UNIFIED THREAT MANAGEMENT—ALL-IN-ONE SECURITY FOR BRANCH AND SMALL TO MEDIUM OFFICES

UTM Offers Consolidated Layered Security Delivered on a Single Junos Operating System Platform

Challenge

In today's world of evolving threats, the increasing volume and sophistication of threats pose a serious challenge for IT teams as they work to protect their companies' most important digital assets with limited resources and budgets.

Solution

Juniper Networks Unified Threat Management (UTM) offers comprehensive security against malware, viruses, worms, trojans, phishing attacks, intrusions, denial-of-service (DoS) attacks, key loggers, spam, and other threats—all delivered on Junos operating system, reducing cost, complexity, and total cost of ownership (TCO).

Benefits

- Comprehensive, all-in-one, layered security solution
- Simplified security operations through Junos OS, a single operating system platform
- Reduced costs and complexity in a single, integrated device
- Better performance through optimized hardware with separate data and control plane
- More management options and control with user-role based policy
- Flexibility with cloud-based and on-box anti-malware options

With the increased volume and sophistication of today's evolving threats, IT security organizations are under enormous pressure to protect their companies' productivity and electronic assets under the daily pressure of frozen budgets and dwindling resources. A stateful firewall is not enough; today's challenges require a comprehensive security solution. Although point products can provide layered security, they also bring the added costs and complexity of multiple boxes and multiple operating systems. What IT teams need is an all-in-one, comprehensive, and integrated security solution that reduces complexity and lowers costs.

The Challenge

In today's world, threats are evolving with increasing volume and sophistication. Businesses are challenged to secure their networks against cyber attacks which have evolved from the "notoriety motive" to the "profit motive." Attackers now use advanced techniques to compromise companies and networks for financial gain. Already, cybercriminals earn billions of dollars a year, demonstrating the fact that they are organized and well financed. In fact, a recent Juniper-sponsored, Ponemon survey of U.S. businesses showed that:

- 90% of respondent businesses had been hacked in 2010
- 59% had been hacked multiple times
- 40% had sustained damages of $500,000 or more

Due to the pervasive nature of attacks, companies can be sure that it's a matter of "when" and not "if" an attack will occur. The threat landscape has borne witness to an exponential growth of malware and an ever decreasing window between vulnerability disclosure to rapid and aggressive exploit. Businesses are left vulnerable, overwhelmed, and alone with their reputations, customers, and assets at stake. With attacks on the rise, how do IT security teams respond and defend their businesses, especially given today's economic environment of frozen budgets and limited IT staff resources?

Juniper Networks Unified Threat Management

Juniper Networks® Unified Threat Management provides a solution to IT's most challenging security problems. It is available with Juniper Networks SRX Series Services Gateways, the only carrier-class security solution consolidating UTM content security services with routing and switching in a single, high-performance, and cost-effective network device. This consolidation enables organizations to securely, reliably, and economically deliver powerful new services and applications to all locations and users with superior service quality. SRX Series gateways are powered by Juniper Networks Junos® operating system, the same industry-leading OS platform that keeps the world's largest networks available, manageable, and secure.

UTM security is a comprehensive security approach providing defense-in-depth with layers that include antivirus/anti-malware, intrusion prevention system (IPS), AppSecure, enhanced Web filtering, content filtering, and anti-spam. The SRX Series also includes many other security layers, including next-generation firewall, VPN, Network Address Translation (NAT), and more.

