IBM Security Network Intrusion Prevention System

Protezione completa dall'evolversi delle minacce odierne

Punti principali

- Livelli di prestazioni senza precedenti senza compromettere un livello di sicurezza estremamente elevato
- Protezione di importanti beni aziendali quali reti, server, endpoint e applicazioni da minacce malevole
- Protezione costantemente aggiornata grazie alla ricerca IBM X-Force che consente di rimanere sempre "ahead of the threat"
- Costi e complessità ridotti grazie al consolidamento di singoli soluzioni e integrazioni con altri strumenti di sicurezza.

Le soluzioni IBM Security Network Intrusion Prevention System (IPS) sono state progettate per contrastare le minacce presenti in Internet prima che possano avere un impatto sul business. È disponibile la protezione preventiva (in grado di anticipare le minacce) offerta da IBM grazie alla combinazione di elevate prestazioni, un sistema di intelligence per la sicurezza e un motore di protezione modulare che garantisce convergenza della sicurezza. Grazie al consolidamento delle esigenze di sicurezza di rete per la protezione dei dati e delle applicazioni web, IBM Security Network IPS funge da piattaforma unica di sicurezza in grado di ridurre i costi e la complessità di implementazione e gestione di più soluzioni singole.

Nel corso della valutazione delle tecnologie di prevenzione delle intrusioni, le aziende spesso hanno difficoltà a bilanciare e ottimizzare i seguenti sei aspetti principali: prestazioni, sicurezza, affidabilità, implementazione, gestione e riservatezza.

IBM Security Network IPS offre in tutti i casi, prestazioni all'avanguardia, protezione preventiva contro le minacce basata sulla ricerca X-Force, alti livelli di disponibilità, implementazione e gestione più semplici e la sicurezza offerta da una assistenza clienti IBM all'avanguardia. Le aziende che desiderano trasferire la responsabilità di protezione della propria rete a un partner specializzato in sicurezza affidabile possono rivolgersi a IBM per la gestione della loro infrastruttura di sicurezza. I clienti IBM potranno inoltre sfruttare i vantaggi offerti da una vasta gamma di servizi di consulenza complementari per la valutazione, la progettazione, l'implementazione, la gestione e la formazione.

Livelli di prestazioni superiori senza compromessi

I sistemi di sicurezza dovrebbero migliorare le prestazioni di rete non ridurle. Le soluzioni IBM Security Network IPS mirate offrono velocità di trasmissione elevate, latenza ridotta e massima disponibilità per garantire l'efficienza delle attività di rete. Questo include inoltre la capacità di utilizzare un'ampia gamma di soluzioni di sicurezza, eliminando così la necessità di scegliere tra i più alti livelli di protezione e le prestazioni richieste per mantenere il livello di servizio necessario ad importanti applicazioni di business. Offrendo prestazioni all'avanguardia che superano i 20 Gigabit al secondo di throughput, le soluzioni IBM Security Network IPS offrono le prestazioni di cui avete bisogno offrendo al tempo stesso alti livelli di sicurezza.

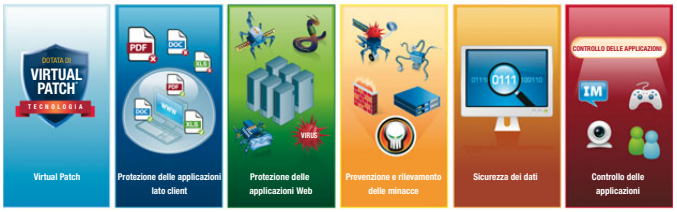
Consolidamento della sicurezza di rete grazie alla protezione preventiva

Grazie a un'architettura di prodotto modulare, le soluzioni IBM Security Network IPS garantiscono la convergenza della sicurezza grazie alla possibilità di aggiungere nuovi moduli di protezione in base all'evoluzione delle minacce. Questa architettura indirizza una vasta gamma di rischi di sicurezza dai worm e botnet, alle problematiche legate alla sicurezza dei dati e delle applicazioni web e permette alle soluzioni IBM Security Network IPS di garantire la protezione richiesta in termini di continuità aziendale, sicurezza dei dati e conformità.

