

Juniper Networks Adaptive Threat Management Solutions

Implement these Dynamic and High-Performance Security Solutions to Gain Network-wide Visibility and Control to Adapt to Evolving Security Risks



Solutions Overview

The high-performance business is under increasing pressure to provide bulletproof protection against today's sophisticated and damaging security threats such as worms, viruses, Trojans, spyware, and other malware and to prevent them from propagating across the enterprise. Because of the strategic importance of the network, organizations cannot afford a security breach, compromised network performance, or unplanned downtime. Concurrently, the high-performance business must meaningfully address business continuity during real-world disasters such as strikes and earthquakes without compromising the security posture of the network.

No longer is the network defined by a model of trusted internal users surrounded by physical network security that protects the enterprise from outsiders who must be granted restricted network access for collaboration and business efficiency and operations. The interconnected global network must support an increased number of users that includes suppliers, partners, customers, and remote workers. Furthermore, there is a proliferation of sophisticated mobile devices by which this diverse set of users accesses the growing number of business critical and collaborative applications.

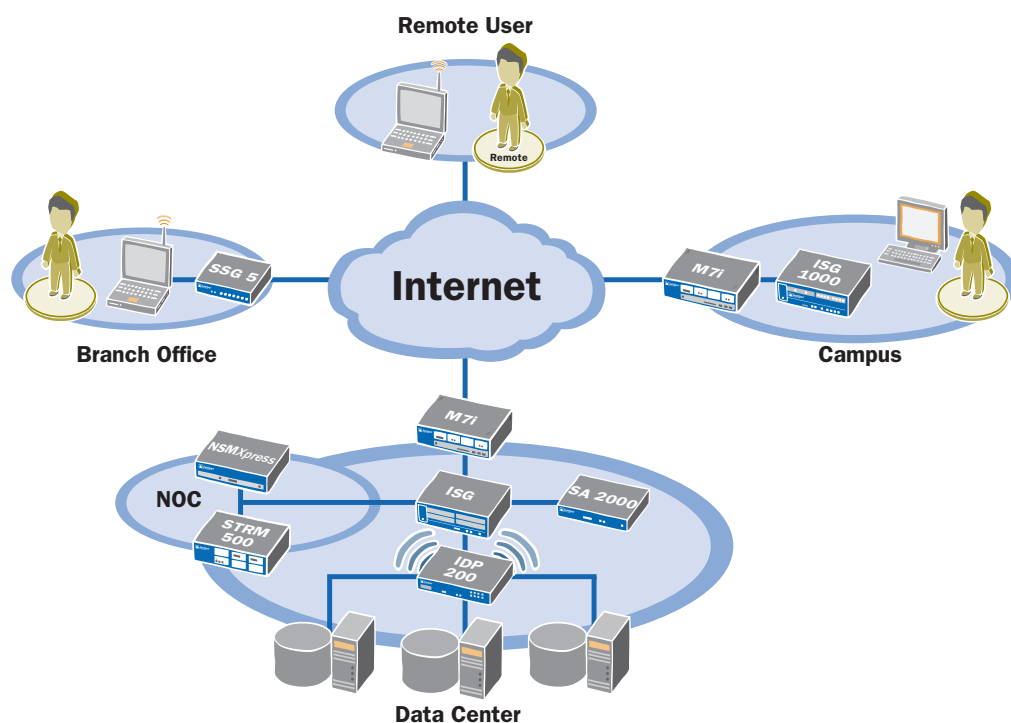
Compliance requirements, as well as governance policies, drive the enterprise's need for both complete visibility and manageability of the network and applications and comprehensive, multilayered security to protect against a wide range of security threats at wire speed. IT departments are tasked with ensuring uninterrupted and network-wide access in this dynamic environment while protecting users, data, applications, and infrastructure from current and emerging security threats.

Juniper Networks Adaptive Threat Management Solutions identify, mitigate, and report on the most complex security attacks in real time while supporting compliance requirements and reducing management overhead so that IT can allocate resources to other initiatives.

