

La risorsa più potente del sistema di difesa della rete

WatchGuard® fornisce una protezione Zero Day effettiva attraverso le funzionalità di Intelligent Layered Security delle appliance Firebox®X Unified Threat Management, consentendo di bloccare numerosi attacchi nuovi e sconosciuti senza utilizzare le firme.

- **Sicurezza di rete affidabile e proattiva**
- **Protegge da minacce nuove e sconosciute**
- **Protegge nel periodo di vulnerabilità**
- **Protezione decisamente superiore ai prodotti basati solo su firme**



Tecnologia eco-compatibile

Protezione Zero Day

Nel settore della sicurezza si parla molto di protezione "Zero Day" dagli attacchi ma le soluzioni offerte differiscono sostanzialmente per il tipo di protezione effettivamente fornita.

- **Le minacce Zero Day** sono attacchi nuovi o sconosciuti per i quali non è stata scritta una patch o una firma
- **Protezione Zero Day**, pertanto, significa proteggersi da una minaccia nuova e sconosciuta prima che sia scoperta la vulnerabilità e sia creato e lanciato l'attacco

Protezione Zero Day effettiva integrata nell'architettura Firebox® X

Intelligent Layered Security di Firebox X combina funzionalità chiave di protezione in grado di esercitare una difesa nei confronti di classi di attacchi e di proteggere da varianti ancora sconosciute. Alcune di queste funzionalità includono:

- **Protocol Anomaly Detection** blocca il traffico sospetto non conforme agli standard di protocollo stabiliti
- **Pattern Matching** contrassegna e rimuove dal sistema i file ad alto rischio, quali file con estensione .exe e file di script, virus, spyware e trojan, attraverso il controllo completo dell'intero pacchetto
- **L'analisi del comportamento** identifica e blocca il traffico proveniente da host che mostra comportamenti sospetti, quali attacchi DoS e DDoS e la scansione di porte e indirizzi

Ruolo delle firme in una soluzione di protezione

Alcuni produttori affermano di fornire una protezione Zero Day ma in realtà queste soluzioni di protezione si affidano semplicemente a una scansione basata su firme.

Le tecnologie di protezione basate su firme tracciano un identikit della minaccia dopo che l'attacco è stato sferrato e pertanto la protezione risulta disponibile quando questo

identikit, o firma, viene aggiunto al sistema. Soluzioni di questo tipo non forniscono una protezione Zero Day. Per loro natura, le firme sono reattive; non sono in grado di fornire protezione nei confronti di attacchi nuovi e sconosciuti senza un aggiornamento del database delle firme.

La scansione basata su firme fornisce un livello di protezione granulare nei confronti di spyware, virus, worm, trojan horse e minacce combinate identificando il codice nocivo conosciuto all'interno del traffico di rete e di file di importanza cruciale per l'azienda. Questa tecnica rappresenta solo un aspetto della soluzione Unified Threat Management completa.

*22 dei 30 più significativi virus e delle relative varianti rilasciati nel 2005 e nel 2006 sono stati bloccati per impostazione predefinita da Firebox®, proteggendo in tal modo i nostri clienti prima che fossero disponibili le firme.**

Il periodo di vulnerabilità

Le soluzioni basate su firme bloccano attacchi già identificati. La rete continua a essere esposta dal momento in cui viene lanciato un attacco fino a quando viene sviluppata e distribuita una firma o una patch.

Considerando la velocità e la distruttività degli attacchi, anche pochi minuti senza protezione possono avere risultati devastanti. La realtà è che a volte trascorrono ore, giorni o persino settimane prima che una firma o una patch sia sviluppata e distribuita e questo periodo di mancata protezione è l'incubo di ogni responsabile IT.

Protezione affidabile subito disponibile

Una effettiva protezione Zero Day disponibile prima che la vulnerabilità sia conosciuta è il cuore delle soluzioni di protezione Firebox X. Per implementare questa protezione, visitare www.watchguard.com

*Sulla base dei metodi di propagazione più comunemente utilizzati (SMTP)

WatchGuard protegge nel periodo di vulnerabilità



Protezione Zero Day significa essere protetti nei confronti di una minaccia nuova o emergente durante il periodo di vulnerabilità.

- **Protezione completamente integrata e versatile**
- **La protezione più completa della propria classe**
- **Include la prevenzione dagli attacchi Zero Day integrata**
- **Potenti servizi di protezione aggiungono maggiore protezione nelle aree critiche oggetto di attacchi**
- **Funzionalità unificate di gestione, monitoraggio e registrazione**



Tecnologia eco-compatibile

Sicurezza con protezione Zero Day effettiva

Le soluzioni Firebox® X Unified Threat Management di WatchGuard forniscono le funzionalità di protezione più complete della propria classe per una protezione completamente integrata e versatile nei confronti delle minacce di rete, inclusi:

- ✓ Spyware
- ✓ Virus
- ✓ Iniezioni SQL
- ✓ Trojan horse
- ✓ Spamming
- ✓ Overflow del buffer
- ✓ Worm
- ✓ Minacce combinate
- ✓ Attacchi DoS/DDoS
- ✓ Bot
- ✓ Attacchi basati sul Web
- ✓ Violazioni dei criteri

Unified Threat Management

Unified Threat Management (UTM) rappresenta una tendenza emergente nel mercato della protezione di rete. Le appliance UTM rappresentano l'evoluzione delle tradizionali appliance firewall e VPN in una soluzione che fornisce numerose funzionalità aggiuntive quali filtraggio URL, blocco dello spamming, protezione da spyware, prevenzione delle intrusioni e gateway antivirus, oltre a funzionalità integrate di gestione, monitoraggio e registrazione, tutte funzioni in precedenza gestite da più sistemi.

