Communiqué de presse

Contacts:
Agence
'Just Say It PR' Le Savoir Dire
Sandra Logut
01 44 61 81 84
sandra@just-say-it.com

WatchGuard
Rym Sullivan
06 72 32 85 47
Rym.Sullivan@watchguard.com

WatchGuard établit une nouvelle référence en matière de sécurité réseau et dévoile un système d'exploitation révolutionnaire pour les boîtiers UTM

Le nouveau système d'exploitation Fireware XTM de WatchGuard offre une gamme complète de fonctions inédites de sécurité, d'administration réseau et de gestion

Paris, le 12 Mai 2009 – WatchGuard® Technologies, un acteur mondial spécialiste des solutions de sécurité et de connectivité réseau évolutives, dévoile WatchGuard Fireware XTM, son nouveau système d'exploitation pour les boîtiers de sécurité WatchGuard. Ce nouveau système d'exploitation va permettre aux clients de WatchGuard d'enrichir les fonctions de leurs boîtiers pare-feu de gestion unifiée des menaces (Unified Threat Management ou UTM) pour intégrer de nouveaux outils de sécurité, d'administration réseau et de gestion.

Le nouveau système d'exploitation de WatchGuard, Fireware XTM, protège les réseaux en leur apportant des fonctions de sécurité innovantes, notamment en termes de contrôle HTTPS intégral, de sécurité de la VoIP et de blocage des applications de messagerie instantanée et peer-to-peer. En outre, Fireware XTM intègre de nouveaux outils d'administration réseau, tels que le clustering ou l'équilibrage de charge. Enfin, le nouveau système d'exploitation complète les fonctions de gestion avec des outils de contrôle d'accès par rôle, une gestion multiboîtier centralisée et un reporting amélioré. La combinaison de ces éléments fait de Fireware XTM le système d'exploitation le plus performant développé par WatchGuard pour répondre aux besoins actuels des environnements dynamiques d'entreprise et faire face aux menaces en constante augmentation.

« Notre vision d'une gestion des menaces évolutive nous conduit à permettre aux clients d'adapter ou de renforcer leur architecture de sécurité », déclare Eric Aarrestad, Vice-président Marketing de WatchGuard Technologies. « Fireware XTM fournit aux entreprises une nouvelle solution exceptionnelle qui maintient une parfaite sécurité de leurs réseaux, ressources et données sensibles » .

Fireware XTM, une protection inégalée des environnements dynamiques d'entreprise

Les connexions HTTPS servent souvent à des opérations de paiement sur le Web (par exemple, la banque en ligne) et à des transactions critiques dans des systèmes d'information d'entreprise. Le trafic HTTPS étant chiffré, il échappe au contrôle des administrateurs réseau en raison de l'absence de visibilité des paquets. Ceci

ouvre les portes du réseau aux attaques de logiciels malveillants et autres menaces pernicieuses, telles que le détournement de cookies HTTPS.

Fireware XTM permet désormais aux administrateurs d'éliminer efficacement le vecteur de menaces réseau HTTPS. Grâce à la technologie WatchGuard de proxy HTTPS qui intercepte, analyse et reconstitue les flux de données HTTPS, les administrateurs peuvent contrôler, informer et protéger avec précision les utilisateurs contre la réception de types de fichiers dangereux.

Avec une croissance prévue de 20,1 %, les services de VoIP représentent à coup sûr l'un des marchés informatiques se développant le plus rapidement, ce qui en fait également l'un des vecteurs de menaces les plus exposés pour les réseaux d'entreprise. En conséquence, des menaces telles que les attaques DoS sur des réseaux VoIP, le pillage d'annuaire et le vishing sont en vif essor.

Contrairement à certaines solutions UTM qui offrent essentiellement une traduction des adresses réseau pour occulter un système VoIP, Fireware XTM assure une protection au niveau applicatif pour les protocoles SIP et H.323. Ces fonctions de sécurité masquent les systèmes VoIP d'entreprise tout en les renforçant pour résister aux attaques de pillage d'annuaire, au buffer overflow et à d'autres menaces VoIP majeures.

Les réseaux de bots (ordinateurs piratés contenant des logiciels malveillants) représentent aussi un risque majeur et une responsabilité pour les entreprises. De nombreux réseaux de bots utilisant les mêmes protocoles que des applications métier légitimes (par exemple, la messagerie instantanée), les administrateurs sont confrontés à un choix limité : éliminer l'application ou le risque d'infection, perte de ressources ou contrôle.

Fireware XTM permet de tirer parti des applications telles que la messagerie instantanée (IM) et de bénéficier d'une protection contre les réseaux de bots. Fireware XTM assure un contrôle des applications ainsi qu'une identification des ports et des protocoles pour garantir la validité et la sécurité du trafic lié aux applications. En outre, la fonction de contrôle HTTPS de WatchGuard fonctionne conjointement au blocage des applications IM et P2P, qui déjoue même les bots utilisant un chiffrement pour tenter d'échapper à la détection.

