IBM Security Network Protection

Integrated security, visibility, and control for next-generation network protection

Highlights

- Delivers superior zero-day threat protection and security intelligence powered by IBM® X- Force®
- Provides critical insight and visibility into network activity, including encrypted traffic
- Integrates with the IBM QRadar® Security Intelligence Platform
- Enables granular control of both web and non-web applications by users and groups
- Reduces cost and complexity through consolidation and reduces bandwidth consumption

IBM Security Network Protection is designed to protect your business-critical network infrastructure through a unique combination of threat protection, visibility and control. IBM extends the abilities of traditional intrusion prevention systems by offering a next-generation solution that provides network security professionals with complete security, visibility and control over their network. IBM Security Network Protection helps reduce cost and complexity by consolidating point solutions into a single, extensible network security platform. And by controlling and eliminating non-critical, high-bandwidth activity, organizations can achieve additional cost savings within the infrastructure.

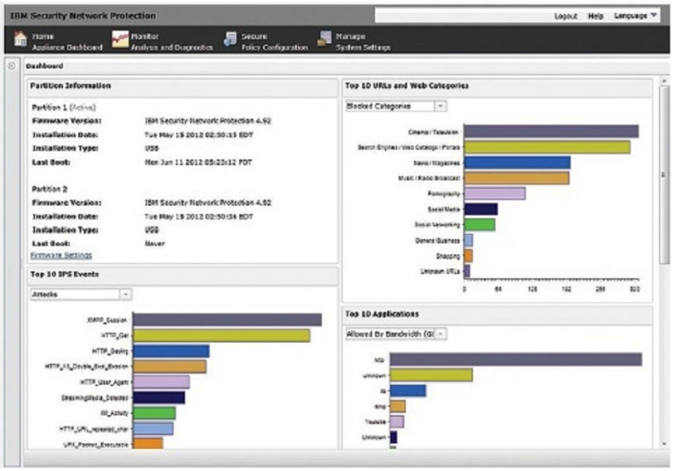
While organizations do require increasingly sophisticated security measures to address today’s security threats, reducing management complexity and containing administration costs are also top priorities. IBM Security Network Protection is an integrated solution that can help you accomplish all of these tasks. By combining several advanced capabilities, this solution can help prevent threats, provide critical insight into network activities and enable granular application control, helping to establish a new level of integrated, simplified security.

Protection against evolving threats

Security threats today are continually evolving. With the rapid growth of cutting-edge web applications and increased file-sharing, activities that may have been considered harmless in the past could become potential openings for attackers. Traditional security means, such as anti-malware software and firewalls, have become easier to bypass. The need for more advanced, proactive threat protection is critical in order to help ensure productivity, data security and compliance. This means providing comprehensive security against new and emerging threats through web application protection, the ability to detect embedded shellcode threats and many other advanced features. The IBM Protocol Analysis Module (PAM) is designed and updated by the X-Force research and development team and is a key element within the IBM Security Network Protection appliance. The X-Force team tracks Internet threat levels from its Global Threat Operations Center to create the world's most comprehensive threat database. PAM then incorporates these continuous content-and-security updates in order to help security professionals stay ahead of emerging threats. The combination of PAM and the X-Force database helps to drive higher protection against zero-day exploits and has the ability to accurately identify a wide range of security risks such as malware, botnets, peer-to-peer activity and many others.

Critical insight and visibility

By combining several key security capabilities, IBM Security Network Protection is able to go beyond basic threat protection and provide critical insight and visibility into network activity, such as which applications are being used, which websites are being visited and who is visiting them. To maintain security, organizations need to know exactly what is going on within their networks including which applications are being used and types of web sites being accessed from the corporate network. These activities can create opportunities for attacks, which can cause data loss, violate corporate policies or introduce compliance issues. IBM Security Network Protection can also provide visibility into bandwidth usage to help identify non-business-critical activities that consume high amounts of bandwidth and resources.



Partition 1 (Active)
Firmware Version: IBM Security Network Protection 4.92
Installation Date: Tue May 15 2012 02:50:15 EDT
Installation Type: USB
Last Boot: Mon Jun 11 2012 05:22:12 PDT

Partition 2
Firmware Version: IBM Security Network Protection 4.92
Installation Date: Tue May 15 2012 02:50:56 EDT
Installation Type: USB
Last Boot: Never

The IBM Security Network Protection dashboard provides an immediate view into the nature of traffic on the network including Web and application use by users and groups.

