产品简介

Tivoli software

IBM Security Network Intrusion Prevention System

全面防御如今不断演化的威胁

要 点

- 无与伦比的性能水平，不会影响安全保护的广度和深度
- 保护网络、服务器、桌面和应用等关键业务资产免遭恶意威胁攻击
- 保护Web应用免遭SQL注入和跨站点脚本攻击等威胁攻击
- 使用整合的Data Loss Prevention (DLP)监控整个网络的数据安全风险
- 预防即时消息和对等文件共享中的网络滥用和数据丢失
- 在全球知名的IBM X-Force®研究团队的强大支持基础上不断改进，以“先发制人”地防御威胁
- 通过合并单点解决方案和整合其他安全工具，降低成本和复杂性

IBM Security Network Intrusion Prevention System (IPS)解决方案设计用于在威胁对业务造成影响之前阻止Internet威胁。抢先保护(在威胁发生之前采取的保护)是通过将IBM专有的线速性能、安全智能和模块化保护引擎相结合实现的。通过整合对数据安全和Web应用保护的网络安全需求，IBM Security Network IPS是一个能够降低部署和管理单点解决方案的成本和复杂性的安全平台。

当评估入侵检测技术时，企业常常很难平衡和优化以下6个关键区域：性能、安全、可靠性、部署、管理和保密性。

IBM Security Network IPS通过行业领先的性能、由X-Force研究团队强力支持的抢先威胁保护、高可用性水平、简化的部署和管理，以及一流IBM客户支持所带来的信心，解决了所有这6方面的问题。那些希望将保护网络的任务交给一个值得信赖的安全合作伙伴的组织，可依靠IBM来为他们管理安全基础架构。IBM客户还可享受评估、设计、部署、管理和培训方面的多种补充性咨询服务。

不折不扣地交付卓越的性能

安全应该增强网络性能，而不会降低它。专用的IBM Security Network IPS解决方案提供了高吞吐量、低延迟和最高的可用性来维持有效的网络操作。这包含能够利用全面的安全保护，消除在最高水平的安全性和维持关键业务应用的服务水平所需的性能之间选择的需要。通过提供超过20 Gbps所检测到的吞吐量的行业领先的性能，IBM Security Network IPS解决方案提供了您需要的性能，同时还提供了高安全水平。

将网络安全与抢先保护整合

借助其模块化的产品架构，IBM Security Network IPS解决方案通过随威胁演化而添加全新的保护模块，促进的安全融合。这解决了从蠕虫和僵尸网络到Web应用和数据安全问题的各种安全威胁，使IBM Security Network IPS解决方案能够提供业务连续性、数据安全和合规性所需的保护。

IBM X-Force研发团队设计了IBM Protocol Analysis Module (PAM)，在威胁之前抢先提供内容更新。具体的保护模块包括：

- IBM Virtual Patch®技术——防御漏洞攻击，与软件补丁独立。
- 客户端应用保护——保护最终用户免受针对日常应用(比如Microsoft® Office文件、Adobe® PDF文件、多媒体文件和Web浏览器)的攻击。
- 高级网络保护——包含DNS保护的高级入侵防御。
- 数据安全——监控和识别未加密的个人可识别信息(PII)和其他机密数据。

IBM协议分析模块技术

IBM Protocol Analysis Module (PAM)促进了安全融合，提供了超越传统的IPS的网络保护，包括客户端应用保护、数据安全、Web应用保护和应用控制。

- Web应用安全——保护Web应用、Web 2.0和数据库(与Web应用防火墙保护相同)。
- 应用控制——回收带宽，阻止Skype、对等网络和隧道。

这些模块使IBM Security Network IPS解决方案能够保护组织免遭各种威胁攻击，包括：

- 蠕虫和间谍软件等恶意软件
- 由僵尸网络启动的攻击
- 即时消息和对等相关攻击，比如网络滥用和数据丢失
- 拒绝服务(DoS)和分布式拒绝服务(DDoS)攻击
- 针对Web应用的有针对性的攻击，比如跨站点脚本和SQL注入
- 与专用或敏感数据相关的数据丢失
- 缓冲区溢出攻击
- 客户端攻击，比如针对Web浏览器的攻击

