SONICWALL INTEGRE DES SERVICES ANTISPAM DANS SES PARE-FEU

*Service puissant, totalement intégré, plus efficace qu'une solution classique hébergée.
C'est une première sur le marché de la sécurité : facilité d'utilisation, antispam complet et efficace et possibilité pour l'utilisateur de mettre en quarantaine en un seul clic*

Paris, 16 juillet 2009 : SonicWALL, Inc. (NASDAQ: SNWL), le leader de la sécurisation des infrastructures réseau, annonce aujourd'hui la disponibilité de son service antispam (Comprehensive Anti-spam Service CASS), une solution assurant une protection avancée contre le spam et qui s'intègre parfaitement avec les firewalls UTM de SonicWALL. Ce nouveau service est conçu pour être très facilement activé sur les appliances de sécurité TZ, NSA et E-class.
En un simple clic, il commence à filtrer le trafic email SMTP (Simple Mail Transfer Protocol) afin d'éliminer le spam, les courriers de phishing et même les emails contenant des virus.

Ce service hybride de type cloud computing facilite la configuration tout en optimisant la protection et, lorsqu'il est activé, arrête le spam avant qu'il ne pénètre le réseau d'entreprise. La solution permet également aux administrateurs informatiques de mettre en quarantaine certaines boites de courrier indésirable, une première sur le marché de la sécurité. Le service antispam se différencie des autres services intégrés aux pare-feu. C'est en effet un véritable antispam destiné aux entreprises et non un simple filtre se basant sur des listes noires ou une liste OEM.

Les courriers indésirables augmentant dans le monde entier, 94 % des emails échangés sont indésirables ou contiennent des menaces comme du spam, des courriers de phishing et des messages infectés. Le spam est donc passé de simple « désagrément » à une véritable men ace pour les entreprises.

Autoriser l'entrée de ce trafic dangereux sur le réseau de l'entreprise peut non seulement affecter les communications mais également la productivité de la société. Ceci est d'autant plus vrai dans les environnements peu ou mal protégés comme les PME et les entreprises aux reseaux distribués géographiquement. En s'intégrant directement dans le firewall, cette solution SonicWALL devient capable d'analyser chaque paquet, sur chaque protocole : des actions que les solutions hébergées ne savent tout simplement pas délivrer. Les entreprises qui mettront en place le service antispam de SonicWALL (CASS) seront donc à même de supprimer les courriers indésirables au niveau de la passerelle, avant même qu'ils ne pénètrent sur le réseau : l'activité du réseau est donc préservée, la bande passante mieux utilisée et la productivité des employées est bien meilleure.

« Le service antispam de SonicWALL permet aux PME et aux entreprises aux reseaux distribués géographiquement de lutter contre le spam au niveau de la passerelle réseau. Le réseau d'entreprise n'en est que mieux protégé » explique Edward Cohen, Vice Président de l'unité Email Security chez SonicWALL. « Les petites entreprises sont désormais protégées contre la prolifération des menaces transmises par email. Elles ont désormais la possibilité de n'autoriser que les emails sains et désirés à atteindre le serveur. »

Les entreprises étendues géographiquement recevant des emails en différents endroits peuvent activer le service CASS sur les pare-feu distants SonicWALL afin réduire le trafic réseau contenant du spam. Il en résulte donc un système de défense complet et efficace contre le spam, le phishing, les virus et l'ensemble des menaces transmises par email, qui sont chaque jour plus nombreuses, complexes et élaborées.