Granular control over network activity

Building upon high levels of threat-protection and network visibility, IBM Security Network Protection includes granular control functionality, which enables users to act on newly acquired insight into the network. Designed to reduce potential attack vectors and exposure to threats, these capabilities provide granular control over common attack delivery methods such as social media sites to prevent emerging attacks such as spear phishing and other advanced threats targeting users. Having the ability to create granular control policies allows organizations to reduce overall risk, as well as the bandwidth costs related to non-business use of the network. To provide maximum application coverage, IBM Security Network Protection includes support for more than 2,000 applications and individual actions, and leverages a database of more than 20 billion URLs. To ensure the highest levels of accuracy, IBM web-crawling technology continually categorizes and re-categorizes URLs as they change. This ensures IBM Security Network Protection appliances are constantly updated in order to maximize the effectiveness of use policies and protect against the latest Internet threats.

The IBM Security Network Protection XGS 5100 appliance can be configured with up to two network interface modules.

Seamless deployment and integration

IBM Security Network Protection can be seamlessly deployed into a wide variety of environments. This family of products includes flexible features such as interchangeable network interface modules (NIMs) to support a wide variety of networking standards and configurations as they change over time. It also provides flexible performance licensing to allow performance upgrades without hardware changes utilizing a simple license upgrade. Immediate security protection is available out-of-the-box through a pre-configured X-Force default security policy, and appliances can be quickly deployed and centrally managed across a large number of sites using IBM Security SiteProtector™ System. As part of the IBM Threat Protection System, IBM Security Network Protection integrates tightly with the IBM QRadar Security Intelligence Platform. This includes the ability for IBM Security Network Protection appliances to send flow data in the standard Internet Protocol Flow Information Export (IPFIX) data format to provide a constant data feed for more sophisticated analysis and correlation. IBM Security Network Protection appliances can also receive quarantine commands with the ability to block traffic in the event that a security risk is detected by QRadar SIEM. This provides QRadar users with the ability to take immediate action when a security threat is detected.

Why IBM?

Taking a smarter approach to network security, IBM Security Network Protection provides next-generation intrusion prevention system capabilities for advanced protection against evolving security threats. As part of the IBM Threat Protection System, it is a key component in preventing attacks at their onset. It enables administrators to greatly increase security, while having more visibility and control over their networks, resulting in improved bandwidth efficiency and reduced costs. Leveraging the IBM X-Force threat database and a vast URL database, the solution ensures up-to-date, preemptive protection against emerging threats. By integrating several key security features into a single offering, IBM Security Network Protection provides a comprehensive, cost-efficient answer to the challenges faced by organizations today.