Il team di ricerca e sviluppo IBM X-Force ha progettato la tecnologia IBM PAM (Protocol Analysis Module) e fornisce costanti aggiornamenti in grado di garantire una protezione preventiva delle minacce. I moduli di protezione specifici sono:

- La tecnologia *IBM Virtual Patch – Isola le vulnerabilità dai attacchi, indipendentemente dall'applicazione delle patch software*
- *Protezione delle applicazioni lato client – Protegge gli utenti finali dagli attacchi rivolti alle applicazioni più comunemente utilizzate quotidianamente come file Microsoft® Office, file PDF Adobe® , file multimediali e browser web*
- *Protezione avanzata della rete – Prevenzione avanzata delle intrusioni inclusa la protezione DNS (Domain Name System)*

Tecnologia IBM PAM (Protocol Analysis Module)



La tecnologia IBM PAM (Protocol Analysis Module) offre la convergenza della sicurezza per garantire una protezione di rete che va oltre il sistema IPS tradizionale, includendo la protezione delle applicazioni lato client, la sicurezza dei dati, la protezione web e il controllo delle applicazioni.

- *Sicurezza dati – Monitoraggio e identificazione di informazioni PII (personally identifiable information) e altri dati riservati non crittografati*
- *Sicurezza delle applicazioni Web – Protezione delle applicazioni web, Web 2.0 e database (stessa protezione di un "web application firewall"*
- *Controllo delle applicazioni – Recupero di banda e blocco di Skype, reti peer-to-peer e del tunneling.*

Questi moduli offrono soluzioni IBM Security Network IPS che proteggono le organizzazioni da una vasta gamma di minacce:

- *Malware inclusi worm e spyware*
- *Attacchi lanciati attraverso una botnet*
- *Rischi correlati all'uso della messaggistica istantanea e dei file P2P (peer-to-peer) come abusi della rete e perdita di dati*
- *Attacchi Dos (Denial of service) e DDoS (Distributed denial of service)*
- *Attacchi mirati contro applicazioni web come cross-site scripting e SQL injection*
- *Perdita di dati correlati al proprietario o ai dati sensibili*
- *Attacchi di tipo buffer overflow*
- *Attacchi lato client come quelli rivolti ai browser web.*

Il team di ricerca e sviluppo X-Force monitora il livello delle minacce Internet di tutto il mondo dal proprio centro dedicato per garantire una migliore e aggiornata protezione nelle soluzioni IBM Security Network IPS.

Alti livelli di disponibilità

I dispositivi nel flusso del traffico di rete devono essere estremamente affidabili. Le soluzioni IBM Security Network IPS offrono i più alti livelli di affidabilità e disponibilità. Ciò viene realizzato grazie a configurazioni ad alta disponibilità (attiva/attiva o attiva/passiva), alimentatori e unità disco ridondanti di tipo hot-swap. La nostra opzione di HA (alta disponibilità) geografico può utilizzare la gestione della porta per condividere le regole di protezione (es. blocco, messa quarantena) per garantire un failover sicuro verso un dispositivo in standby remoto.

Semplicità di implementazione

Ogni appliance IBM Security Network IPS viene fornito già configurato insieme alle policy di sicurezza predefinite e comprovate da X-Force. Questo fornisce una protezione di sicurezza "out of the box" immediata con la garanzia di un'attenta verifica da parte dei ricercatori X-Force per garantire i più alti livelli di accuratezza. IBM Security Network IPS offre inoltre un'architettura Layer-2 che non richiede la riconfigurazione della rete. Per consentire un adeguato livello di testing, gli amministratori di rete e della sicurezza possono scegliere facilmente una delle seguenti tre modalità operative:

- *Protezione attiva (modalità di prevenzione delle intrusioni)*
- *Rilevamento passivo (modalità rilevamento intrusioni)*
- *Simulazione in linea (simulazione prevenzione in linea).*

Gestione centralizzata della sicurezza

Gli appliance IBM Security Network IPS vengono gestiti a livello centrale dal sistema IBM Security SiteProtector. SiteProtector offre un sistema di configurazione e controllo, semplice e potente degli agent IBM unitamente a capacità avanzate di reporting, correlazione degli eventi e gestione completa degli allarmi. È compreso anche il supporto di gestione IPv6 degli appliance IBM Security Network IPS, compresa la capacità di visualizzare gli eventi IPv6 e gli indirizzi IP (Internet Protocol) origine/destinazione IPv6.

Affidarsi a un partner e a un'assistenza specializzata in sicurezza

IBM è l'azienda leader nel rilevamento e nella prevenzione delle intrusioni con una comprovata esperienza di assistenza clienti di livello superiore. IBM è stata una delle prime divisioni aziendali nel settore della sicurezza a ricevere la certificazione Global SCP (Support Centre Practices) ed è attualmente membro della SSPA (Service and Support Professionals Association) Advisory Board.

Perché IBM?

