PROTECT FROM VIRUSES AND SPYWARE WITH SSG SERIES SECURE SERVICES GATEWAYS

Delivering Extremely Quick Response Times to Emerging Threats with Best-in-Class Detection Rates and Performance

Challenge

With the costs and complexity of modern malware threats on the rise, many companies face the challenge of how to choose an antimalware solution that will guarantee maximum protection and will not impede network performance.

Solution

By integrating a best-in-class gateway antivirus offering from Kaspersky Lab, Juniper Networks integrated security appliances can protect Web traffic, email and Web mail from file-based viruses, worms, backdoors, trojans and other types of malware.

Benefits

- Detection of all malware and other potentially harmful programs with practically zero false alarms
- Wire speed threat protection with minimal impact on network performance
- Comprehensive virus, worm, and spyware protection

Today's Internet threats have become more complex and costly than ever before. Much of the current malware (short for malicious software)—which includes trojans, backdoors and spammers' proxy servers as well as viruses and worms—is purpose-built to hijack users' machines. In fact, a single trojan can easily be found on many thousands of infected PCs. Apart from financial losses, malware can result in internal security threats, productivity losses, leakage of confidential information and damaged corporate reputation.

Accordingly, gateway antivirus protection has become a necessary first layer of defense in corporate network security today (together with second layer server and third layer desktop protection). This is due to a number of reasons:

- It considerably enhances overall security—most of the dangerous fast-spreading threats are stopped before they enter the network.
- It lifts the load from desktop machines—resource-intensive tasks are not executed on the employee's PCs.
- It improves network performance and scalability—antivirus filtering can be done at the gateway on a few boxes simultaneously.
- It's more optimal as malicious email sent to multiple recipients needs to be scanned and blocked only once.
- It's easier to enforce timely updates and proper configuration at the gateway compared to remote laptops.

The Challenge

Now more than ever, as the costs and complexity of malware threats continue to grow, many companies are struggling to find a best-of breed gateway antimalware solution that will guarantee maximum protection and not impede network performance.

With malware that can reach epidemic proportions in hours or, in the worse cases, in minutes, antivirus vendors must provide a fix within the same timeframe. A gateway antivirus solution that is built for speed is essential. It must also guarantee the highest detection rates of all existing and newly emerging malware threats. On the other hand, it must not be too aggressive in detecting new malware threats: high proactive detection levels are only useful if they don't come with a high false positive rate.

If an antivirus program reports an infection in a clean file, this is called a false alarm, or false-positive, and could be as harmful as viruses. Not only do frequent false alarms undermine a user's confidence in a program's heuristic analyzer, they can also prevent a user from recognizing a new virus (the program wrongly detects legitimate programs so often that the user stops trusting it).

The Juniper Networks SSG Series Secure Services Gateways

By integrating an antivirus offering from Kaspersky Lab, Juniper Networks® integrated security appliances can protect Web traffic, email and Web mail from file-based viruses, worms, backdoors, trojans and other types of malware. Using policy-based management, inbound and outbound traffic can be scanned, thereby protecting the network from attacks originating from outside the network, as well as those that originate from inside the network. Unlike other integrated antivirus solutions that are packet- or network signature-based, the Juniper-Kaspersky solution deconstructs the payload and files of all types, evaluating them for potential viruses and then sending the original data on its way.

The vast majority of malware is trying to sneak into organizations inside packers, archieves and compressed files. Kaspersky technology is known to support the largest number of formats. This approach boosts overall company security as the gateway solution stops malware threats even if they come in a packed format, which is quite common for e-mail attachments.

The Juniper-Kaspersky solution detects and protects against all viruses, worms, malicious backdoors, dialers, keyboard loggers, password stealers, trojans and other malicious code. Included in the joint solution is detection of spyware, adware and other malware-related programs. The optimal combination of signature and proactive technologies, as well as thorough testing of all updates, guarantees an almost 100 percent detection rate with practically zero false positive alarms (according to AV-Comparatives and other authoritative tests).

Unlike some solutions that will use multiple non-file based scanners to detect different types of malware, the Juniper-Kaspersky solution is based upon one unified comprehensive scanner, database, and update routine that protects against all malicious and malware-related programs.

