

# Managing Threats Across the Enterprise Network

## Situation

With the threat landscape continuing to evolve, organizations require a solution to stop threats at all layers of the network to protect their critical business resources across all areas of the network.

## Solution

Juniper Networks enables enterprises to deploy seamless threat protection for all locations of the network to prevent attacks from compromising corporate assets.

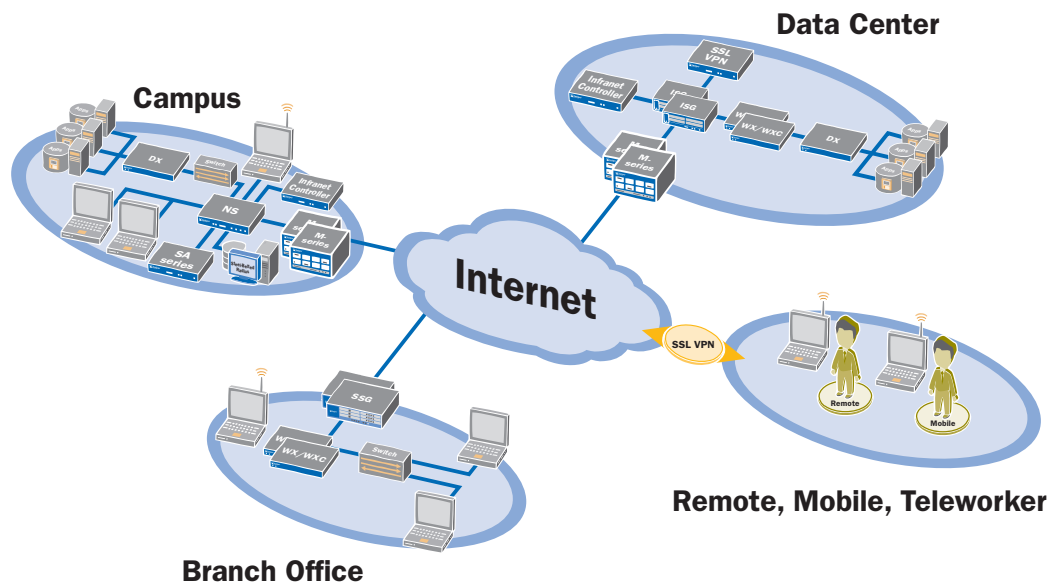
## Business Value

- Protect networks from threats to prevent network downtime and service degradation, which can result in lost employee productivity and lost sales opportunities.
- Reduce operating expenses with integrated security solutions that are easy to deploy, manage, and maintain.
- Mitigate threats to meet an organization's risk stance, protecting corporate assets anywhere in the network and ensuring that lack of security doesn't negatively affect the organization's reputation.

## Enterprise Threat Management Overview

The threat landscape continues to evolve, with increasingly complex attacks directed at the corporate network to achieve malicious goals. Protecting the network from internal and external threats to prevent harm to the network, applications, and users is becoming an increasingly difficult job. Threats are emerging and spreading more quickly than ever before and have more possible points of entry into a network because of increases in user mobility, the number of remote locations, and the number of devices accessing the network. The continued rollout of new applications also poses incremental risks for new attacks.

Enterprises require a complete, holistic solution that provides layered security for threat protection at all layers of the network and at every location of the network, including the data center, branch offices, campus, and extended enterprise. Without such a solution to manage threats in a network, enterprises can incur losses. If a network is attacked, or if clients and servers are infected with malware, the company can suffer from lost productivity and revenue. Failure to meet compliance requirements for proper security and threat controls can result in heavy fines. Further, if an attacker manages to successfully compromise an organization's network that does not have proper threat protection in place, the financial impact can be enormous. In addition to the potential loss of precious corporate assets such as confidential customer data, a successful targeted attack can yield negative publicity for an organization, resulting in damage to its reputation and possible loss of brand equity and weakening of competitive positioning.



Juniper Networks Provides Seamless Threat Protection Across the Entire Network

## Juniper Networks Threat Management Solutions

The Juniper Networks approach to threat management provides seamless protection across the entire network, providing network and application layer threat protection (Figure 1).

Solutions from Juniper Networks:

- Protect the network from internal and external threats
- Allow organizations to set and enforce security policies
- Provide visibility into network activity

### Protection from Internal and External Threats

Juniper Networks provides protection from internal and external threats through a range of integrated security solutions appropriate for all locations of the distributed enterprise. These solutions prevent unauthorized access to secure corporate data, applications, and intellectual property and help securely connect remote locations to each other and to central sites such as data centers. Juniper Networks threat management solutions stop viruses, spyware, adware, and other malware and block unwanted e-mail from known spammers and phishers. When new business applications are introduced and new vulnerabilities emerge, Juniper Networks threat management solutions prevent application-level attacks from flooding the network, thereby minimizing service interruptions.

### Setting and Enforcement of Security Policies

Juniper Networks enables organizations to set and enforce security policies with robust centralized management that gives administrators the capability to manage all aspects of security from a single location, thereby reducing operational costs and removing complexity from policy configuration and administration. Centralized management can reduce risk by helping ensure more consistent deployment of threat management policies throughout the network and by restricting application access to valid users and devices. Additionally, Juniper Networks threat management solutions can help businesses enforce acceptable network use policies by providing the capability to restrict access to an undesirable or malicious Web site, thus preventing inappropriate use of corporate resources.