IBM è al corrente delle minacce che possono abbattersi sulla vostra rete ma anche dell'equilibrio fondamentale che deve esistere tra prestazioni e protezione. Di conseguenza, IBM ha implementato la propria tecnologia di sicurezza all'avanguardia per la prevenzione delle vulnerabilità per bloccare le minacce provenienti da Internet prima che colpiscano la vostra azienda. Con IBM Security Network IPS, otterrete una soluzione economica ed altamente efficiente che offre:

- *Protezione preventiva supportata dal team di ricerca e sviluppo IBM X-Force*
- *Tecnologia di sicurezza all'avanguardia che comprende la funzionalità IBM PAM per l'analisi approfondita dei pacchetti*
- *Elevate prestazioni che consentono di garantire la disponibilità di rete*
- *Semplicità di installazione, configurazione e gestione.*

Protezione preventiva che si adatta alla vostra rete

Con una linea completa di modelli ad alte prestazioni, la tecnologia IBM Security Network IPS è progettata per offrire una protezione senza compromessi per ogni livello di rete, proteggendo il vostro business da minacce interne ed esterne.

Specifiche tecniche

Modello	GX4004 -200	GX4004	GX5008	GX5108	GX5208	GX7412 -5	GX7412 -10	GX7412	GX7800
Caratteristiche prestazionali									
Throughput rilevato	Fino a 200 Mega bit al secondo (Mbps)	Fino a 800 Mbps	Fino a 1.5 Gbps	Fino a 2.5 Gbps	Fino a 4 Gbps	Fino a 5 Gbps	Fino a 10 Gbps	Fino a 15 Gbps	Fino a 20 Gbps+
Latenza media	<200 µs	<200 µs	<200 µs	<200 µs	<200 µs	<100 µs	<100 µs	<100 µs	<100 µs
Connessioni al secondo	35.000	35.000	37.000	40.000	50.000	600.000	600.000	600.000	650.000
Sessioni simultanee (max)	1.300.000	1.300.000	1.500.000	1.700.000	2.200.000	12.500.000	12.500.000	12.500.000	12.500.000
Caratteristiche fisiche									
Formato	1U	1U	2U	2U	2U	3U	3U	3U	3U
Altezza (poll/mm)	1.75/44	1.75/44	3.5/88	3.5/88	3.5/88	5.25/133	5.25/133	5.25/133	5.25/133
Larghezza (poll/mm)	16.9/429	16.9/429	16.9/429	16.9/429	16.9/429	Parte anteriore: 18.85/479 Parte posteriore: 17.28/439	Parte anteriore: 18.85/479 Parte posteriore: 17.28/439	Parte anteriore: 18.85/479 Parte posteriore: 17.28/439	Parte anteriore: 18.85/479 Parte posteriore: 17.28/439
Profondità (poll/mm)	15.5/394	15.5/394	21.5/546	21.5/546	21.5/546	26/662	26/662	26/662	26/662
Peso (libbre/kg)	24.5/11.1	24.5/11.1	40.0/18	40.0/18	40.0/18	55/25	55/25	55/25	55/25
Interfaccia di gestione	10/100/ 1000 (IPv6 sup portato)	10/100/ 1000 (IPv6 sup portato)	10/100/ 1000 (IPv6 supp ortato)	10/100/ 1000 (IPv6 supp ortato)	10/100/ 1000 (IPv6 supp ortato)	10/100/ 1000 (IPv6 suppo rtato)	10/100/ 1000 (IPv6 suppo rtato)	10/100/ 1000 (IPv6 supp ortato)	10/100/ 1000 (IPv6 supp ortato)
Protezione Inline di segmenti di rete	(2) 1 Gigabit Ethernet (GbE)	(2) 1 GbE	(4) 1 GbE	(4) 1 GbE	(4) 1 GbE	(2) 10/1 GbE + (6) 1 GbE	(2) 10/1 GbE + (6) 1 GbE	(2) 10/1 GbE + (6) 1 GbE	(4) 10/1 GbE
Interfacce di monitor	4×1GbE	4×1GbE	8×1GbE	8×1GbE	8×1GbE	4×10GbE (SFP+) + 12×1GbE (SFP)	4×10GbE (SFP+) + 12×1GbE (SFP)	4×10GbE (SFP+) + 12×1GbE (SFP)	8×10GbE (SFP+)
Tipi di supporti fisici supportati	RJ-45	RJ-45	RJ-45 o SFP/ mini-GBIC (1000 TX/SX/LX)	RJ-45 o SFP/ mini-GBIC (1000 TX/SX/LX)	RJ-45 o SFP/ mini-GBIC (1000 TX/SX/LX)	Direct Attach Copper, RJ-45, Fiber (SX/LX), 10G Fiber (SR/LR)	Direct Attach Copper, RJ-45, Fiber (SX/LX), 10G Fiber (SR/LR)	Direct Attach Copper, RJ-45, Fiber (SX/LX), 10G Fiber (SR/LR)	Direct Attach Copper, RJ-45, Fiber (SX/LX), 10G Fiber (SR/LR)

