One appliance, six security features designed to preemptively stop Internet threats

IBM Proventia Network Multi-Function Security – MX0804 and MX1004

No one is safe

Single layered security such as a firewall or antivirus protection is no longer enough. Security threats have become more sophisticated in their approaches to attacking businesses. The severity of a security breach can be disastrous, if not fatal to an organization. Mid-market organizations, as well as remote and branch offices, face the same types of Internet threats that larger enterprise-level networks face. The IBM Proventia® Network Multi-Function Security (MFS) MX0804 and MX1004 appliances from IBM Internet Security Systems™ (ISS) provide comprehensive security designed to preemptively stop Internet threats before they penetrate the network and disrupt business operations.

Big security in a small form factor

The complexity of the modern network landscape requires businesses to adopt a multilayered approach to security. Proventia Network MFS incorporates six security technologies onto a single appliance. The Proventia Network MFS product family combines an industry-leading Intrusion Prevention System (IPS) with Stateful firewall, signature and behavioral Antivirus, virtual private network (VPN) capabilities, content filtering and anti-spam. By joining these six security modules, Proventia Network MFS provides all the security content needed to support enterprise-level networks on a single appliance, while retaining an affordable price for mid-market organizations and business locations. Proventia Network MFS MX0804 and MX1004 are ideal for mid-market businesses, branch offices and smaller retail locations. Since these technologies are consolidated onto a single device, organizations benefit from an industrial-strength security technology that does not require a host of in-house security experts to monitor and manage, or possibly jeopardize network performance.

Flexible and scalable

By default, the Proventia Network MFS product family provides comprehensive security the moment the appliance is attached to the network. For organizations with limited information technology (IT) expertise, the default settings on the Proventia Network MFS provide the security coverage needed to secure the network from attack.

Module	Protection Delivered
Intrusion prevention	More than 7,400 vulnerabilities blocked by default using 1,000+ detection algorithms
Antivirus	Sophos provides more than 340,000 virus signatures for known viruses and behavioral detection of unknown viruses
Anti-spam	95 percent+ of spam blocked
Web filtering	More than 9 Billion URLs categorized to the filter list

For businesses with IT expertise, Proventia Network MFS MX0804 and MX1004 can be customized to seamlessly integrate into even the most advanced network environments. Businesses can choose which security modules to utilize, create policies that allow/deny specific Internet traffic, and build groups within the network to establish permission to access certain information.

Proventia Network MFS can also help organizations manage the security posture of multiple locations from a single site. The security architecture can even be standardized through the use of such features as locally resolved variables. For organizations with more than ten locations or those looking for advanced reporting features and management capabilities, Proventia Network MFS, combined with the IBM Proventia Management SiteProtector™ system, can provide a complete set of central management features that help save time and reduce complexity.

Meeting compliance requirements

Business compliance and industry regulations can also add a level of complexity to network security, as well as increase cost and drain IT resources in an often already-strained department. Proventia Network MFS MX0804 and MX1004 are designed to protect organizations against security threats, safeguard critical data and help meet security requirements for regulation such as Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry (PCI) Data Security Standard (the Proventia Network MFS family helps to achieve 10 out of the 12 security standards defined by the PCI Data Security Standard) – without increasing the budget or draining IT resources. In fact, the Proventia Network MFS product family can help reduce IT resource requirements, allowing organizations to focus on revenue-generating activities.

Features and benefits at a glance

- ***Performance-based protection –*** *offers the industry's leading performance-based service level agreements (SLAs) with a cash-back payment when managed by IBM ISS.*
- ***All-in-one protection –*** *helps eliminate the need to acquire, install and manage multiple solutions from different vendors by offering all six security modules for one low price.*
- ***Easy to manage –*** *allows organizations the option to plug and play the device or customize the security features to meet their needs.*
- ***Easy to update –*** *supplies prompt updates via IBM X-Press Update product enhancements, to help protect businesses against the newest security threats by updating without manual intervention or system downtime.*
- ***Virtual patch protection –*** *helps provide pre-emptive protection that is designed to put organizations in control over ad-hoc and emergency patching by shielding vulnerabilities at the network level.*
- ***IBM Internet Security Systems X-Force® research and development team security intelligence –*** *provides easily accessible event details, including full descriptions with recommended actions and responses.*
- ***Intuitive reporting –*** *transforms raw data into informative and intuitive reports to aid decision making.*
- ***Streamlined compliance –*** *helps achieve compliance with security protocols in such industry regulations such as HIPAA, SOX and the PCI Data Security Standard.*

