



WatchGuard lancia il nuovo Sistema Operativo per le appliance UTM che stabilisce nuovi standard per la Network Security

WatchGuard Fireware XTM fornisce una gamma estesa di nuove funzionalità avanzate per la sicurezza, il networking e la gestione delle reti

Milano, 22 aprile 2009 – WatchGuard® Technologies, fra i leader mondiali di soluzioni per la connettività e la sicurezza estensibile delle reti, presenta il nuovo sistema operativo **WatchGuard Fireware XTM** per le security appliance di WatchGuard. Con il nuovo sistema operativo i clienti WatchGuard possono estendere le capacità dei loro firewall UTM con una serie di nuove funzioni per la sicurezza, il networking e il management.

WatchGuard Fireware XTM protegge le reti aggiungendo funzioni innovative di sicurezza, quali il **controllo HTTPS in entrata e in uscita**, la **protezione VoIP** e il **blocco delle applicazioni Instant Messaging (IM) e Peer-to-Peer (P2P)**. Inoltre, Fireware XTM integra nuove opzioni avanzate di networking quali il clustering, il load-balancing (bilanciamento del carico server) e altre funzioni di rete. In aggiunta, il nuovo sistema operativo estende anche le capacità di gestione aggiungendo il controllo di accesso basato su ruoli (RBAC, role-based access control), la gestione centralizzata multi-box e avanzate funzionalità di reportistica. La combinazione di tutte queste caratteristiche fanno di Fireware XTM il più potente sistema operativo sviluppato da WatchGuard, ideale per le minacce in costante aumento e per gli attuali ambienti dinamici di business.

"Per WatchGuard con l' «eXtensible threat management» si dà al cliente la possibilità di estendere, aggiungere o aumentare la propria sicurezza di base," sostiene Eric Aarrestad, Vice Presidente Marketing di WatchGuard Technologies. "Con Fireware XTM le aziende hanno a disposizione un nuovo e formidabile strumento per la massima protezione delle loro reti, risorse e dati sensibili."

Fireware XTM. Sicurezza superiore per gli odierni ambienti dinamici di business

Le connessioni HTTPS sono spesso usate per le transazioni di pagamento sul web, così come per l'online banking e per transazioni delicate nei sistemi informatici aziendali. Dal momento che il traffico HTTPS è criptato, questo rappresenta un 'blind spot' per gli amministratori di rete, che non sono in grado di 'vedere' dentro questi pacchetti.

Ciò apre le porte della rete ad attacchi malware e ad altre insidiose minacce, come gli attacchi di cookie hijacking.

Con Fireware XTM, ora gli amministratori possono eliminare efficacemente le minacce derivanti dalla reti HTTPS. Grazie alla tecnologia **HTTPS proxy** di WatchGuard che

intercetta, scansiona e ricostruisce i flussi di dati HTTPS, gli amministratori possono accuratamente verificare, fare report e proteggere gli utenti dalla ricezione di file dannosi.

Con una crescita prevista del 20.1 %, il VoIP è sicuramente uno dei mercati IT in più rapida crescita, il che lo rende anche il più esposto veicolo di minacce all'interno delle reti aziendali. A causa di ciò, minacce quali attacchi DoS su reti VoIP, attacchi di directory harvesting e attacchi 'vishing' (evoluzione del phishing, effettuati tramite servizi di telefonia VoIP) sono rapidamente aumentati in popolarità.

Diversamente da alcune soluzioni UTM che forniscono semplicemente una traduzione dell'indirizzo di rete per oscurare un sistema VoIP, Fireware XTM fornisce l'application-level security per i protocolli SIP e H.323. Queste funzionalità di sicurezza oscurano i sistemi VoIP e allo stesso tempo li rafforzano per sostenere attacchi di directory harvesting, input validation hacks (buffer overflows) e le altre maggiori minacce derivanti dal VoIP.

Anche le botnets – computer infettati contenenti applicazioni malware – sono oggi elemento di grande preoccupazione per le aziende. Dal momento che molte botnets utilizzano lo stesso protocollo usato per applicazioni business, come l'instant messaging, gli amministratori di rete si trovano di fronte a poche soluzioni: eliminare l'instant messaging o rischiare attacchi botnet, perdita di risorse e controllo.

Con Fireware XTM gli amministratori possono beneficiare sia dell'instant messaging che, allo stesso tempo, della protezione dalle botnet. Fireware XTM fornisce l'application inspection, così come l'identificazione della porta e del protocollo, per assicurare che il traffico sia valido e sicuro. In aggiunta, il controllo HTTPS di WatchGuard lavora in tandem con il blocco delle applicazioni IM e P2P, che ferma anche quei bots che usano la criptazione nei loro tentativi di evadere il rilevamento.

Fireware XTM. Capacità di sicurezza e di networking più estese

Oggi gli utenti richiedono reti con un throughput continuo, di alto livello. Fireware XTM supporta funzionalità di clustering, soddisfacendo elevati requisiti, inclusi load balancing active/active, seamless fail-over, full session synchronization e la possibilità di aggiungere capacità di throughput ad elevata sicurezza quando la rete cresce.