### Visibility into Network Activity

Juniper Networks offers visibility into network- and application-layer traffic to provide the granular threat protection and control required to stop threats in the network. Custom reporting using centralized management provides enterprise-wide network visibility from a centralized location. With visibility into who is using what specific applications and assets on the network, organizations can tailor their security policies to ensure that the network is safe and also deliver on the critical business requirements of the enterprise. Without visibility, organizations can be victimized by attacks that they didn't know they were vulnerable to and can waste resources researching, containing, and responding to these attacks.

## Juniper Networks Partners and Alliances

Company	Products and Services
Symantec	Symantec Anti-Spam for Juniper Networks is an integrated anti-spam solution that blocks spam by using a robust, IP-based, constantly updated worldwide list of spammers and phishers.
Kaspersky	Kaspersky Anti-Virus for Juniper Networks is an integrated gateway anti-virus solution that protects Web traffic, e-mail, and Web mail from file-based viruses, worms, backdoors, Trojans, and malware.
SurfControl	SurfControl Web Filter for Juniper Networks is a fully integrated firewall/VPN and Web filtering solution that enables companies to cost-effectively monitor network use and abuse anywhere in the organization across the full spectrum of Web-based content: instant messaging, peer-to-peer (P2P), streaming media, file downloads, and Web-based e-mail. Best-in-class protection against Web-based threats is combined with a high level of visibility and control to reduce risk, enable business compliance, and help ensure business continuity.

## Juniper Networks Solution Portfolio for Threat Management

Firewall and VPN	Intrusion Prevention	Centralized Management
Secure Services Gateways (SSGs) and NetScreen Firewall/VPN appliances	Intrusion Detection and Prevention (IDP)	NetScreen-Security Manager (NSM)
<ul style="list-style-type: none"> <li>Complete line of integrated firewall / VPN solutions that scales from small branch offices to the largest data centers</li> <li>Unified Threat Management (UTM) security features, including Stateful firewall, IPS, Antivirus (Anti-Spyware, Anti-Phishing, Anti-Adware), Anti-Spam, and Web Filtering, to protect the network from attack (some models)</li> <li>Multiple management mechanisms, including complete command-line interface (CLI), WebUI, and centralized management with NetScreen Security-Manager, to facilitate rapid deployment while reducing ongoing operating costs</li> </ul>	<ul style="list-style-type: none"> <li>Quick inline deployment to effectively identify and stop network and application-level attacks before they inflict any damage, minimizing the time and costs associated with intrusions</li> <li>Zero-day protection against worms, Trojans, spyware, keyloggers, and other malware through the use of industry-recognized stateful detection and prevention techniques</li> <li>On-demand views of network and application-level activity to help administrators determine the root cause of attacks</li> </ul>	<ul style="list-style-type: none"> <li>Centralized administration and simplification of policy management</li> <li>Unsurpassed visibility into application- and network-layer traffic</li> <li>Granular control of configuration, network settings, and security policies</li> </ul>

## About Juniper Networks

Juniper Networks develops purpose-built, high-performance IP platforms that enable customers to support a wide variety of services and applications at scale. Service providers, enterprises, governments, and research and education institutions rely on Juniper to deliver a portfolio of proven networking, security, and application acceleration solutions that solve highly complex, fast-changing problems in the world's most demanding networks. Additional information can be found at [www.juniper.net](http://www.juniper.net).

CORPORATE HEADQUARTERS  
AND SALES HEADQUARTERS  
FOR NORTH AND SOUTH AMERICA

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](http://www.juniper.net)

EAST COAST OFFICE

Juniper Networks, Inc.  
10 Technology Park Drive  
Westford, MA 01886-3146 USA  
Phone: 978.589.5800  
Fax: 978.589.0800

ASIA PACIFIC REGIONAL  
SALES HEADQUARTERS

Juniper Networks (Hong Kong) Ltd.  
Suite 2507-11, 25/F  
ICBC Tower  
Citibank Plaza, 3 Garden Road  
Central, Hong Kong  
Phone: 852.2332.3636  
Fax: 852.2574.7803

EUROPE, MIDDLE EAST, AFRICA  
REGIONAL SALES HEADQUARTERS

Juniper Networks (UK) Limited  
Building 1  
Aviator Park  
Station Road  
Addlestone  
Surrey, KT15 2PG, U.K.  
Phone: 44.(0).1372.385500  
Fax: 44.(0).1372.385501

Copyright © 2007, Juniper Networks, Inc.  
All rights reserved. Juniper Networks and  
the Juniper Networks logo are registered  
trademarks of Juniper Networks, Inc. in  
the United States and other countries. All  
other trademarks, service marks, registered  
trademarks, or registered service marks in this  
document are the property of Juniper Networks  
or their respective owners. All specifications  
are subject to change without notice. Juniper  
Networks assumes no responsibility for  
any inaccuracies in this document or for  
any obligation to update information in this  
document. Juniper Networks reserves the  
right to change, modify, transfer, or otherwise  
revise this publication without notice.