Specifications

	MX0804	MX1004
Hardware specifications		
Form factor	Desktop	Desktop
Interfaces (10/100/1000)	Four 10/100/1000	Four 10/100/1000 Mbps
Weight	1.2 kg (2.6 lbs)	1.2 kg (2.6 lbs)
Dimensions (W x H x D)	250 x 39 x 177 mm 9.8 x 1.5 x 6.9 inches	250 x 39 x 177 mm 9.8 x 1.5 x 6.9 inches
Enclosure	Desktop	Desktop
Serial ports	One	One
UPS support	No	No
AC power	9–264V @ 47–63Hz full range	9–264V @ 47–63Hz full range
Operating	0º–40º Celsius 32º–104º Fahrenheit 5–85 percent @ 40ºC/104ºF	0º–40º Celsius 32º–104º Fahrenheit 5–85 percent @ 40ºC/104ºF
Emissions/Product Safety/Certifications	• U.S.: FCC CFR47 Part 15 Class A • Europe: CISPR 22 Class A; "CE" Mark of Conformity • Japan: VCCI-A • Korea: Korean Requirement Class A • Australia/New Zealand: ACA C-Tick • UL 60950-1 1st Edition Underwriters Laboratory, Safety Information • CAN/CSA 22.2 No. 60950-1 1st Edition • EN60950-1:2001 European Norm • IEC 60950-1 1st Edition, International Electrotechnical Commission, Safety Information • Nordic deviations to IEC 60950-1 1st Edition	• U.S.: FCC CFR47 Part 15 Class B • Europe: CISPR 22 Class B; "CE" Mark of Conformity • Japan: VCCI-B • Korea: Korean Requirement Class B • Australia/New Zealand: ACA C-Tick • UL 60950-1 1st Edition Underwriters Laboratory, Safety Information • CAN/CSA 22.2 No. 60950-1 1st Edition • EN60950-1:2001 European Norm • IEC 60950-1 1st Edition, International Electrotechnical Commission, Safety Information • Nordic deviations to IEC 60950-1 1st Edition
Redundant power supply	No	No
Redundant disk array	No	No
Operating system (OS)	Proprietary	Proprietary
Mean time between failure (MTBF)	30,000 hours (3.4 years)	30,000 hours (3.4 years)
Network features		
Network Address Translation (NAT)	Yes	Yes
Masquerading/port address translation	Yes	Yes
Reverse NAT	Yes	Yes
Traffic-based access control	IP, port, protocol	IP, port, protocol
Dynamic Host Configuration Protocol (DHCP)	Client and server	Client and server
Point-to-Point Protocol over Ethernet (PPPoE)	Yes	Yes
Layer 2 mode	Yes	Yes
Open Shortest Path First (OSPF)	Yes	Yes

	MX0804	MX1004
VPN features**		
Internet Protocol Security (IPSec) with Internet Key Exchange (IKE)	Yes	Yes
Layer Two Tunneling Protocol support (L2TP)	Yes	Yes
Encryption algorithms	DES, 3DES, AES	DES, 3DES, AES
Authentication algorithms	MD5, SHA-1	MD5, SHA-1
Perfect forward secrecy (Diffie-Hellman)	Groups 1,2,5	Groups 1,2,5
IPSec NAT traversal	Yes	Yes
Public Key Infrastructure (PKI) support	Yes	Yes
Interoperability with major VPN vendors (IPSec)	Yes	Yes
Microsoft® Windows® XP client wizard	Included	Included
Web Filtering		
URL blocking	More than 9 Billion URLs categorized	More than 9 Billion URLs categorized
Rate of URL database updates	More than 120,000 updated URLs daily	More than 120,000 updated URLs daily
Number of URL categories	62	62
Image analysis	Yes	Yes
Text analysis	Yes	Yes
User-configurable include/exclude lists	Yes	Yes
Spyware analysis	Yes	Yes
Anti-spam		
Spam-detection rate	More than 95 percent	More than 95 percent
False-positive rate	0.01 percent (1 in 10,000)	0.01 percent (1 in 10,000)
Subject-line tagging	Yes	Yes
Automatic spam deletion	Yes	Yes
Spam sample database	More than 200,000	More than 200,000
Supports mail protocols Simple Mail Transfer Protocol (SMTP) and Post Office Protocol 3 (POP3)	Yes	Yes
Intrusion Prevention System (IPS) / Intrusion Detection System (IDS)		
Number of protocols inspected	More than 170	More than 170
Number of attack detection algorithms	More than 2,500	More than 2,500
Blocking	Yes	Yes
Number of blocked vulnerabilities out-of-box	More than 7400	More than 7400
Drop offending packet	Yes	Yes
Reset connection	Yes	Yes
Block connection	Yes	Yes
Block worm	Yes	Yes
Block Trojan	Yes	Yes

