IBM Security Network Intrusion Prevention System

Protecting the network Ahead of the threat®

Highlights

- Stop threats before impact without sacrificing high-speed network performance
- Provide a platform for security convergence that helps reduce the cost of deploying and managing point solutions
- Protect networks, servers, desktops and revenue-generating applications from malicious threats

Blocking network threats with security convergence

The IBM Security Network Intrusion Prevention System (IPS) is 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 costs and complexity of deploying and managing point solutions.

When evaluating intrusion prevention technology, businesses often struggle to balance and optimize the following six areas:

- *Performance*
- *Security*
- *Reliability*
- *Deployment*
- *Management*
- *Confidence*

IBM Security Network IPS delivers on all six counts, with performance, preemptive protection, high availability, simple deployment and management, and excellent customer support. Organizations that want to transfer the burden of protecting their network to a trusted security partner can rely on IBM to manage the products for them. IBM customers also benefit from a range of complementary consulting services for assessment, design, deployment, management and education.

Delivering superior performance and protection

Security should enhance network performance, not detract from it. Purpose-built IBM Security Network IPS solutions offer high throughput, low latency and quick uptime to maintain efficient network operations. It includes the following performance features:

- *A full spectrum of high-performance solutions that can scale up to 8 Gbps of protection with an appliance or 40 Gbps with a blade-based system*
- *Intelligent deep-packet inspection using FlowSmart technology*
- *Bounded latency*
- *Traffic flow in the event of system error or loss of power*

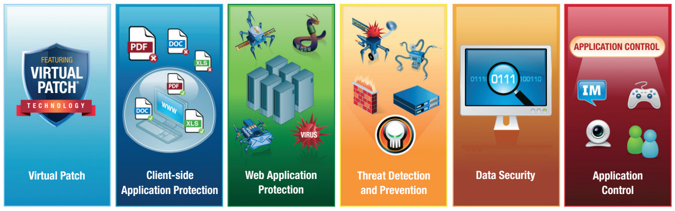
Consolidating network security with preemptive protection

With its modular product architecture, IBM Security Network IPS drives security convergence by adding entirely new modules of protection as threats evolve. From worms to botnets to data security to Web applications, IBM Security Network IPS delivers the protection demanded for business continuity, data security and compliance.

The IBM X-Force® research and development team designed the IBM Protocol Analysis Module and provide the content updates that maintain ahead of the threat protection. X-Force also designed the protection modules, which 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 Modular Technology



The IBM Protocol Analysis Modular Technology (PAM) drives security convergence to deliver network protection that goes beyond traditional IPS to now include 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 power IBM Security Network IPS to protect networks from attack categories and threats, including:

- *Worms*
- *Spyware*
- *Peer to peer (P2P)*
- *Denial of service (DoS) and distributed denial of service (DDoS)*
- *Botnets*
- *Targeted attacks against Web applications*
- *Proprietary or sensitive data leaving the network*
- *Cross-site scripting*
- *SQL injection*
- *Buffer overflow*
- *Web directory traversal*

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

Delivering reliability

Devices placed in the flow of network traffic must be extremely reliable. Our Network IPS offers high availability (active/active or active/passive), hot-swappable redundant power supplies and hot-swappable redundant hard drives to help maintain the flow of network traffic. 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 IPS device.

Providing ease of deployment

IBM Security Network IPS features Layer 2 architecture that does not require network reconfiguration. In addition, network and security administrators can become comfortable and familiar with the device's behavior by choosing one of three operating modes:

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

Also, with our new and improved local management interface, basic policy configuration management now takes 30 percent less time freeing up resources to work on mission critical tasks.

In addition, starting with Firmware 4.1, IBM Security Network IPS provides IPv6 administrative management of the appliance, displays IPv6 events and provides the ability to display the IPv6 source and destination IP addresses.

Centralizing security management

IBM Security Network IPS is centrally managed by the IBM Security Management SiteProtector™ system. SiteProtector provides simple, powerful configuration and control of IBM agents, along with robust reporting, event correlation and comprehensive alerting.

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 for 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-V2-200**	**GX4004-V2**	**GX5008-V2**	**GX5108-V2**	**GX5208-V2**	**GX6116**
Performance Characteristics[1]						
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 8 Gbps
Average Latency	<200 microseconds	<200 microseconds	<200 microseconds	<200 microseconds	<200 microseconds	<150 microseconds
Connections per second	35,000	35,000	37,000	40,000	50,000	296,000
Concurrent sessions (max rated)	1,300,000	1,300,000	1,500,000	1,700,000	2,200,000	5,000,000
IPv6 Management	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
IPv6 Protection & Reporting	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
Physical characteristics						
Form factor	1 rack unit	1 rack unit	2 rack units	2 rack units	2 rack units	2 rack units
Dimensions						
Height (in/mm)	1.75/44	1.75/44	3.5/88	3.5/88	3.5/88	3.5/88
Width (in/mm)	16.9/429	16.9/429	16.9/429	16.9/429	16.9/429	16.9/429
Depth (in/mm)	15.5/394	15.5/394	21.5/546	21.5/546	21.5/546	21.5/546
Weight (lb/kg)	24.5/11.1	24.5/11.1	40.0/18	40.0/18	40.0/18	37.5/17
Management Interface	10/100/1,000 (IPv6 Supported)	10/100/1,000 (IPv6 Supported)	10/100/1,000 (IPv6 Supported)	10/100/1,000 (IPv6 Supported)	10/100/1,000 (IPv6 Supported)	10/100/1,000 (IPv6 Supported)
Monitoring Interfaces	4x10/100/1,000 copper only	4x10/100/1,000 copper only	8x10/100/1,000 copper or 8x SFP/mini-GBIC ports (1,000 TX/SX/LX)	8x10/100/1,000 copper or 8x SFP/mini-GBIC ports (1,000 TX/SX/LX)	8x10/100/1,000 copper or 8x SFP/mini-GBIC ports (1,000 TX/SX/LX)	16x SFP/mini-GBIC ports (1,000 TX/SX/LX)
Inline protected segments	2 network segments	2 network segments	4 network segments	4 network segments	4 network segments	8 network segments
Redundant power supplies	No	No	Yes	Yes	Yes	Yes
Redundant storage	No	No	Yes	Yes	Yes	Yes