Specifiche tecniche

Modello	GX4004 -200	GX4004	GX5008	GX5108	GX5208	GX7412 -5	GX7412 -10	GX7412	GX7800
Alimentazione ridondante	No	No	Sì	Sì	Sì	Sì	Sì	Sì	Sì
Dischi ridondanti	No	No	Sì	Sì	Sì	Sì	Sì	Sì	Sì
HA	Bypass livello hardware integrato	Bypass livello hardware integrato	Attivo/ attivo; Attivo/ passivo; HA geografico; bypass esterno hardware (opzionale)	Attivo/ attivo; Attivo/ passivo; HA geografico; bypass esterno hardware (opzionale)	Attivo/ attivo; Attivo/ passivo; HA geografico; bypass esterno hardware (opzionale)	Attivo/ attivo; Attivo/ passivo; HA geografico; bypass esterno hardware (opzionale)	Attivo/ attivo; Attivo/ passivo; HA geografico; bypass esterno hardware (opzionale)	Attivo/ attivo; Attivo/ passivo; HA geografico; bypass esterno hardware (opzionale)	Attivo/ attivo; Attivo/ passivo; HA geografico; bypass esterno hardware (opzionale)
Parametri elettrici e ambientali									
Tipo di voltaggio e alimentazione	100 - 240 V, full range; 50/60 Hz								
Input current rating	5-3 A		8-4 A			10-5 A			
Temperatura operativa:	da 0° fino a 40° C (da 32° fino a 104° F)					da 5° fino a 35° C (da 41° fino a 95° F)			
Umidità relativa:	dal 5% fino all'85% a 40° C (104° F)					dall'8% fino all'80% a 28° C (82° F)			
Certificazione/dichiarazione di sicurezza	UL 60950-1, CAN/CSA C22.2 No. 60950-1, EN 60950-1 (CE Mark), IEC 60950-1, GB4943, GOST, UL-AR								
Certificazione/ dichiarazione EMC (Electromagnetic compatibility)	FCC Class A, Industry Canada Class A, AS/NZS CISPR 22 Class A, EN 55022 Class A (CE Mark), EN 61000-3-2 (CE Mark), EN 61000-3-3 (CE Mark), EN 55024 (CE Mark), VCCI Class A, KCC Class A, GOST Class A, GB9254 Class A, GB17625.1								
Dichiarazione ambientale	ROHS, WEEE e REACH								

*I dati delle prestazioni offerte per IBM Security Network IPS si basano su verifiche effettuate in condizioni di traffico misto TCP (Transfer Control Protocol)/UDP (User Datagram Protocol) indicative del consueto traffico reale. I fattori ambientali legati all'uso di un mix di protocolli diversi ed alla media delle dimensioni dei pacchetti sono diversi in ogni rete, quindi i risultati delle prestazioni rilevate possono variare di conseguenza. Il valore di throughput (IPS) di rete è stato stabilito, forzando un traffico di protocollo misto attraverso l'appliance e facendo una stima del throughput risultante senza alcuna perdita di pacchetti. Per il benchmark test, sono stati utilizzati gli appliance serie GX7 nella modalità di protezione in linea predefinita con la politica "Trust X-force"; Spirent Avalanche 3100 test gear, firmware 3.50 (o successivi); Traffico misto: HyperText Transfer Protocol (HTTP)=41%, HTTPS=17%, Simple Mail Transfer Protocol (SMTP)=10%, POP3=5%, File Transfer Protocol (FTP)=9%, DNS=15%, Simple Network Management Protocol (SNMP)=3%; traffico HTTP/HTTPS con object size da 44Kb con richieste GET HTTP/S 1.1 standard; Ricerca record A DNS standard; Richieste FTP GET di 15000 byte in burst da 2ms, traffico POP3 con "objects" di 100KB tra due mailbox "utenti", connessioni SMTP semplici senza trasferimento di oggetti, interrogazioni e risposte sullo stato SNMP.

Ulteriori informazioni

Per ulteriori informazioni sulle soluzioni IBM Security Network IPS, contattare il vostro responsabile commerciale o un Business Partner (BP) IBM o visitare il seguente sito Web: **ibm.com**/software/it/tivoli/solutions/threat-mitigation/

IBM Italia S.p.A.
Circonvallazione Idroscalo
20090 Segrate (Milano)
Italia

La home page di IBM Italia si trova all'indirizzo **ibm.com/**it

WGD03002-ITIT-04