STOPPING INBOUND AND OUTBOUND THREATS

JUNIPER NETWORKS SECURE ROUTER and FIREWALL/IPSEC VPN WITH UNIFIED THREAT MANAGEMENT (UTM)

Challenge

As the network attack landscape continues to evolve, IT managers can no longer afford to focus solely on protection against a single type of attack and expect their network to remain unaffected.

Solution

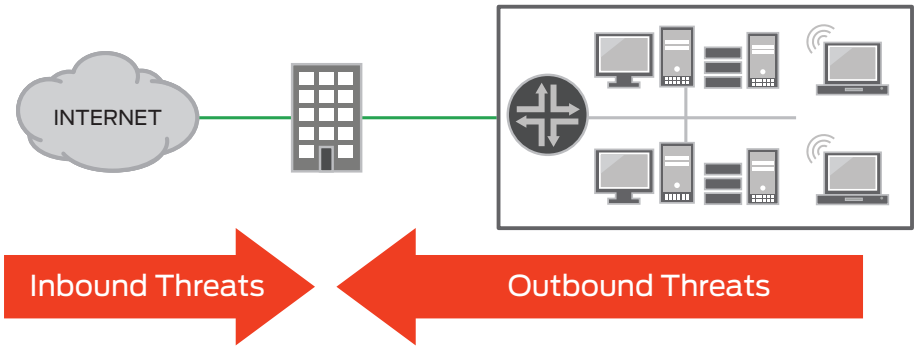
Stopping all manner of inbound and outbound attacks, requires a concerted, multi-layered solution to eliminate damage to the network, company assets and the end user.

Benefits

To provide protection against inbound and outbound attacks at all levels, Juniper Networks integrates a complete set of best-in-class Unified Threat Management (UTM) features into their line of branch and regional office secure router and firewall/VPN platforms. By leveraging the development, support and market expertise of many of the leading content security partners, Juniper is able to deliver a set of best-in-class UTM features.

As the network attack landscape continues to evolve, IT managers can no longer afford to focus solely on protection against a single type of attack and expect their network to remain unaffected. All types of attacks are squarely targeted at the corporate network. Relatively simple network level attacks have morphed into more complex attacks that use both network and application-level components to achieve their malicious goals. With more and more companies providing direct access to the web, end-users are casually surfing sites that may be known malware download sources, and/or unknowingly revealing personal or corporate private data (credit cards, passwords, corporate trade secrets, etc) via email scams or hidden background programs that collect and forward data. This means that an IT manager must not only stop attacks at each layer of the network, for each application and for all types of content, but they also need to stop both inbound and outbound threats.

- Inbound threats are those that originate from outside the corporate network, for example, from an attacker on the Internet who intends to penetrate the corporation's perimeter defenses. These threats include virtually all types of attacks from worms to viruses to spyware to phishing emails.
- Outbound threats are those that originate from someone inside, such as an employee of the company who has a machine that has been unknowingly compromised and is propagating a worm or virus throughout the corporate network. Other examples of outbound attacks are users who respond to phishing attacks by entering their personal data on a malicious web site, and spyware which is resident on an employee's machine that quietly sends sensitive corporate information to a malicious party on the Internet.



- Windows, macro & script viruses, back doors
- Spyware, adware, keyloggers
- Spam, phishing
- Worms, trojans, DDoS, SoS, port and reconnaissance scans

- Spyware, adware, malware, downloads
- Virus and file-based trojan propagation
- Response to phishing attacks
- Worm and trojan propagation

Stopping all inbound and outbound attacks requires a concerted, multi-layered solution to prevent damage to the network, company assets and end users.

The Right Tool for the Job

While bi-directional protection is a critical component, it is equally critical to implement solution components that target specific types of attacks. No single solution component will stop the long list of network-level, application-level and content-based attacks. For example, viruses are embedded within files, such as an attachment or an executable. To ensure maximum protection against viruses, IT managers should implement a true, file-based antivirus offering that deconstructs the payload, decodes the file or script, evaluates it for potential viruses and then reconstructs it, sending it on its way. Network signature antivirus solutions look only at a limited amount of data, such as packets or stream, for virus detection, resulting in a false sense of security. Antivirus offerings that are solely looking at network streams will not provide adequate protection because they do not have the ability to decode the plethora of files and file formats that range from Word documents to Excel spreadsheets to GIF images to zipped files, etc.