Technical Specifications

Model	GX4004-V2-200	GX4004-V2	GX5008-V2	GX5108-V2	GX5208-V2	GX6116
High availability	Active-active: no; Active-passive: no; Hardware-level bypass: integrated bypass	Active-active: no; Active-passive: no; Hardware-level bypass: integrated bypass	Active-active: yes; Active-passive: yes; Geo-dispersed HA: yes; Hardware-level bypass: external bypass (optional)	Active-active: yes; Active-passive: yes; Geo-dispersed HA: yes; Hardware-level bypass: external bypass (optional)	Active-active: yes; Active-passive: yes; Geo-dispersed HA: yes; Hardware-level bypass: external bypass (optional)	Active-active: yes; Active-passive: yes; Geo-dispersed HA: yes; Hardware-level bypass: external bypass (optional)
Electrical and Environment Parameters						
Voltage:	100/240 V ac	100/240 V ac	100/240 V ac	100/240 V ac	100/240 V ac	100/240 V ac
Input range:	100 - 240 V at 50/60 Hz, full range	100 - 240 V at 50/60 Hz, full range	100 - 240 V at 50/60 Hz, full range	100 - 240 V at 50/60 Hz, full range	100 - 240 V at 50/60 Hz, full range	100 - 240 V at 50/60 Hz, full range
KVA:	0.141 KW	0.141 KW	0.389 KW	0.389 KW	0.389 KW	0.377 KW
Heat:	0.481 kBTU/hr	0.481 kBTU/hr	1.328 kBTU/hr	1.328 kBTU/hr	1.328 kBTU/hr	1.287 kBTU/hr
Operating temperature:	0° to 40° C (32° to 104° F)	0° to 40° C (32° to 104° F)	0° to 40° C (32° to 104° F)	0° to 40° C (32° to 104° F)	0° to 40° C (32° to 104° F)	10° to 40° C (50° to 104° F)
Relative humidity:	5% to 85% at 40° C (104° F)	5% to 85% at 40° C (104° F)	5% to 85% at 40° C (104° F)	5% to 85% at 40° C (104° F)	5% to 85% at 40° C (104° F)	20% to 90% at 40° C (104° F)
Safety certification/ declaration	UL 60950-1, CAN/CSA C22.2, No. 60950-1, EN 60950-1, (CE Mark), IEC 60950-1					
Electromagnetic compatibility (EMC) certification/declaration	FCC Part 15, Class A Verification Canada ICES-003, Class A EN 55022, Class A (CE Mark) EN55024 (CE Mark) EN 61000-3-2 (CE Mark) EN 61000-3-3 (CE Mark) VCCI Class A	FCC Part 15, Class A Verification Canada ICES-003, Class A EN 55022, Class A (CE Mark) EN55024 (CE Mark) EN 61000-3-2 (CE Mark) EN 61000-3-3 (CE Mark) VCCI Class A	FCC Part 15, Class A Verification Canada ICES-003, Class A EN 55022, Class A (CE Mark) EN55024 (CE Mark) EN 61000-3-2 (CE Mark) EN 61000-3-3 (CE Mark) VCCI Class A	FCC Part 15, Class A Verification Canada ICES-003, Class A EN 55022, Class A (CE Mark) EN55024 (CE Mark) EN 61000-3-2 (CE Mark) EN 61000-3-3 (CE Mark) VCCI Class A	FCC Part 15, Class A Verification Canada ICES-003, Class A EN 55022, Class A (CE Mark) EN55024 (CE Mark) EN 61000-3-2 (CE Mark) EN 61000-3-3 (CE Mark) VCCI Class A	FCC Part 15, Class A Verification Canada ICES-003, Class A EN 55022, Class A (CE Mark) EN55024 (CE Mark) EN 61000-3-2 (CE Mark) EN 61000-3-3 (CE Mark) VCCI Class A
Environmental declaration	ROHS	ROHS	ROHS	ROHS	ROHS	ROHS

[1] Throughput metrics were attained based on RFC2544 Standards (http://www.ietf.org/rfc/rfc2544.txt) and have been validated by third party testing organizations.

For more information

To learn more about IBM Security Network Intrusion Prevention System, please contact your IBM Sales representative or IBM Business Partner, or visit the following website: **ibm.com**/tivoli/solutions/threat-mitigation

About Tivoli software from IBM

Tivoli® software from IBM helps organizations efficiently and effectively manage IT resources, tasks and processes to meet ever-shifting business requirements and deliver flexible and responsive IT service management, while helping to reduce costs. The Tivoli portfolio spans software for security, compliance, storage, performance, availability, configuration, operations and IT life-cycle management, and is backed by world-class IBM services, support and research.

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

Produced in the United States of America
September 2010
All Rights Reserved

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

The information provided in this document is distributed "as is" without any warranty, either express or implied. IBM expressly disclaims any warranties of merchantability, fitness for a particular purpose or noninfringement. IBM products are warranted according to the terms and conditions of the agreements (e.g. IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided.

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.

♻ Please Recycle