IBM Security Network Intrusion Prevention System Virtual Appliance

Highlights

- Addresses consolidation efforts and costly appliance sprawl with a virtual platform for security convergence
- Extends the same robust intrusion prevention for virtual networks that you expect from traditional networks
- Designed to ease security and compliance efforts by helping to detect and block network attacks and unauthorized network access
- Enables cloud computing service providers to deliver segmented security services in multitenant virtual environments
- Integrates virtualized security with traditional network protection for overall reduced complexity of security operations

Combining security with efficiency for your traditional and virtual environments

Although security has always been a top priority for your organization, the growing complexity and volume of security incidents and compliance regulations has dramatically reinforced the need for sophisticated network protection. Yet economic reality presents an equally compelling need to find ways to reduce hardware requirements through consolidation and virtualization. The challenge is reconciling these priorities without jeopardizing either the security of your organization or your consolidation efforts.

IBM Security Network Intrusion Prevention System Virtual Appliance offers advanced preemptive protection in a virtual security appliance to help you achieve maximum business continuity using minimal resources. Powered by the IBM X-Force® research and development team, IBM Security Network Intrusion Prevention System Virtual Appliance operates on virtual platforms to help protect both your physical and virtual networks with the same high level of security. As a virtual appliance, IBM Security Network Intrusion Prevention System Virtual Appliance provides the ideal solution for managed cloud service providers by enabling flexible deployments in multitenant virtual environments. A single management console and a broad range of consulting services to help simplify the complexity of deploying and managing security operations, while its modular architecture provides extensible protection to help ensure you're ready for the next big threat—whenever and wherever it may occur.

Boosting consolidation efforts through a virtual security appliance

Network security for traditional and virtual platforms often requires appliances that can increase data center requirements, adding to their size and cost. IBM Security Network Intrusion Prevention System

Virtual Appliance offers the best of both worlds: the power and protection of advanced network intrusion prevention in a virtual security appliance. Sophisticated detection technology and virtual form can help keep appliance sprawl to a minimum and your consolidation plans on track, without jeopardizing the security of network operations. High throughput and low latency help maintain traffic flow and ensure efficient network operations.

Extending and simplifying security operations

IBM Security Network Intrusion Prevention System Virtual Appliance extends the same high level of preemptive protection to your virtual operations, helping you block threats to these environments. At the same time, our solution helps ease complexity by enabling you to manage virtual security, traditional enterprise security and vulnerability management from a single management interface. In addition to minimizing the need for multiple point solutions and resources, the ability to share network policies and best practices between your virtual and physical network security operations can help ensure consistency.

Staying ahead of evolving threats and compliance measures

IBM Security Network Intrusion Prevention System Virtual Appliance relies on the IBM Protocol Analysis Module (PAM), which is designed by the IBM X-Force team, to offer a robust extensible protection engine that adds new areas of protection as threats evolve. With the full power of PAM technology, IBM Security Network Intrusion Prevention System Virtual Appliance is a comprehensive network protection solution that includes:

- 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.
- 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.

By consolidating security demands, such as threat detection and prevention, data security, Web application protection and application control, IBM Security Network Intrusion Prevention System Virtual Appliance helps reduce the cost of deploying and maintaining point solutions. This modular technology can help safeguard your networks from attack categories and threats, including:

- Worms and spyware
- Denial-of-service (DoS) and distributed denial-of-service (DDoS)
- Botnets
- Targeted attacks against Web applications
- Proprietary or sensitive data leaving the network

Enabling security services in cloud computing

IBM Security Network Intrusion Prevention System Virtual Appliance provides the virtual appliance that enables managed cloud service providers to protect specific virtual network segments with the option of customized security policies or “trust X-Force” default configurations. With the ability to deliver new revenue-generating services powered by the security of X-Force, cloud service providers can gain a significant competitive differentiator while delivering the reliability their clients demand.

Requirements and technical specifications

	GV1000	**GV200**		
Processor	2x Quad Core Intel® Xeon® E5440 @ 2.83 GHz			
Operating system	VMware ESX Infrastructure 3 Version 3.5	VMware ESX Infrastructure 3 Version 3.5, VMware ESXi 3.5. VMware Server 2.0		
VM guest operating system support	N/A	N/A		
Memory	1 GB RAM	1 GB RAM		
Network connection	Any VMware supported NIC	Any VMware supported NIC		
Disk space	10 GB hard drive	10 GB hard drive		
Performance characteristics*		**ESX 3.5**	**ESXi 3.5**	**VMware Server 2.0**
Throughput	Up to 700 Mbps	Up to 200 Mbps	Up to 150 Mbps	Up to 50 Mbps
Connections per second	19,000	19,000	19,000	12,000
Concurrent sessions (max rate)	500,000	500,000	500,000	400,000
Operating modes	**GV 1000**	**GV 200**		
Active protection	Yes	Yes		
Passive detection	Yes	Yes		
Inline simulation	Yes	Yes		pres
Protected network segments	1	1		
*Performance achieved with the following configuration	IBM BladeCenter® HT Chassis, Blade IBM eServer™ HS21 - 8853AC1, NICs NetXtreme Broadcom5704S, Processor 2x Quad Core Intel Xeon E5440 @ 2.83 GHz, OS Version ESX 3.5.0 Build 123630 Update 3	IBM BladeCenter HT Chassis, Blade IBM eServer HS21 - 8853AC1, NICs NetXtreme Broadcom5704S, Processor 2x Quad Core Intel Xeon E5440 @ 2.83 GHz		

Offering simplified implementation and maintenance

Designed for easy installation, configuration and management, IBM Security Network Intrusion Prevention System Virtual Appliance can help you juggle the conflicting priorities of staffing requirements and network security. As a virtual appliance and self-contained solution, the solution can deliver security without altering server images, virtual servers, applications or the virtual infrastructure. You can select from several operating modes, including:

- Active – intrusion prevention for blocking
- Inline simulation – displays what would be blocked
- Passive – intrusion detection for alerting without blocking

If you prefer to transfer the burden of protecting your network to a trusted security partner, IBM offers established consulting and managed services through skilled service solution teams for assessment, design, deployment and management.

Why IBM?

IBM Security Network Intrusion Prevention System Virtual Appliance brings world-class vulnerability-based security technology in a virtual form to help protect your virtual and physical network environments and support your consolidation goals. In addition to offering preemptive protection across every layer of your network and simple deployment and integrated management, this comprehensive security platform is backed by the industry-leading IBM X-Force research and development team.

For more information

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

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

Produced in the United States of America
May 2010

SED03058-USEN-02