X-Force研发团队从其Global Threat Operations Center跟踪Internet威胁水平，以加强和更新IBM Security Network IPS解决方案中的保护。

提供高水平的可用性

网络流量流经的设备必须非常可靠。IBM Security Network IPS解决方案提供了最高水平的可靠性和可用性。这是通过高可用性配置(主动/主动或主动/被动)、可热交换冗余电源和可热交换冗余硬盘驱动器来实现的。此外，我们高度可用的地理位置选项可使用管理端口来共享隔离决策，确保在需要时安全地将故障转移到异地的备用设备上。

提供轻松的部署

每个IBM Security Network IPS设备都预先配置了成熟的X-Force默认安全策略。这开箱即用地提供了直接安全保护，并经过X-Force研究人员的验证，可以确保最高水平的准确性。IBM Security Network IPS还包含不需要网络重新配置的双层架构。网络和安全管理员可轻松选择3种操作模式中的一种，包括:

- 主动保护(入侵防御模式)
- 被动保护(入侵检测模式)
- 内部模拟(模拟内部防御)

集中的安全管理

IBM Security Network IPS设备可由IBM Security SiteProtector系统集中管理。SiteProtector提供了简单、强大的IBM代理配置和控制，以及强健的报告、事件关联和完善的提醒。还包含对IBM Security Network IPS设备的IPv6管理支持，包括显示IPv6事件和IPv6来源/目标IP地址的能力。

通过专家经验和支持增强您的信心

IBM是入侵检测和防御领域的领导者，保持着卓越的客户支持记录。IBM是安全行业中首批获得Global Support Center Practices (SCP)认证的企业之一，是Service & Support Professionals Association (SSPA) Advisory Board的成员。

为何选择IBM?

IBM理解您的网络的威胁，以及性能与保护之间的重要平衡。因此，IBM基于漏洞的一流安全技术能够在Internet威胁影响您的业务之前阻止它们。使用IBM Security Network IPS，您可以获得提供了以下功能的高度有效、经济实惠的解决方案:

- 由IBM X-Force研发团队强力支持的抢先保护
- 领先的安全技术，包括用于深度包检查的IBM Protocol Analysis Module (PAM)
- 帮助维持网络可用性的高性能
- 轻松安装、配置和管理

适合您的网络的抢先保护

使用完善的高性能模块，IBM Security Network Intrusion Prevention System (IPS)旨在不妥协地提供对网络的每一层的保护，保护您的业务免遭内部和外部威胁攻击。