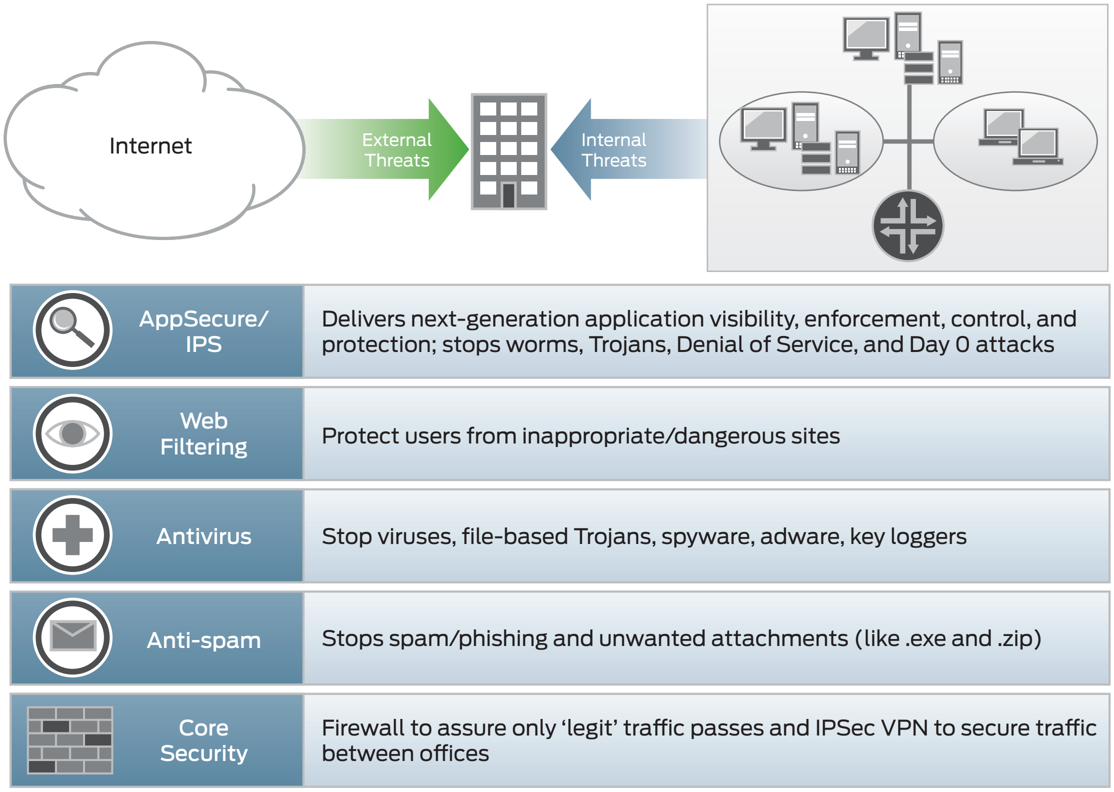
Features and Benefits

FEATURES	BENEFITS
Consolidated, all-in-one security	· Comprehensive, layered protection, including anti-malware, IPS, Web filtering, content filtering, and anti-spam · Application visibility and protection with user-role based policies against evolving application and Web 2.0 attacks · Preinstalled and quickly activated UTM capabilities on demand for zero-day, easy, and instant protection · Minimized purchase and management costs in a single-vendor security gateway device
Unified management	· Reduced IT management costs and complexity · Simplified operations for all security and networking delivered through Junos OS, a single operating system platform · Consolidated, centralized management simplifying efforts to plan, deploy, operate, and report on secure networks and applications
High value and performance	· Leverage Juniper's market proven security services and heritage in high-performance, carrier-grade networking technology · Lower TCO with a single integrated UTM solution that delivers all security and networking, avoiding costs of multiple boxes and acquisition complexity of a multi-vendor solution · Automation via modular scripting, integrated diagnostics, and embedded debugging

Solution Components

Antivirus/anti-malware protects the network from malware, viruses, spyware, worms, trojans, and other attacks, as well as e-mail and web-based threats that can compromise business productivity and corporate assets. Anti-malware can be delivered via two different models:

- **Cloud-based protection** leverages real-time, up-to-date, cloud-based resources with the on-box horsepower of SRX Series gateways to deliver a lightweight and fast anti-malware solution. It also delivers Web security by blocking access to malicious URLs. The result is a highly effective barrier against malware that also delivers top-notch network performance for users and business productivity.
- **On-box protection** leverages a scanning engine that deconstructs the payload to evaluate and detect potential malware. Unlike other solutions that use multiple disparate scanners and evaluate only a subset of data (i.e., packet or stream level only), Juniper takes full advantage of a unified, best-in-class engine to protect business productivity.



AppSecure/ IPS	Delivers next-generation application visibility, enforcement, control, and protection; stops worms, Trojans, Denial of Service, and Day 0 attacks
Web Filtering	Protect users from inappropriate/dangerous sites
Antivirus	Stop viruses, file-based Trojans, spyware, adware, key loggers
Anti-spam	Stops spam/phishing and unwanted attachments (like .exe and .zip)
Core Security	Firewall to assure only 'legit' traffic passes and IPSec VPN to secure traffic between offices

Figure 1: UTM protects organizations against outgoing and incoming threats with a comprehensive, layered security approach.

IPS accurately detects and protects the network against intrusions and other attacks. By implementing detection methods that include protocol and traffic anomaly, stateful signatures, synflood, spoofing, and backdoor detection. IPS secures the network with sophisticated analysis techniques, fast response to new attacks, and the expertise of a dedicated security research team. IPS is able to prevent reconnaissance (the ability for attackers to gain valuable network information), incoming attacks (to stop hackers before they can compromise the network), and proliferation (attacks that can readily spread in the network after they have found a foothold).

AppSecure is a suite of application-aware security services that classifies traffic flows, brings greater application visibility, enforces application firewall rules, controls application usage, and protects the network. AppSecure uses a sophisticated classification engine to gain intelligence that accurately identifies applications regardless of port or protocol, including nested applications that reside within trusted network services. These capabilities combine to deliver needed protection against the growing number of application and Web 2.0 attacks.

Enhanced Web Filtering (EWF) delivers protection against potentially malicious websites in a number of ways. EWF features 95 URL categories, providing fine-grained control of URLs to help administrators monitor network activity and ensure compliance with acceptable use policies. EWF uses the most up-to-date, real-time reputation analysis, powered by a next-generation network that scans more than 40 million websites every hour for malicious code, to ensure that the latest URL category and content classification data is available to the security gateway. EWF also utilizes a cumulative threat score for all URLs, both categorized and uncategorized, enabling businesses to log and/or block disreputable sites. In addition, EWF improves business productivity and network performance, as IT can limit user access to non work-related websites.

Anti-spam improves network performance by blocking spam messages. It offers flexibility and is compatible with both on-premise or hosted e-mail solutions. An SRX Series security gateway receives e-mails destined for the e-mail server in the DMZ or the trust zone to compare the e-mail source address with the local white list/black list. If there is no match, the SRX Series device sends the e-mail source address to the cloud-based anti-spam service. This service checks the host address against the constantly updated list and returns a block, permit, or log to the SRX Series device. Lastly, the SRX Series tags the e-mail as spam or allows it through, and the e-mail server can then use the tag locally for subsequent decisions. In this way, anti-spam blocks e-mails from malicious sources to counter phishing attacks and also to improve network performance.

Summary—All-in-One Security with Unified Management for Superior Performance and Lower TCO

With evolving threats growing in number and sophistication, businesses need a comprehensive, layered solution that is easily managed to provide the security, performance, and value IT teams require. Juniper Networks Unified Threat Management is the solution to IT's most challenging security issues. It provides comprehensive protection against incoming and outgoing threats, simplifies operations, reduces costs, and delivers exceptional value.

Next Steps

For more information about UTM and its components, including SRX Series Services Gateways, please contact your Juniper Networks representative.

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.

3510202-005-EN Apr 2012

Printed on recycled paper