutant en interne dans le centre de traitement de données à un mode d'exécution externalisé en tant que service (voire, à terme, en ligne) et ce que Gartner appelle la "consumérisation de l'informatique" ont redéfini rapidement la "frontière de la confiance" et les types de contrôle de sécurité au niveau de celle-ci », ajoute Gartner.[3]

Dans son analyse, Gartner a évalué le pare-feu de nouvelle génération de Palo Alto Networks en fonction de sa "capacité d'exécution" et de "l'étendue de sa vision".

Grâce à la technologie de Palo Alto Networks, les entreprises peuvent identifier précisément les applications, analyser le contenu afin de bloquer les menaces et empêcher la fuite de données au moyen d'un dispositif unique. En réduisant le nombre de dispositifs de sécurité sur leurs réseaux, les entreprises réduisent à la fois leurs investissements et leurs coûts d'exploitation.

« De toute évidence, le rapport de Gartner confirme l'émergence de Palo Alto Networks comme architecte incontournable de l'avenir de la sécurité des réseaux », a déclaré René Bonvanie, vice-président du marketing mondial de Palo Alto Networks. « Les applications Enterprise 2.0 jouent un rôle de plus en plus décisif dans l'augmentation de la productivité des entreprises. Malheureusement, elles introduisent également des menaces. Notre pare-feu permet aux informaticiens de protéger le parc de leur entreprise contre les nouvelles menaces liées aux applications Enterprise 2.0. »

Recommandations de Gartner dans "Defining the Next-General Firewall",[4] rapport publié en octobre 2009 :

- Si vous n'avez pas encore déployé de solution de prévention des intrusions sur le réseau, demandez un pare-feu de nouvelle génération à l'occasion de la prochaine mise à jour.

- Si vous avez déployé à la fois des pare-feu et un dispositif de prévention des intrusions, synchronisez le cycle de mise à jour des deux technologies et migrez vers un pare-feu de nouvelle génération.

- Si vous utilisez des services de sécurité périmétrique administrés, envisagez d'opter pour des services de pare-feu de nouvelle génération lorsque vous renouvellerez votre contrat.

Pare-feu de nouvelle génération de Palo Alto Networks : fonctionnement
Palo Alto Networks a résolu les problèmes liés aux pare-feu classiques en combinant trois technologies d'identification offrant la visibilité et le contrôle des applications, des utilisateurs et du contenu.

- **App-ID** identifie exactement les applications en cours d'exécution sur le réseau, ainsi que les risques associés. Les administrateurs peuvent ainsi déployer des règles

complètes de contrôle de l'utilisation des applications pour le trafic entrant et sortant.

- **User-ID** s'intègre aux services d'annuaire de l'entreprise (par exemple, Microsoft Active Directory et les autres annuaires LDAP), afin de mettre en corrélation l'activité réseau et les utilisateurs et les groupes plutôt que les adresses IP. Ce module offre une parfaite visibilité des applications et permet l'instauration de règles ainsi que la journalisation et le reporting des événements.
- **Content-ID** combine un moteur de prévention des menaces en temps réel et une base de données complète d'URL. Cette technologie détecte et bloque un large éventail de menaces, limite le transfert non autorisé de fichiers et de données, et contrôle la navigation sur le Web sans rapport avec le travail.

Les DSI peuvent ainsi identifier avec précision les applications en cours d'exécution sur leur réseau et prendre des décisions informées pour améliorer l'ensemble de leur politique de sécurité.

Des informations sur plus de 950 applications identifiées par Palo Alto Networks ont été publiées dansApplipedia, du centre de recherche sur les applications et les menaces de la société. Pour connaître l'actualité, les commentaires et les dernières découvertes sur les applications et les menaces, rendez-vous sur http://www.paloaltonetworks.com/researchcenter/.

À propos du Magic Quadrant

Le Magic Quadrant a été publié le 15 mars 2010 par Gartner, Inc. Protégé par des droits d'auteur, il est réutilisé avec autorisation préalable. Le Magic Quadrant est une représentation graphique d'un marché à l'instant T et pour une période donnée. Il illustre l'analyse faite par Gartner du positionnement de certains fournisseurs par rapport à ses propres critères, définis pour le marché en question. Gartner ne cautionne aucun fournisseur, produit ou service décrit dans le Magic Quadrant et ne recommande pas aux acheteurs potentiels de ne sélectionner que les fournisseurs figurant dans le quadrant des "Leaders". Le Magic Quadrant doit être considéré exclusivement comme un outil de recherche, et non comme un guide d'achat. Gartner décline toute garantie, expresse ou tacite, liée à cette étude, y compris toute garantie de qualité marchande ou d'adéquation à un usage particulier.

À propos de Palo Alto Networks

Palo Alto Networks™ est spécialiste de la sécurité des réseaux. Ses pare-feu de nouvelle génération offrent une visibilité sans précédent et un contrôle granulaire des règles concernant les applications et le contenu - par utilisateur et non seulement par adresse IP - jusqu'à 10 Gb/s sans dégradation des performances. Reposant sur la technologie en cours d'homologation App-ID™, les pare-feu de Palo Alto Networks identifient et contrôlent les applications avec précision, quels que soient le port, le protocole, la tactique d'évasion et le chiffrement SSL employés. Ils analysent le contenu, bloquant les menaces et évitant les fuites de données. Les entreprises peuvent enfin bénéficier de la technologie Web 2.0 et conserver une visibilité et un contrôle complets, tout en réduisant considérablement le prix de revient total de leur parc au travers d'un équipement consolidé. Pour plus d'informations, rendez-vous surhttp://www.paloaltonetworks.com.

[1] Gartner "Magic Quadrant for Enterprise Network Firewalls", par Greg Young et John Pescatore, 15 mars 2010.

2 Gartner "Magic Quadrant for Enterprise Network Firewalls", par Greg Young et John Pescatore, 15 mars 2010, page 1.

3 Gartner “Magic Quadrant for Enterprise Network Firewalls”, par Greg Young et John Pescatore, 15 mars 2010, page 1.

4 Gartner “Defining the Next-Generation Firewall” par John Pescatore et Greg Young, 12 octobre 2009, page 1.