« Notre solution précédente ne semblait pas intercepter tous les spams et mes utilisateurs se plaignaient fréquemment, demandant pourquoi le service de filtrage ne savait pas arrêter ces messages indésirables. A chaque message indésirable que je recevais, je devais comprendre pourquoi et comment il avait été autorisé » explique Andy Gee, directeur informatique chez Royal Food Service. « Le service antispam CASS de SonicWALL a été, pour nous, un excellent choix. Nous sommes en effet mieux protégés mais n'avons pas été obligés d'investir dans une nouvelle appliance. Nous avons donc gagné de l'espace dans nos racks et n'avons plus à nous inquiéter de la consommation d'énergie. Je ne me préoccupe plus de rien. Je sais que si le firewall fonctionne, le service fonctionne également. Par ailleurs, mes utilisateurs ne se plaignent plus, cela me fait gagner un temps considérable. »

Fonctionnalités clés comprises dans le service CASS :

- **Administration avancée de la réputation (ARM**) : basée sur la réputation de l'adresse IP de l'expéditeur afin de rejeter les courriers indésirables, le spam, les courriers de phishing avant même qu'ils n'atteignent le réseau. L'ARM supprime le recours aux services de blacklisting, qui sont généralement moins efficace, plus lents et souvent source de faux positifs.
- **Gestion avancée et de type cloud computing des contenus (ACM) :** élimine les courriers indésirables restants via la technique reconnue de lutte contre le spam de SonicWALL. La conception de type cloud computing utilise ces techniques antispam sans avoir d'impact sur le firewall et la productivité réseau en général.

- **Routage flexible des emails indésirables :** permet de classer les courriers indésirables comme spam, spam potentiel, phishing, phishing potentiel, virus et probable virus. Permet d'assurer le contrôle et à la conformité aux politiques internes à l'entreprise et aux standards de sécurité.
- **Boite de courrier indésirable pour Outlook :** permet de configurer rapidement des boîtes « courriers indésirables ». Les utilisateurs peuvent ainsi y stocker tous leurs messages indésirables. Les utilisateurs peuvent recevoir un résumé des messages indésirables dont ils se serviront pour visualiser (en format texte) les messages et les libérer si besoin.
- **L'antivirus GRID de SonicWALL est automatiquement activé avec le service CASS** afin de détecter les emails transmis via le SMTP et les rediriger, comme défini par l'administrateur (ex : rejeté ou effacé) à la passerelle.
- **Listes blanches et noires intégrées :** elles sont intégrées aux appliances réseau de SonicWALL, parallèlement avec le reporting et les journaux de logs.

Pour plus d'informations, connectez-vous à : http://www.sonicwall.com

Vous cherchez des informations mises à jour sur les menaces à la sécurité transmises par email ?

Connectez-vous au site du réseau GRID de SonicWALL à l'adresse suivante :

www.sonicwall.com/us/11605.html.

À propos de SonicWALL, Inc

SonicWALL s'engage à améliorer les performances et la productivité des petites et des grandes entreprises, ainsi qu'à diminuer les coûts et la complexité d'un réseau sécurisé. SonicWALL a déjà vendu plus d'un million d'applications via un réseau international de dix mille partenaires de canal. Ainsi, des dizaines de millions d'utilisateurs du monde entier peuvent contrôler et sécuriser leurs données professionnelles. SonicWALL conçoit, développe et produit des solutions étendues de sécurisation des réseaux, d'accès sécurisé à distance, de protection permanente des données (stockage et réparation inclus), de techniques organisationnelles et de gestion professionnelle. Pour trouver plus d'informations sur l'entreprise, rendez-vous sur son site web à http://www.sonicwall.com/.

Safe Harbor Regarding Forward-Looking Statements

Certain statements in this press release are "forward-looking statements" within the meaning of the Private Securities Litigation Reform Act of 1995. The forward-looking statements include but are not limited to statements regarding the benefits of the benefits associated with the Network Security Appliance Series and the benefits of the integration of Application Firewall into the Network Security Appliance Series These forward-looking statements are based on the opinions and estimates of management at the time the statements are made and are subject to certain risks and uncertainties that could cause actual results to differ materially from those anticipated in the forward-looking statements. In addition, please see the "Risk Factors" described in our Securities and Exchange

Commission filings, including our Annual Report on Form 10-K for the year ended December 31, 2006, for a more detailed description of the risks facing our business. All forward-looking statements included in this release are based upon information available to SonicWALL as of the date of the release, and we assume no obligation to update any such forward-looking statement.