To protect the network against application level attacks via the network such as targeting software vulnerabilities—which includes most network worms, or the sending of sensitive credit card data from a spyware infected system—an Intrusion Prevention System (IPS) is the recommended solution. Antivirus and IPS are two complementary solutions protecting against different types of attacks. An IPS should look deep into the application layer traffic to detect attacks. Here too, it is important to choose a solution that does more than merely inspects the packets at the network layer or decodes only a few protocols at Layer 7– the solution should understand and inspect application traffic of all types, fully understand the details of each protocol, and use a combination of methods such as application level stateful inspection, anomaly detection and other heuristics to stop threats.

Limit Attack Frequency With Access Control

An often overlooked attack protection element is the ability to control access to known malware download sites. By assembling an attack protection solution that incorporates Web filtering to block access to known malicious Web sites, IT managers can reduce the number of malicious downloads that are brought into the network. Another mechanism that can help reduce the number of incoming attacks is to implement a gateway antispam solution that can act as a preliminary filter by blocking known spam and phishing sources.

The Juniper Networks Solution – Best-in-Class Technology and Alliance Partners

To provide protection against inbound and outbound attacks at all levels, Juniper Networks® integrates a complete set of best-in-class content security software features (commonly referred to as Unified Threat Management (UTM) features) into the secure router and firewall/VPN line of platforms. By leveraging the development, support and market expertise of many of the leading content security partners, Juniper is able to deliver a set of best-in-class UTM features. Other vendors spread their development resources too thin by trying to develop and maintain every UTM component in-house. Still others use open source offerings which tend to be inconsistent in their quality and "catch-rate". However, with best-in-class technology partnerships, Juniper customers are assured that their networks will be protected against all types of malware attacks.

Stopping Inbound and Outbound Viruses, Spyware, and Adware Attacks

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. 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 reconstructs them, sending them on their way.

The Juniper-Kaspersky solution detects and protects against the most dangerous and virulent viruses, worms, malicious backdoors, dialers, keyboard loggers, password stealers, trojans and other malicious code. Included in the joint solution is a best-of-class detection of spyware, adware and other malware-related programs. Unlike some solutions that use multiple non-file based scanners to detect different types of malware, the Juniper-Kaspersky solution is based upon one unified comprehensive best-of-breed scanner, database, and update routine to protect against all malicious and malware-related programs.

Day-Zero Protection Against Application Level Attacks

Juniper Networks secure routers with IPS tightly integrates the same software found on the Juniper Networks IDP Series Intrusion Detection and Prevention Appliances to provide unmatched application-level protection against worms, trojans, spyware, and malware. More than 60 protocols are supported including those used by advanced applications such as VoIP and streaming media. Unmatched security processing power and network segmentation features protect critical high-speed networks against the penetration and proliferation of existing and emerging application-level threats. With multiple attack detection mechanisms including stateful signatures, protocol and traffic anomaly detection, backdoor detection, IP spoofing, and layer 2 attack detection, the secure routers perform in-depth analysis of application protocol, context, and state to deliver zero-day protection from application level attacks.

Integrated on Juniper Networks branch firewall/VPN platforms is the Deep Inspection firewall, a proven, IPS solution that builds on the strengths of Stateful inspection and integrates Stateful signatures and protocol anomaly detection mechanisms to provide both network

and application-level attack protection at the perimeter. Using policy-based management, administrators can pick and choose which protocols to inspect with protocol anomaly detection and/or Stateful signatures, what types of attacks to look for and which action to take if an attack is discovered. Attack coverage can be tailored to specific attack protection requirements using any one of four different Signature Packs[1]:

- **Base Signature Pack:** Protects Internet-facing protocols and services with a wide range of worm, client-to-server, and server-to-client signatures.
- **Server Signature Pack:** Detects and blocks external attacks that are targeting server infrastructure
- **Client Signature Pack:** Stops trojans, worms and other malware with an array of "client" oriented attack objects
- **Worm Mitigation Signature Pack:** Detects client-to-server and server-to-client worms to deliver comprehensive worm coverage against en masse, fast-moving worm outbreaks

Controlling Access to Known Virus Download sites

To block access to malicious Web sites, Juniper Networks has teamed with Websense by integrating their Web filtering software into the Juniper secure router and firewall/VPN appliances. Using the management GUI, an administrator can assemble an appropriate Web use policy based upon 54 different categories encompassing over 25 million URLs (and growing every day).