Protezione Zero Day integrata di base

Una potente protezione è alla base delle nostre soluzioni. Intelligent Layered Security (ILS) in Firebox X offre una protezione Zero Day effettiva immediatamente disponibile. Fornisce protezione nei confronti di minacce nuove e sconosciute prima che la vulnerabilità sia scoperta e che sia creato e lanciato un attacco. Molti produttori forniscono solo funzionalità di protezione basata su firme. Queste soluzioni reattive in realtà lasciano i clienti esposti a nuovi tipi di minacce fino a quando non si manifesta l'attacco e non viene creata e distribuita una firma aggiornata.

Potente difesa integrata multilivello

A differenza di molte appliance con gestione unificata delle minacce disponibili attualmente sul mercato, i livelli di protezione dell'architettura ILS del Firebox X operano insieme per rafforzare la sicurezza complessiva della rete. Grazie alle funzionalità software coordinate, ogni componente può coordinare la struttura di protezione complessiva. Ad esempio, quando Intrusion Prevention Service identifica un attacco, può indicare al firewall in che modo comportarsi.

Una comunicazione cooperativa tra livelli riduce e ottimizza l'elaborazione richiesta dalle funzioni di protezione. Il risultato è una protezione potente e prestazioni ottimizzate.

Potenti servizi di protezione per rafforzare le difese

Le soluzioni flessibili offerte consentono di aggiungere con facilità uno dei servizi avanzati di protezione per potenziare la protezione nelle aree critiche oggetto di attacchi e gestirle da una console di gestione integrata.

I servizi di protezione includono:

- **spamBlocker:** migliore servizio sul mercato, consente di riconoscere in tempo reale gli attacchi di spamming, con una percentuale di e-mail bloccate del 97%, con un numero incredibilmente basso di falsi positivi.
- **Gateway AV/IPS:** robusta protezione al gateway basata su firme contro virus, spyware, trojan e attacchi basata sul Web conosciuti.
- **WebBlocker:** per aumentare la produttività e diminuire i rischi per la protezione attraverso il blocco dell'accesso a contenuti Web nocivi e la gestione della navigazione in Internet degli utenti.

Il ruolo della gestione integrata

Sia gli esperti IT che i principianti avranno modo di apprezzare quanto la gestione integrata, il monitoraggio interattivo in tempo reale e le funzionalità di registrazione delle soluzioni UTM risultino semplici da utilizzare durante le attività di configurazione e gestione del sistema di protezione.

- Gestione centralizzata di più appliance
- Facile creazione e implementazione dei criteri di protezione a livello globale per semplificare la configurazione di criteri di protezione coerenti
- Monitoraggio e registrazione interattivi in tempo reale
- Interfaccia intuitiva per l'installazione e la gestione di tutte le funzionalità di protezione, inclusi i servizi di protezione

Importanti benefici in termini di costi e scalabilità

L'esecuzione di diversi software e appliance di protezione comporta costi in termini di tempo e budget che incidono sulle spese complessive per il reparto IT. Altre soluzioni UTM prevedono costi di licenza per ogni singolo utente o richiedono costi aggiuntivi per le funzionalità di logging e reporting. Le soluzioni UTM di WatchGuard non hanno prevedono costi per singolo utente o per il software di gestione e presentano un'unica interfaccia utente grafica. Ogni funzionalità di protezione, integrata e gestita centralmente, fornisce protezione su tutta la rete a tutti gli utenti configurati a monte di Firebox X.

L'unica limitazione è la vostra capacità di traffico. Quando si raggiunge tale capacità, è sufficiente attivare una chiave di licenza per l'aggiornamento a un modello superiore che fornisce subito velocità e capacità aggiuntive. È questo il modo meno faticoso e più economicamente vantaggioso per proteggere il proprio investimento in tecnologie di protezione della rete.



Stronger Security. Simply Done™

E-MAIL: italy@watchguard.com · VENDITE: +39-011-9542227 · WEB: www.watchguard.com

Non sono qui fornite garanzie esplicite o implicite. Tutte le specifiche sono soggette a modifica e tutte le funzionalità o i prodotti futuri saranno forniti in base alla disponibilità. © 2006 WatchGuard Technologies, Inc. Tutti i diritti riservati. WatchGuard, il logo WatchGuard, Firebox, Firewall e LiveSecurity, Peak e Stronger Security, Simply Done sono marchi o marchi registrati di WatchGuard Technologies, Inc. negli Stati Uniti e/o in altri paesi. Tutti gli altri marchi e nomi commerciali sono di proprietà dei rispettivi titolari. Numero di parte WGCE66355_0506