IBM Security Network Protection appliances at a glance

	XGS 3100	XGS 4100	XGS 5100	XGS 7100
Performance characteristics*				
Inspected throughput	Up to 800 Mbps	Up to 1.5 Gbps	Up to 7 Gbps	Up to 20 Gbps
Flexible performance levels (FPL)	Up to 400 Mbps (FPL 1) Up to 800 Mbps (FPL 2)	Up to 750 Mbps (FPL 1) Up to 1.5 Gbps (FPL 2)	Up to 2.5 Gbps (FPL 1) Up to 4 Gbps (FPL 2) Up to 5.5 Gbps (FPL 3) Up to 7 Gbps (FPL 4)	Up to 5 Gbps (FPL 1) Up to 10 Gbps (FPL 2) Up to 15 Gbps (FPL 3) Up to 20 Gbps (FPL 4)
Inspected SSL throughput (inbound)	Up to 500 Mbps	Up to 900 Mbps	Up to 4.5 Gbps	Up to 12 Gbps
Inspected SSL throughput (outbound)	Up to 400 Mbps	Up to 700 Mbps	Up to 2.5 Gbps	Up to 7.5 Gbps
Maximum throughput (UDP)	3.5 Gbps	10 Gbps	15 Gbps	45 Gbps
Average latency	<150 µs	<75 µs	<75 µs	<75 µs
Connections per second (HTTP)	10,000	15,000	75,000	225,000
Concurrent sessions (HTTP)	500,000	1,000,000	2,200,000	15,000,000
Physical characteristics				
Form factor	1U	1U	1U	2U
Height	44.2 mm/1.75 in.	44.2 mm/1.75 in.	44.2 mm/1.75 in.	88.4mm/.3.5 in.
Width (rack)	430 mm/16.9 in.	430 mm/16.9 in.	430 mm/16.9 in.	430 mm/16.9 in.
Depth (rack)	540 mm/21.26 in.	540 mm/21.26 in.	540 mm/21.26 in.	570 mm / 22.44 in.
Weight	8.62 kg/19 lb	9.36 kg/20.6 lb	11.58 kg/25.4 lb	18.0kg/29.7 lb
Rack mounting rails	Sliding with square hold post support			
Management interfaces	2 x 1GbE, RJ-45 (IPv6 supported)			
Fixed monitoring interfaces	4 x 1GbE, RJ-45 (integrated bypass)			N/A
Maximum monitoring interfaces (1GbE)	4	Up to 12	Up to 20	Up to 32
Maximum monitoring interfaces (10GbE)	N/A	Up to 2	Up to 4	Up to 8
Supported physical media types	100/1000 RJ-45	100/1000 RJ-45 copper, 1G fiber (SX/LX), 10G fiber (SR/LR), 1G SFP, 10G SFP+	100/1000 RJ-45 copper, 1G fiber (SX/LX), 10G fiber (SR/LR), 1G SFP, 10G SFP+	100/1000 RJ-45 copper, 1G fiber (SX/LX), 10G fiber (SR/LR), 1G SFP, 10G SFP+
Number of supported network interface modules (NIMs)	N/A	1	2	4
Network interface modules (NIMs) with integrated bypass	N/A	8 x 1GbE TX (100/1000) 4 x 1GbE SX 4 x 1GbE LX 2 x 10GbE SR 2 x 10GbE LR	8 x 1GbE TX (100/1000) 4 x 1GbE SX 4 x 1GbE LX 2 x 10GbE SR 2 x 10GbE LR	8 x 1GbE TX (100/1000) 4 x 1GbE SX 4 x 1GbE LX 2 x 10GbE SR 2 x 10GbE LR
Network interface modules (NIMs) with external bypass optional	N/A	4 x 1GbE SFP 2 x 10GbE SFP+	4 x 1GbE SFP 2 x 10GbE SFP+	4 x 1GbE SFP 2 x 10GbE SFP+
Redundant power supplies	Optional	Optional	Included	Included
Storage type	HDD	MLC-SSD	EMLC-SSD	EMLC-SSD
High-availability support	Support for active/active and active/passive environments			
Electrical and environmental parameters				
AC input rating	460 W (100-127 V @ 5.6A/200-240 V @ 2.8A			
Average power consumption	62 W	81 W	194 W	360 W
Operating temperature/relative humidity	0°C – 40°C (32°F – 104°F)/ 5% – 85% @ 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, GB4943, GOST, UL- AR			
Electromagnetic compatibility 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	Restriction of Hazardous Substances (RoHS)			

For more information

To learn more about this offering contact your IBM representative or IBM Business Partner, or visit: ibm.com

*Performance data quoted for IBM Security Network Protection is based on testing with mixed Throughput was determined by sending uncompressed mixed-protocol traffic through the appliance and measuring how much throughput was achieved with zero packet loss. For the benchmark testing, XGS series appliances were deployed with fully populated Network Interface Modules in default inline protection mode with “Trust X-Force” policy , in drop unanalyzed mode; Spirent Avalanche and Spirent TestCenter testing equipment running firmware v4.03 (or later); traffic mix: HTTP=69%, HTTPS=20%, SMTP=5%, FTP=5%, DNS=1%; where HTTP/HTTPS traffic is uncompressed using a 44 Kb object size with standard HTTP/S 1.1 GET requests; SMTP simple connections with no object transfer, FTP GET requests of 15,000 bytes in 2 ms bursts, and DNS standard A record lookup. SSL Inspection rates were measured by enabling SSL Decryption Policy. Maximum Throughput was generated using 1518 byte frame size UDP traffic.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
October 2014

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

♲ Please Recycle