Blocking Common Inbound Spam and Phishing Attacks

Juniper Networks has teamed with Sophos to leverage its market leading real-time antispam reputation service for Juniper's branch and regional office platforms to help slow the flood of unwanted email and the potential attacks they carry. Installed on the Juniper Networks secure router or firewall/VPN gateway, the antispam reputation service filters incoming email traffic for known spam and phishing senders to act as a first line of defense. When email traffic from a malicious sender arrives, it is blocked and/or flagged so that the email server can take an appropriate action.

ANTIVIRUS SPECIFICATIONS (KASPERSKY LAB)	
Protocols scanned	SMTP, POP3, Webmail, FTP, IMAP, HTTP
Inbound/outbound protection	Yes/Yes
New virus responsiveness	On average every 30 minutes
Update frequency	On average hourly
Number of virus signatures	450,000 +
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

[1] Only one Signature Pack can be installed at any given time.
*Includes phishing, spyware, Keylogger and adware protection

INTEGRATED WEB FILTERING SPECIFICATIONS (WEBSENSE)	
URL database	>25 Million – growing daily
Pages covered within database	>3.9 Billion
New pages added	250,000 list changes every day
Number of categories covered	40 including phishing & fraud, spyware, Adult/Sexually Explicit, Alcohol & Tobacco, Criminal Activity, Gambling, Hacking, illegal Drugs, Intolerance & Hate, Tasteless & Offensive, Violence, Weapons
Languages	70
Countries	200
ANTISPAM SPECIFICATIONS (SOPHOS)	
SPAM list update frequency	The antispam list is updated every 60 seconds.
Types of spam covered	Botnet IPs, open proxies, known spam sources, and consumer IP ranges (usually dynamically assigned) known to be spammy or governed by service provider usage policies prohibiting direct sending of email.
Mechanisms (spam traps etc.) used for visibility and analysis	Reputation data is generated from millions of messages per day coming into Sophos's worldwide spam traps, analysis of queries and statistical customer feedback, DNS analysis, third-party relationships, and other mechanisms.

IPS	DEEP INSPECTION	INTRUSION PREVENTION SYSTEM (IPS)
Methods of detection	Two methods of detection: 1. Stateful Signatures 2. Protocol Anomaly (Zero-day coverage)	Six methods of detection: 1. Stateful Signatures 2. Protocol Anomaly (Zero-day coverage) 3. Traffic Anomaly 4. Backdoor Detection 5. IP spoofing 6. Layer 2 Attack Detection
Worm protection	Yes	Yes
Trojan protection	Yes	Yes
Other malware protection	Yes	Yes
Reconnaissance protection	Yes	Yes
Client to server and server to client attack protection	Yes	Yes
Create custom attack signatures	Yes	Yes
Application contexts for signature customization	90+	300+
Stream Signatures for worm mitigation	Yes	Yes
Number of response options	1. Close: Severs connection and sends RST to client and server 2. Close Server: Severs connection and sends RST to server 3. Close Client: Severs connection and sends RST to client 4. Drop: Severs connection without sending anyone a RST 5. Drop Packet: Drops a particular packet, but does not sever connection 6. Ignore: After detecting an attack signature or anomaly, the Juniper Networks device makes a log entry and stops checking – or ignores – the remainder of the connection 7. None: No action	1. Close: Severs connection and sends RST to client and server 2. Close Server: Severs connection and sends RST to server 3. Close Client: Severs connection and sends RST to client 4. Drop: Severs connection without sending anyone a RST 5. Drop Packet: Drops a particular packet, but does not sever connection 6. Ignore: After detecting an attack signature or anomaly, the Juniper Networks device makes a log entry and stops checking – or ignores – the remainder of the connection 7. None: No action

IPS	DEEP INSPECTION	INTRUSION PREVENTION SYSTEM (IDP)
Attack notification mechanisms	1. Session Packet Log 2. Session Summary 3. E-mail 4. SNMP 5. Syslog 6. Webtrends	1. Session Packet Log 2. Session Summary 3. E-mail 4. SNMP 5. Syslog 6. Webtrends
Create and enforce appropriate application usage policies	Yes	Yes
Frequency of updates	Monthly and Emergency	Daily and Emergency