Dato che ogni rete è unica e richiede capacità differenti, WatchGuard ha progettato il suo nuovo sistema operativo per la massima flessibilità di rete. Con Fireware XTM gli amministratori possono usare i firewall UTM WatchGuard in molte nuove modalità: supporto per il transparent mode, reindirizzamento HTTP per supportare i server proxy caching, supporto multicast per i tunnel VPN, NAT (network address translation) per branch office VPN, e l'abilità di assegnare multi-VLAN su interfacce esterne.

Per i lavoratori mobili che necessitano di mantenere connessioni VPN sicure, Fireware XTM supporta il roaming usando VPN Mobile con IPSEC. Con questa funzionalità, i tunnel VPN rimangono attivi mentre gli utenti si muovono fra diversi punti di connessione, APs

(access points) o 3G. Questo dà agli utenti un nuovo livello di libertà, insieme ad un'elevata sicurezza.

Fireware XTM. La sicurezza diventa più gestibile

Gli amministratori concorderanno che l'efficacia dell'information security dipende strettamente da come la si gestisce. WatchGuard introduce nuove funzioni che consentono all'amministratore di lavorare nel modo che preferisce. Con Fireware XTM gli amministratori possono gestire le loro appliances attraverso un'interfaccia a riga di comando programmabile (CLI - command line interface), web GUI o dalla console WatchGuard System Manager (WSM). Inoltre, con il controllo CLI, gli amministratori possono creare e usare i loro strumenti di script preferiti per automatizzare i task comuni, salvando tempo e riducendo gli errori.

Oltre ad aggiungere funzionalità di difesa maggiore e di controllo della gestione della rete, Fireware XTM ora supporta il controllo di accesso basato su ruoli (RBAC - Role Based Access Control). Questo controllo consente di creare e assegnare ruoli di gestione di firewall/UTM a specifici amministratori sulla base della best security practise e della regola del "least privilege rule".

Per soddisfare gli ultimi requisiti normativi, gli amministratori sono chiamati a standardizzare e automatizzare la gestione del firewall e le configurazioni del dispositivo. Con WatchGuard System Manager (WMS), incluso in tutte le appliance Firebox X Core e Peak, gli amministratori possono avere una gestione multi-box completa e centralizzata e il controllo delle appliance WatchGuard, inclusa la programmazione degli update dei software, la configurazione dei dati, la creazione di procedure di policy e la possibilità di pubblicare cambiamenti globalmente su tutti i dispositivi WatchGuard.

Le organizzazioni hanno bisogno di report dettagliati per diverse ragioni, che vanno dal Regulatory Compliance e Security Incident Troubleshooting, al monitoraggio dell'uso del web, a requisiti di fatturazione. WatchGuard System Manager offre nuovi report di verifica guidati da records di controllo accessi basato su ruoli, rapporti personalizzati e nuove opzioni di filtering, così che gli amministratori possono reperire velocemente le informazioni per loro più importanti.

WatchGuard Fireware XTM. Prezzi e disponibilità

Fireware XTM è gratuito per i clienti del servizio WatchGuard LiveSecurity. E' supportato da tutte le famiglie e-Series delle appliance firewall UTM Edge, Core e Peak. Il nuovo sistema operativo di WatchGuard sarà disponibile nella seconda parte del 2009.

Informazioni su WatchGuard Technologies, Inc.

WatchGuard fornisce soluzioni per la sicurezza delle reti. Con la famiglia di appliance espandibili Firebox X è in grado di rispondere alle esigenze di organizzazioni di ogni dimensione grazie alla potenza offerta in termini di performance, funzionalità e sicurezza. L'architettura Intelligent Layered Security di WatchGuard offre una protezione efficace contro le minacce emergenti e fornisce una piattaforma in grado di integrare i servizi aggiuntivi offerti dalla società. Tutti i prodotti WatchGuard sono corredati dall'abbonamento al servizio LiveSecurity, che fornisce agli utenti allarmi sulla vulnerabilità, aggiornamenti software, istruzioni sulla sicurezza forniti da esperti e assistenza al cliente personalizzata e autonomamente gestibile. La sede centrale di WatchGuard si trova a Seattle, Washington, mentre uffici sono presenti in tutta Europa e in Asia. Per maggiori informazioni visitare il sito www.watchguard.com

#

WatchGuard e LiveSecurity sono marchi registrati di WatchGuard Technologies, Inc. Tutti gli altri marchi citati sono proprietà dei loro rispettivi proprietari.

Per ulteriori informazioni:

WatchGuard Technologies

Tel: 011-9542.227

Fax: 011-9542.228

italy@watchguard.com

www.watchguard.com

Informazioni per la stampa:

SSP Communication

Lorenzo Giangiacomo

Tel. 039-6080085

lorenzo@sspcommunication.com

www.sspcommunication.com