Fireware XTM, renforcer la sécurité et améliorer l'administration du réseau

Les utilisateurs demandent que leurs réseaux soient pleinement opérationnels en permanence. Pour répondre à ce besoin tout en offrant une protection évolutive, Fireware XTM permet un clustering intégral des boîtiers afin que les entreprises puissent respecter les exigences de haute disponibilité, avec équilibrage de charge actif/actif, basculement transparent, synchronisation complète des sessions et possibilité d'ajouter une capacité de débit haute sécurité selon la croissance du réseau.

Chaque réseau étant unique et nécessitant des fonctions différentes, WatchGuard a conçu son nouveau système pour un maximum de souplesse. Fireware XTM permet aux administrateurs réseau d'utiliser un boîtier pare-feu UTM WatchGuard de multiples manières. Cela comprend la gestion du mode transparent, la redirection HTTP pour les serveurs proxy-cache, la multidiffusion via des tunnels VPN, la prise en charge NAT/VPN et la possibilité d'affecter plusieurs VLAN sur des interfaces externes.

Pour le collaborateur nomade qui a besoin de maintenir une connectivité VPN sécurisée lorsqu'il se déplace entre des points d'accès, Fireware XTM assure l'itinérance tout en utilisant un VPN mobile IPSec. Grâce à cette fonction, les tunnels VPN restent actifs alors que les utilisateurs se déplacent entre des points d'accès ou de connexion 3G. Les utilisateurs disposent d'un degré de liberté sans précédent avec une sécurité élevée.

Fireware XTM, faciliter la gestion de la sécurité

Les administrateurs conviendront que la sécurité informatique vaut également par sa gestion. WatchGuard propose de nouvelles fonctions permettant aux administrateurs de travailler selon leurs préférences. Ils peuvent désormais gérer leurs boîtiers via une interface de ligne de commande (CLI), une interface Web ou la console WatchGuard System Manager (WSM). En outre, l'interface CLI permet aux administrateurs de créer et d'utiliser leurs outils de script favoris pour automatiser des tâches courantes, d'où des gains de temps et une réduction des erreurs.

Pour renforcer davantage la protection et la gestion, Fireware XTM offre désormais un contrôle d'accès par rôle. Les entreprises peuvent ainsi créer et attribuer des rôles de gestion UTM/pare-feu à des administrateurs désignés selon les meilleures pratiques de sécurité et une règle de droit d'accès minimal.

Afin de respecter les toutes dernières exigences réglementaires, les administrateurs sont confrontés au défi de normaliser et d'automatiser le recueil et la gestion des configurations de pare-feu et d'unité. WatchGuard System Manager, qui est fourni avec tous les modèles Firebox X Core et Peak, permet aux administrateurs de disposer d'une gestion complète et centralisée des différents boîtiers WatchGuard : planification des mises à jour de logiciels, configuration des données, création de procédures et possibilité de diffuser globalement des modifications vers toutes les unités WatchGuard.

Pour répondre aux besoins des entreprises en matière de rapports détaillés, (conformité réglementaire, résolution des incidents de sécurité, contrôle de l'utilisation du Web, impératifs de facturation, etc), WatchGuard System Manager propose de nouveaux rapports d'audit axés sur les enregistrements de contrôle d'accès par rôle, une génération de rapports personnalisés et de nouvelles options de filtrage. Ainsi les administrateurs peuvent obtenir rapidement les informations essentielles.

Prix et disponibilité de WatchGuard Fireware XTM

Fireware XTM est gratuit pour les clients actuellement abonnés à WatchGuard LiveSecurity. Le système d'exploitation est pris en charge par toutes les gammes WatchGuard e-Series de boîtiers pare-feu UTM Edge, Core et Peak. Fireware XTM sera disponible sous 45 jours.

À propos de WatchGuard Technologies, Inc.

Depuis 1996, WatchGuard® Technologies, Inc. fournit des solutions de sécurité réseau, et permet à des centaines de milliers d'entreprises dans le monde entier de protéger leurs systèmes d'information. La gamme WatchGuard de boîtiers de gestion unifiée des menaces, câblés ou sans fil, et de solutions d'accès à distance VPN SSL permet une sécurité réseau évolutive, un contrôle réseau inégalé ainsi qu'une administration complète. Les produits WatchGuard sont supportés par le service WatchGuard LiveSecurity® et des programmes innovants en termes de support, maintenance et formation. WatchGuard, dont le siège se trouve à Seattle (États-Unis), possède des bureaux en Amérique du Nord, Europe, sur la région Asie-Pacifique et en Amérique latine. Pour en savoir plus, rendez-vous sur http://www.watchguard.fr.