Features and Benefits

Features:

- An effective combination of signature and proactive technologies proved in respected industry tests (AV-Comparatives, AV-Test)
- The largest number of file formats supported (over 3,300 versions and variations as of December 2007)
- Hourly regular updates
- Quickly updates urgent, new threats
- Optimal filtering functionality and performance customized for company network topology

Benefits:

- Best-in-class detection of all malware and potentially harmful programs with practically zero false alarms
- Wire speed threat protection with minimal impact on network performance
- Comprehensive virus, worm, and spyware protection
- Early detection and defense against malware
- Minimize network disruptions caused from virus and worm outbreaks
- Proactive threat prevention ensures complete, up-to-date protection from the latest security threats

Solution Components

The Juniper Networks family of purpose-built security solutions are designed to satisfy customer networking and security requirements that range from small branch office and telecommuter locations to high speed carrier and data center environments. The solutions consist of the following components:

- Purpose-built security appliance delivers a perfect mix of high performance, security and LAN/WAN connectivity
- Dedicated, security-specific processing hardware and a complete set of Unified Threat Management (UTM) security features including stateful firewall, IPsec VPN, intrusion prevention system (IPS), antivirus (includes antispyware, anti-adware, antiphishing), antispam, and Web filtering
- Tightly integrated set of best-in-class UTM security solutions to protect against worms, trojans, viruses, spyware, and other malware
- Multiple management mechanisms, including complete command-line interface (CLI), WebUI or centralized management via Juniper Networks Network and Security Manager, facilitate rapid deployment while minimizing ongoing operational costs

Table 1: Antivirus Specifications

ANTIVIRUS SPECIFICATIONS (KASPERSKY LAB)	
Protocols scanned	SMTP, POP3, Webmail, FTP, IMAP, HTTP
Inbound/outbound protection	Yes/Yes
New virus responsiveness	Average 30 minutes
Update frequency	Hourly
Number of virus signatures	480,000 +
Archive and extractor formats	ACE, ARJ, Alloy, Astrum, BZIP2, BestCrypt, CAB, CABSFX, CHM, Catapult, CaveSFX, CaveSetup, ClickTeam, ClickTeamPro, Commodore, CompiledHLP, CreateInstall, DiskDupe, DiskImage, EGDial, Effect Office, Embedded, Embedded Class, Embedded EXE, Embedded MS Expand, Embedded PowerPoint, Embedded RTF, FlyStudio, GEA, GKWare Setup, GZIP, Gentee, Glue, HA, HXS, HotSoup, Inno, InstFact, Instyler, IntroAdder, LHA, MS Expand, MSO, Momma, MultiBinder, NSIS, NeoBook, OLE files, PCAcme, PCCrypt, PCInstall, PIMP, PLCreator, PaquetBuilder, Perl2Exe, PerlApp, Presto, ProCarry, RARv 1.4 and above, SEA, SbookBuilder, SetupFactory, SetupSpecialist, SilverKey, SmartGlue, StarDust Installer, Stream 1C, StubbieMan, Sydex, TSE, Tar, Thinstall, ViseMan, WinBackup, WiseSFX, ZIP, 7-Zip
WIN semi-executable extensions	pif, lnk, reg, ini (Script.Ini, etc), cla (Java Class), vbs (Visual Basic Script), vbe (Visual Basic Script Encrypted), js (Java Script), jse (Java Script Encrypted), htm, html, htt (HTTP pages), hta - HTA (HTML applications), asp (Active Server Pages), chm – CHM (compressed HTML), pht – PHTML, php – PHP, wsh, wsf, the (.theme)
MS Office extensions	doc, dot, fpm, rtf, xl*, pp*, md*, shs, dwg (Acad2000), msi (MS Installer), otm (Outlook macro), pdf (AcrobatReader), swf (ShockwaveFlash), prj (MapInfo project), jpg, jpeg, emf (Enhanced Windows Metafile), elf
DOS executable extensions	com, exe, sys, prg, bin, bat, cmd, dpl(Borland's Delphi files), ov*
WIN executable extensions	dll, scr, cpl, ocx, tsp, drv, vxd, fon 386
Email file extensions	Eml, nws, msg, plg, mbx (Eudora database)
Help file extensions	hlp
Other file extensions	sh, pl, xml, itsf, reg, wsf, mime, rar, pk, lha, arj, ace, wmf, wma, wmv, ico, efi

Summary

Juniper Networks SSG Series Secure Services Gateways are pre-integrated with the Kaspersky® antivirus engine, now in its fifth generation, which is purpose-built to protect enterprises from the threats of today and tomorrow. It provides a combination of best-in-class response times, industry-leading detection of all kinds of malicious content and superior performance.

Next Steps

To learn more about Juniper's best-in-class line of UTM appliances featuring Kaspersky antivirus technology, please visit **www.juniper.net/security**.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at **www.juniper.net**.

About Kaspersky Lab

Kaspersky Lab delivers the world's most immediate protection against IT security threats, including viruses, spyware, crimeware, hackers, phishing, and spam. Kaspersky Lab products provide superior detection rates and the industry's fastest outbreak response time for home users, SMBs, large enterprises and the mobile computing environment. Kaspersky® technology is also used worldwide inside the products and services of the industry's leading IT security solution providers. Learn more at **www.kaspersky.com**. For the latest on antivirus, antispyware, antispam and other IT security issues and trends, visit **www.viruslist.com**.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

3510280-002-EN April 2010

Printed on recycled paper