IBM Security Network Intrusion Prevention System

Comprehensive protection from today's evolving threats

Highlights

- Unmatched levels of performance without compromising breadth and depth of security
- Protect business critical assets such as networks, servers, endpoints and applications from malicious threats
- Evolving protection powered by world renowned IBM X-Force® research to stay "ahead of the threat"
- Reduced cost and complexity through consolidation of point solutions and integrations with other security tools

IBM Security Network Intrusion Prevention System (IPS) solutions are designed to stop Internet threats before they impact your business. Preemptive protection—protection that works ahead of the threat—is available from IBM through its proprietary combination of line-speed performance, security intelligence and a modular protection engine that enables security convergence. By consolidating network security demands for data security and protection for web applications, IBM Security Network IPS serves as the security platform that reduces the cost and complexity of deploying and managing point solutions.

When evaluating intrusion prevention technology, businesses often struggle to balance and optimize the following six key areas: performance, security, reliability, deployment, management and confidence.

IBM Security Network IPS delivers on all six counts, with industry-leading performance, preemptive threat protection powered by X-Force research, high levels of availability, simplified deployment and management, and the confidence that comes with world-class IBM customer support. Organizations that want to transfer the burden of protecting their network to a trusted security partner can rely on IBM to manage their security infrastructure for them. IBM customers also benefit from a wide range of complementary consulting services for assessment, design, deployment, management and education.

Delivering superior performance without compromise

Security should enhance network performance, not detract from it. Purpose-built IBM Security Network IPS solutions offer high throughput, low latency and maximum availability to maintain efficient network operations. This includes the ability to utilize the full spectrum of security protections and eliminates the need to choose between the highest levels of security and the performance required to maintain service levels for business critical applications. By offering industry-leading performance beyond 20 Gbps of inspected throughput, IBM Security Network IPS solutions provide the performance you need, while delivering high levels of security.

Consolidating network security with preemptive protection

With its modular product architecture, IBM Security Network IPS solutions drive security convergence by adding entirely new modules of protection as threats evolve. This addresses a wide spectrum of security risk from worms and botnets to web application and data security issues and enables IBM Security Network IPS solutions to deliver the protection demanded for business continuity, data security and compliance.

The IBM X-Force research and development team designed the IBM Protocol Analysis Module (PAM) and provides the content updates that maintain ahead of the threat protection. Specific protection modules include:

- *IBM Virtual Patch® technology—Shielding vulnerabilities from exploitation, independent of a software patch.*
- *Client side application protection—Protects end users against attacks targeting applications used everyday such as Microsoft Office files, Adobe PDF files, multimedia files and web browsers.*
- *Advanced network protection—Advanced intrusion prevention including DNS protection.*

IBM Protocol Analysis Module Technology

The IBM Protocol Analysis Module (PAM) drives security convergence to deliver network protection that goes beyond traditional IPS including client-side application protection, data security, web application protection and application control.

- *Data security—Monitoring and identification of unencrypted personally identifiable information (PII) and other confidential data.*
- *Web application security—Protection for web apps, Web 2.0 and databases (same protection as web application firewall).*
- *Application control—Reclaim bandwidth and block Skype, peer-to-peer networks and tunneling.*

These modules enable IBM Security Network IPS solutions to protect organizations from a wide range of threats including:

- *Malware including worms and spyware*
- *Attacks launched by botnets*
- *Instant messaging and peer-to-peer related risks such as network abuse and data loss*
- *Denial of service (DoS) and distributed denial of service (DDoS) attacks*
- *Targeted attacks against web applications such as cross-site scripting and SQL injection*
- *Data loss related to proprietary or sensitive data*
- *Buffer overflow attacks*
- *Client-side attacks such as those targeting web browsers*

The X-Force research and development team tracks Internet threat levels around the world from its Global Threat Operations Center to enhance and update the protection in IBM Security Network IPS solutions.

Delivering high levels of availability

Devices placed in the flow of network traffic must be extremely reliable. IBM Security Network IPS solutions offer the highest levels of reliability and availability. This is accomplished through high availability configurations (active/active or active/passive), hot-swappable redundant power supplies and hot-swappable redundant hard drives. In addition, our geographic high availability option can use the management port to share quarantine blocking decisions to ensure secure failover to a geographically remote standby device if needed.

Providing ease of deployment

Each IBM Security Network IPS appliance comes preconfigured with the proven X-Force default security policy. This provides immediate security protection out of the box and is closely verified by X-Force researchers to ensure the highest levels of accuracy. IBM Security Network IPS also features Layer-2 architecture that does not require network reconfiguration. Network and security administrators can easily choose one of three operating modes including:

- *Active protection (intrusion prevention mode)*
- *Passive detection (intrusion detection mode)*
- *Inline simulation (simulates inline prevention)*

Centralizing security management

IBM Security Network IPS appliances are centrally managed by the IBM Security SiteProtector system. SiteProtector provides simple, powerful configuration and control of IBM agents, along with robust reporting, event correlation and comprehensive alerting. Also included is IPv6 management support of IBM Security Network IPS appliances, including the ability to display IPv6 events and IPv6 source/destination IP addresses.

Earning your confidence with security expertise and support

IBM is a leader in intrusion detection and prevention with an established record of superior customer support. IBM was one of the first in the security industry to receive Global Support Center Practices (SCP) Certification and is a member of the Service & Support Professionals Association (SSPA) Advisory Board.

Why IBM?