产品简介

技术规范							
型号	GX4004-V2-200	GX4004-V2	GX5008-V2	GX5108-V2	GX5208-V2	GX6116	GX7800
性能特征*							
检测到的吞吐量	最高 200 Mbps	最高 800 Mbps	最高 1.5 Gbps	最高 2.5 Gbps	最高 4 Gbps	最高 8 Gbps	23 Gbps
平均延迟	<200 µs	<200 µs	<200 µs	<200 µs	<200 µs	<150 µs	<150 µs
每秒连接数	35,000	35,000	37,000	40,000	50,000	296,000	390,000
并发会话(最大值)	1,300,000	1,300,000	1,500,000	1,700,000	2,200,000	5,000,000	12,500,000
物理特征							
规格	1U	1U	2U	2U	2U	2U	3U
尺寸							
高(英寸/毫米)	1.75/44	1.75/44	3.5/88	3.5/88	3.5/88	3.5/88	5.25/133
宽(英寸/毫米)	16.9/429	16.9/429	16.9/429	16.9/429	16.9/429	16.9/429	前面: 18.85/479 后面: 17.28/439
深(英寸/毫米)	15.5/394	15.5/394	21.5/546	21.5/546	21.5/546	21.5/546	26/662
重(磅/千克)	24.5/11.1	24.5/11.1	40.0/18	40.0/18	40.0/18	37.5/17	55/25
管理接口	10/100/1000 (支持IPv6)	10/100/1000 (支持IPv6)	10/100/1000 (支持IPv6)	10/100/1000 (支持IPv6)	10/100/1000 (支持IPv6)	10/100/1000 (支持IPv6)	10/100/1000/10000 (支持IPv6)
监控接口	4x10/100/1,000 (仅限铜线)	4x10/100/1,000 (仅限铜线)	8x10/100/1,000根铜线或8x SFP/微型GBIC端口(1,000 TX/SX/LX)	8x10/100/1,000根铜线或8x SFP/微型GBIC端口(1,000 TX/SX/LX)	8x10/100/1,000根铜线或8x SFP/微型GBIC端口(1,000 TX/SX/LX)	16xSFP/微型GBIC端口(1,000 TX/SX/LX)	8x10GbeSFP+ (SR/LR)/8x10Gbe直接附加铜线/8x1G SFP (TX/SX/LX)
内联保护网段	2个网段	2个网段	4个网段	4个网段	4个网段	8个网段	4个网段
冗余电源	否	否	是	是	是	是	是
冗余存储	否	否	是	是	是	是	是
高可用性	主动-主动: 否; 主动-被动: 否; 硬件级旁路: 整合的旁路	主动-主动: 否; 主动-被动: 否; 硬件级旁路: 整合的旁路	主动-主动: 否; 主动-被动: 否; 地理上分散的高可用性: 是; 硬件级旁路: 外部旁路(可选)	主动-主动: 否; 主动-被动: 否; 地理上分散的高可用性: 是; 硬件级旁路: 外部旁路(可选)	主动-主动: 否; 主动-被动: 否; 地理上分散的高可用性: 是; 硬件级旁路: 外部旁路(可选)	主动-主动: 否; 主动-被动: 否; 地理上分散的高可用性: 是; 硬件级旁路: 外部旁路(可选)	主动-主动: 否; 主动-被动: 否; 地理上分散的高可用性: 否; 硬件级旁路: 外部旁路(可选)

技术规范							
型号	GX4004-V2-200	GX4004-V2	GX5008-V2	GX5108-V2	GX5208-V2	GX6116	GX7800
电力和环境参数							
电压:	100/240 V ac	100/240 V ac	100/240 V ac	100/240 V ac	100/240 V ac	100/240 V ac	100/240 V ac
输入范围:	100 - 240 V, 50/60 Hz, 全范围	100 - 240 V, 50/60 Hz, 全范围	100 - 240 V, 50/60 Hz, 全范围	100 - 240 V, 50/60 Hz, 全范围	100 - 240 V, 50/60 Hz, 全范围	100 - 240 V, 50/60 Hz, 全范围	100 - 240 V, 50/60 Hz, 全范围
操作温度:	0˚到40˚C (32˚到104˚F)	0˚到40˚C (32˚到104˚F)	0˚到40˚C (32˚到104˚F)	0˚到40˚C (32˚到104˚F)	0˚到40˚C (32˚到104˚F)	10˚到40˚C (50˚到104˚F)	5˚到35˚C (41˚到95˚F)
相对湿度:	5%到85%, 40˚C (104˚F)	5%到85%, 40˚C (104˚F)	5%到85%, 40˚C (104˚F)	5%到85%, 40˚C (104˚F)	5%到85%, 40˚C (104˚F)	20%到90%, 40˚C (104˚F)	8%到80%, 28˚C (82˚F)
安全认证/声明	UL 60950-1, CAN/CSA C22.2, 编号 60950-1, EN 60950-1, (CE Mark), IEC 60950-1	UL 60950-1, CAN/CSA C22.2, 编号 60950-1, EN 60950-1, (CE Mark), IEC 60950-1	UL 60950-1, CAN/CSA C22.2, 编号 60950-1, EN 60950-1, (CE Mark), IEC 60950-1	UL 60950-1, CAN/CSA C22.2, 编号 60950-1, EN 60950-1, (CE Mark), IEC 60950-1	UL 60950-1, CAN/CSA C22.2, 编号 60950-1, EN 60950-1, (CE Mark), IEC 60950-1	UL 60950-1, CAN/CSA C22.2, 编号 60950-1, EN 60950-1, (CE Mark), IEC 60950-1	UL 60950-1, CSA 60950-1, EN 60950-1 (CE Mark), IEC 60950-1, GB4943, GOST, UL-AR
电磁兼容性 (EMC) 认证/声明	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	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
环境声明	ROHS	ROHS	ROHS	ROHS	ROHS	ROHS	ROHS , WEEE 和REACH