	MX0804	MX1004
Block intruder	Yes	Yes
Neuter attack	Yes	Yes
Block future traffic	Yes	Yes
Performance		
Maximum recommended users***	50	100
Stateful throughput speed (firewall only)	100 Mbps	100 Mbps
Full inspection speed—firewall, IPS and Web filtering	100 Mbps	100 Mbps
Full inspection speed—IPS, Web filtering and antivirus (mail only)	25 Mbps	43 Mbps
Full inspection speed—IPS, Web filtering and antivirus (mail, FTP, Web)	15 Mbps	34 Mbps
Maximum connections per second	2,000	3,000
Maximum concurrent sessions	101,000	101,000
VPN performance		
VPN capacity or maximum recommended tunnels (site-to-site/remote)	100	100
Maximum VPN 3DES encryption speed	15 Mbps	25 Mbps
Maximum VPN AES encryption speed****	30 Mbps	50 Mbps
Maximum VPN 3DES encryption speed with hardware acceleration****	N/A	N/A
Maximum VPN AES encryption speed with hardware acceleration****	N/A	N/A
E-mail (with both antivirus and anti-spam)		
Maximum number of 1KB messages throughput per hour	600	1,320
Maximum number of 1KB messages with 500KB attachments throughput per hour	120	264
Logging / notification		
Event logging	Yes	Yes
E-mail	Yes	Yes
Simple Network Management Protocol (SNMP)	Yes	Yes
High-availability / failure		
Active / passive	Yes	Yes
VPN user authentication		
Internal database	Yes	Yes
RADIUS (external) database	Yes	Yes
LDAP support	Through RADIUS	Through RADIUS
RSA SecureID (external) database	Through RADIUS	Through RADIUS
Xauth over RADIUS for IPSec VPN	Yes	Yes
IP/MAC address binding	Yes	Yes

	MX0804	MX1004
Management		
Centralized management	Yes (with SiteProtector system)	Yes (with SiteProtector system)
Local management	Web-based	Web-based
Multiple administrators and user levels	Yes (with SiteProtector system)	Yes (with SiteProtector system)
External administrator database	Yes (with SiteProtector system)	Yes (with SiteProtector system)
Multilanguage support	No	No
Secure shell (SSH) access	SSH	SSH
Customer support		
Hours available—Standard	24x7x365	24x7x365
Hours available—Premium	24x7x365	24x7x365
Number of support incidents	Unlimited	Unlimited
Number of designated callers	From two to five	From two to five
Additional designated callers	Optional	Optional
Additional languages	Optional	Optional
Customer portal	Yes	Yes
Customer knowledgebase	Yes	Yes
Warranty	One year + contract	One year + contract
Advanced hardware replacement	Yes	Yes
Third Party Certifications	SCP (support center practices) NSS ICSA	SCP (support center practices) NSS ICSA

*** Free VPN client available using Windows XP L2TP VPN client or by purchasing a separate VPN client.*

**** Capacity ratings based on nodes represent general guidelines about the size of the network that should be placed behind a particular Proventia NetworkMulti-Function appliance model.*

*****The Proventia Network MFS MX0804W, MX1004W, MX3006W, MX4006W, MX5008W & MX5110W models only contain the DES Encryption Algorithm to meet Russian Federation encryption requirements.*

About IBM ISS

IBM ISS is the trusted security expert to global enterprises and world governments, providing products and services that protect against Internet threats. An established world leader in security since 1994, IBM ISS delivers proven cost efficiencies and reduces regulatory and business risk across the enterprise. IBM ISS products and services are based on the proactive security intelligence conducted by the X-Force team—a world authority in vulnerability and threat research. For more information about Proventia Network MFS MX0804 or MX1004, please contact your IBM representative or IBM Business Partner. You may also call 1 800 776-2362 or visit **ibm.com**/services/us/iss.

© Copyright IBM Corporation 2008

IBM Global Services

Route 100

Somers, NY 10589

U.S.A.

Produced in the United States of America.

03-08

All Rights Reserved.

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Proventia, SiteProtector and X-Force are trademarks or registered trademarks of Internet Security Systems, Inc., in the United States, other countries, or both. Internet Security Systems, Inc., is a wholly-owned subsidiary of International Business Machines Corporation.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.

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

* Money-back payment (for Managed Protection Ser¬vices - Premium Level only): If IBM Internet Security Systems fails to meet the Security Incidents Prevention Guarantee, client shall be paid US$50,000 for each instance this guarantee has not been met. Please see IBM Internet Security Systems SLAs for more details.

GTD03068-USEN-00