	ANTIVIRUS*	ANTSPAM	WEB FILTERING (INTEGRATED / REDIRECT)**	IPS (DEEP INSPECTION / IDP)
SRX650 Services Gateway	Yes	Yes	Yes / Yes	No / Yes
SRX240 Services Gateway	Yes	Yes	Yes / Yes	No / Yes
SRX210 Services Gateway	Yes	Yes	Yes / Yes	No / Yes
SRX100 Services Gateway	Yes	Yes	Yes / Yes	No / Yes
J6350 Services Router	No	Yes	Yes / Yes	No / Yes
J4350 Services Router	Yes	Yes	Yes / Yes	No / Yes
J2350 Services Router	Yes	Yes	Yes / Yes	No / Yes
J2320 Services Router	Yes	Yes	Yes / Yes	No / Yes
SSG550M Secure Services Gateway	Yes	Yes	Yes / Yes	Yes / No
SSG520M Secure Services Gateway	Yes	Yes	Yes / Yes	Yes / No
SSG350M Secure Services Gateway	Yes	Yes	Yes / Yes	Yes / No
SSG320M Secure Services Gateway	Yes	Yes	Yes / Yes	Yes / No
SSG140 Secure Services Gateway	Yes	Yes	Yes / Yes	Yes / No
SSG20 Secure Services Gateway	Yes	Yes	Yes / Yes	Yes / No
SSG5 Secure Services Gateway	Yes	Yes	Yes / Yes	Yes / No

*Includes phishing, spyware, Keylogger and adware protection
**Includes protection against phishing and spyware sites (outbound)

Summary

Juniper Networks secure router and firewall/VPN appliances include UTM features that are backed by world class technology partnerships. When combined with market-leading performance and networking deliver a powerful solution that can protect against inbound and outbound attacks traversing the LAN and/or the WAN.

About Juniper Networks Content Security UTM Technology Partners

Kaspersky Lab – Integrated Antivirus (Antispyware, Anti-Adware, Antiphishing)

Founded in 1997, Kaspersky Lab is an international information security software vendor. The Kaspersky team of international virus analysts and developers work round-the-clock gathering information, evaluating new threats and designing new utilities for in-house and customer use. Over a decade of expertise ensures rapid responses to new threats, providing users with virus removal tools and information to pro-actively combat threats. The Kaspersky Lab Virus Lab has one of the largest collections of virus definitions in the world.

Websense – Integrated Web Filtering

Websense, Inc. (NASDAQ: WBSN), a global leader in integrated Web, messaging and data protection technologies, provides Essential Information Protection™ for more than 42 million employees at more than 50,000 organizations worldwide. Distributed through its global network of channel partners, Websense software and hosted security solutions help organizations block malicious code, prevent the loss of confidential information and enforce Internet use and security policies. Websense web filtering integrates seamlessly with Juniper Networks secure router and firewall/VPN products to offer unequaled flexibility and control.

Websense – Redirect Web Filtering (Off Box)

As an alternative to integrated web filtering, Juniper secure router and firewall/VPN solutions can redirect web traffic to a Websense server / gateway to provide customers a full-featured offering to control web access privileges, generate detailed usage reports, while still leveraging all the firewall/VPN features of the Juniper Networks devices.

Sophos – Integrated Antispam Protection

Trusted by over 100 million users in 150 countries and endorsed by industry analysts as a leader, Sophos provides a full range of security and data protection solutions that are simple to deploy, manage and use. At the core of Sophos's antispam technology is SophosLabs, a global network of blended threat research facilities. SophosLabs analyzes millions of emails and billions of web pages every day to deliver comprehensive threat protection to customers. Antispam analysis techniques such as IP reputation, advanced heuristics, message and attachment fingerprinting, keyword analysis, and malware, spam, and phishing URL detection are combined with real-time SXL technology to deliver proactive protection from emerging threats. Also available via SophosLabs, Behavioral Genotype provides proactive protection from fast-moving modern web threats including malware, spyware, adware and phishing, effectively guarding against evolving and zero-day threats.

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**.

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.

3510202-003-EN July 2010 Printed on recycled paper