*援引的IBM Security Network Intrusion Protection System性能数据基于旨在反映典型的实时流量的混合TCP/UDP流量测试。协议组合和平均包大小等环境因素将因每个网络不同而异，度量的性能结果也将相应地变化。Network Intrusion Prevention System (NIPS)吞吐量的确定方式是，推送经过设备的混合协议流量并度量以零包流失实现了多少吞吐量。对于基准测试，GX7800在默认的内联保护模式下使用"信任X-force"策略来部署；Spirent Avalanche 3100测试工具、固件3.50 (或更新版本)；流量混合：HTTP=41%、TTPS=17%、SMTP=10%、POP3=5%、FTP=9%、DNS=15%、SNMP=3%；使用标准HTTP/S 1.1 GET请求的44Kb对象大小的HTTP/HTTPS流量；DNS标准A记录查找；在2ms内爆发的15000字节的FTP GET请求；两个"用户"邮箱之间包含100KB对象的POP3流量；没有对象传输、SNMP状态查询和响应的SMTP简单连接。

更多信息

有关IBM Security Network Intrusion Protection System的更多信息，请联系您的IBM销售代表或IBM业务合作伙伴，或访问以下网站：**ibm.com**/software/tivoli/products/security-network-intrusion-prevention/

客户应自行确保遵守法律规定要求。请有能力的法律顾问提供有关任何相关法律的鉴定和解释的建议是客户自己的责任，它们可能会影响客户的业务以及客户为遵守这些法律可能需要采取的任何行动。

IBM不提供法律建议，也不表示或保证其服务或产品将确保客户遵守任何法律。

© 版权所有IBM Corporation 2011

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

在中国印刷
2011年6月

保留所有权利

IBM和IBM徽标是国际商业机器公司在美国和/或其他国家/地区的商标。

如果这些和其他IBM商标在本文档中初次出现时带有商标符号(®或™)，则表示在此信息发布时，这些商标是IBM拥有的、在美国注册的商标或普通法规定的商标。此类商标在其他国家(地区)也可能是注册商标或普通法规定的商标。关于IBM商标的最新列表，请访问**ibm.com**/legal/copytrade.shtml的 "Copyright and trademark information" 部分。

Adobe、Adobe徽标、PostScript和PostScript徽标是Adobe Systems Incorporated在美国和/或其他国家的商标或注册商标。

Microsoft、Windows、Windows NT和Windows徽标是Microsoft公司在美国和/或其他国家的商标。

其他公司、产品或服务名称可能是其他公司的商标或服务标记。

本出版物中对IBM产品或服务的引用，不代表它们可用于所有IBM运营的国家。

到发布之日止，产品数据都进行了准确性审校。产品数据可能随时更改，恕不通知。关于IBM未来方向或打算的声明仅代表IBM的发展目标，如有变更，恕不另行通知。

本文档中的信息按 "原样" 提供，不承担任何隐含或明确的担保。

IBM明确声明不提供任何关于适销性、符合特定用途或非侵权的担保。IBM产品的担保依据是其遵循的协议(比如IBM Customer Agreement、Statement of Limited Warranty、International Program License Agreement等)中的条款和条件。

请回收利用

Tivoli software

WGD03002-USEN-03