IBM understands the threats to your network and the critical balance between performance and protection. As a result, IBM has enabled its world-class vulnerability-based security technology to stop Internet threats before they impact your business. With IBM Security Network IPS, you gain a highly effective, cost-efficient solution that delivers:

- *Preemptive protection backed by the IBM X-Force research and development team*
- *Leading security technology, including the IBM Protocol Analysis Module (PAM) for deep packet inspection*
- *High performance that helps maintain network availability*
- *Ease of installation, configuration and management*

Preemptive protection that fits your network

With a comprehensive line of high performance models, the IBM Security Network Intrusion Prevention System (IPS) is designed to deliver uncompromising protection for every layer of the network, protecting your business from both internal and external threats.

Technical Specifications

Model	GX4004 -200	GX4004	GX5008	GX5108	GX5208	GX7412 -5	GX7412 -10	GX7412	GX7800
Performance Characteristics*									
Inspected Throughput	Up to 200 Mbps	Up to 800 Mbps	Up to 1.5 Gbps	Up to 2.5 Gbps	Up to 4 Gbps	Up to 5 Gbps	Up to 10 Gbps	Up to 15 Gbps	Up to 20 Gbps+
Average Latency	<200 µs	<200 µs	<200 µs	<200 µs	<200 µs	<100 µs	<100 µs	<100 µs	<100 µs
Connections per second	35,000	35,000	37,000	40,000	50,000	600,000	600,000	600,000	650,000
Concurrent sessions (max rated)	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
Physical characteristics									
Form factor	1U	1U	2U	2U	2U	3U	3U	3U	3U
Height (in/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
Width (in/mm)	16.9/429	16.9/429	16.9/429	16.9/429	16.9/429	Front: 18.85/479 Rear: 17.28/439	Front: 18.85/479 Rear: 17.28/439	Front: 18.85/479 Rear: 17.28/439	Front: 18.85/479 Rear: 17.28/439
Depth (in/mm)	15.5/394	15.5/394	21.5/546	21.5/546	21.5/546	26/662	26/662	26/662	26/662
Weight (lb/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
Management Interface	10/100/ 1000 (IPv6 supported)	10/100/ 1000 (IPv6 supported)	10/100/ 1000 (IPv6 supported)	10/100/ 1000 (IPv6 supported)	10/100/ 1000 (IPv6 supported)	10/100/ 1000 (IPv6 supported)	10/100/ 1000 (IPv6 supported)	10/100/ 1000 (IPv6 supported)	10/100/ 1000 (IPv6 supported)
Inline protected network segments	(2) 1 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
Monitoring Interfaces	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+)
Supported Physical Media Types	RJ-45	RJ-45	RJ-45 or SFP/ mini-GBIC (1000 TX/SX/LX)	RJ-45 or SFP/ mini-GBIC (1000 TX/SX/LX)	RJ-45 or 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)

Technical Specifications

Model	GX4004 -200	GX4004	GX5008	GX5108	GX5208	GX7412 -5	GX7412 -10	GX7412	GX7800
Redundant power supplies	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Redundant storage	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
High availability	Integrated hardware-level bypass	Integrated hardware-level bypass	Active/ active; Active/ passive; Geo-dispersed HA; External hardware-level bypass (optional)	Active/ active; Active/ passive; Geo-dispersed HA; External Hardware-level bypass (optional)	Active/ active; Active/ passive; Geo-dispersed HA; External Hardware-level bypass (optional)	Active/ active; Active/ passive; Geo-dispersed HA; External Hardware-level bypass (optional)	Active/ active; Active/ passive; Geo-dispersed HA; External Hardware-level bypass (optional)	Active/ active; Active/ passive; Geo-dispersed HA; External Hardware-level bypass (optional)	Active/ active; Active/ passive; Geo-dispersed HA; External Hardware-level bypass (optional)

Electrical and Environment Parameters

Voltage and Input Range	100 - 240 V, full range; 50/60 Hz		
Input current rating	5-3 A	8-4 A	10-5 A
Operating temperature:	0° to 40° C (32° to 104° F)		5° to 35° C (41° to 95° F)
Relative humidity:	5% to 85% at 40° C (104° F)		8% to 80% at 28° C (82° F)
Safety certification/ declaration	UL 60950-1, CAN/CSA C22.2 No. 60950-1, EN 60950-1 (CE Mark), IEC 60950-1, GB4943, GOST, UL-AR		
Electromagnetic compatibility (EMC) certification/ declaration	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		
Environmental declaration	ROHS, WEEE and REACH		

*Performance data quoted for the IBM Security Network Intrusion Protection System is based on testing with mixed TCP/UDP traffic that is intended to be reflective of typical live traffic. Environmental factors such as protocol mix and average packet size will vary in each network, and measured performance results will vary accordingly. Network Intrusion Prevention System (NIPS) throughput was determined by pushing mixed protocol traffic through the appliance and measuring how much throughput was achieved with zero packet loss. For the benchmark testing, GX7 series appliances were deployed in default inline protection mode with “Trust X-force” policy; Spirent Avalanche 3100 test gear, firmware 3.50 (or later); Traffic mix: HTTP=41%,HTTPS=17%, SMTP=10%,POP3=5%, FTP=9%, DNS=15%, SNMP=3%; HTTP/HTTPS traffic with 44Kb object size with standard HTTP/S 1.1 GET requests; DNS standard A record lookup; FTP GET requests of 15000 bytes in 2ms bursts, POP3 traffic with 100KB objects between two “user” mailboxes, SMTP simple connections with no object transfer, SNMP status query and response.

For more information

To learn more about IBM Security Network Intrusion Prevention solutions, please contact your IBM Sales representative or IBM Business Partner, or visit the following website:
ibm.com/software/tivoli/products/security-network-intrusion-prevention/

The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

IBM Corporation
Software Group
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
September 2011

WGD03002-USEN-04