Challenges

Today's businesses are becoming increasingly global, requiring employees, contractors, partners, and customers to collaborate and access a variety of applications from a variety of locations. This collaboration explosion, fueled by the adoption of new business applications and the Webification of existing applications, is driving the demand for higher bandwidth networks. Further adding to the challenge is the increased use of new devices, such as smart phones and handheld mobile computing devices, to access enterprise applications in real time.

The sophistication of threats and the sheer volume of attacks and their speed of occurrence makes proactively identifying and responding to malicious activity increasingly difficult for today's IT departments. Collecting and analyzing enormous volumes of data from multiple sources (routers, switches, firewalls, and so on) is extremely time and resource intensive for IT, preventing IT from taking timely preventive actions without spending time needlessly chasing false positives. This situation is further complicated by limited or even shrinking budgets that preclude the possibility of hiring additional staff to attempt this sort of manual intervention. Without a comprehensive solution of highly integrated security products that can proactively address security breaches without IT intervention, this task can be insurmountable.



The Challenge

Because the network is a strategic asset, enterprises cannot afford a security breach, compromised network performance, or unplanned downtime. Existing security solutions cannot adapt and scale to meet the changing security landscape that challenges the enterprise.

The Solutions

Juniper Networks Adaptive Threat Management Solutions comprise high-performance security platforms that leverage a dynamic cooperative system and network-wide visibility and control in order to adapt to changing risks

Juniper Benefits

Juniper Networks Adaptive Threat Management Solutions provide a responsive and trusted security environment for your high-performance network.

Figure 1. Example of a Network Protected by Juniper Networks Adaptive Threat Management Solutions

Trends

Commonly deployed security solutions fall short of protecting high-performance networks because they:

- Fail to adapt to and mitigate evolving threats
- Lack multi-layered security to protect against a wide range of threats coming from multiple attack vectors
- Lack network-wide visibility and control through tight integration between security products
- Lack automation to stop attacks in real time
- Create performance bottlenecks in the network under heavy traffic load
- Lack centralized management and reporting capabilities needed to determine the health of the network, ensure compliance, and correlate and analyze vast amounts of data for insightful analysis, recommendations, and reports
- Cannot provide consistent policy and protection for remote users

Juniper Networks Adaptive Threat Management Solutions

Juniper Networks Adaptive Threat Management Solutions are a set of dynamic and high-performance security solutions that adapt to changing risks. By leveraging a cooperative system that uses each of the individual security components, Adaptive Threat Management Solutions provides networkwide visibility and control that adapts and secures the environment against constantly evolving threats through dynamically sharing risk information and performing mitigation actions, as illustrated in figures 2 and 3.

Figure 2. Evolution of Threat Management Solutions to Address Enterprise Security Requirements

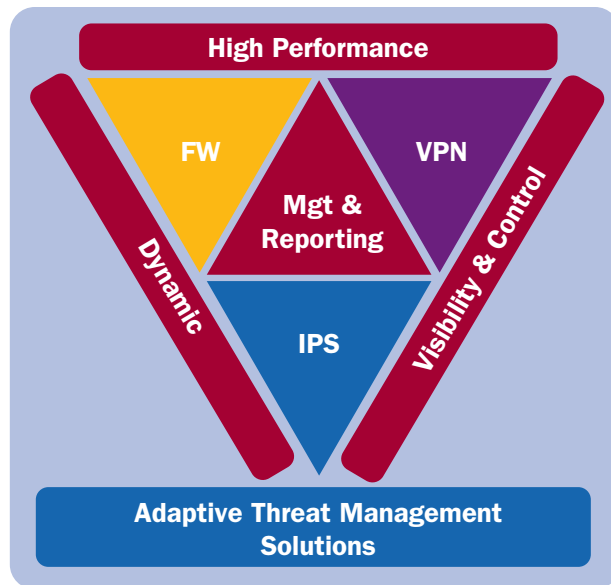
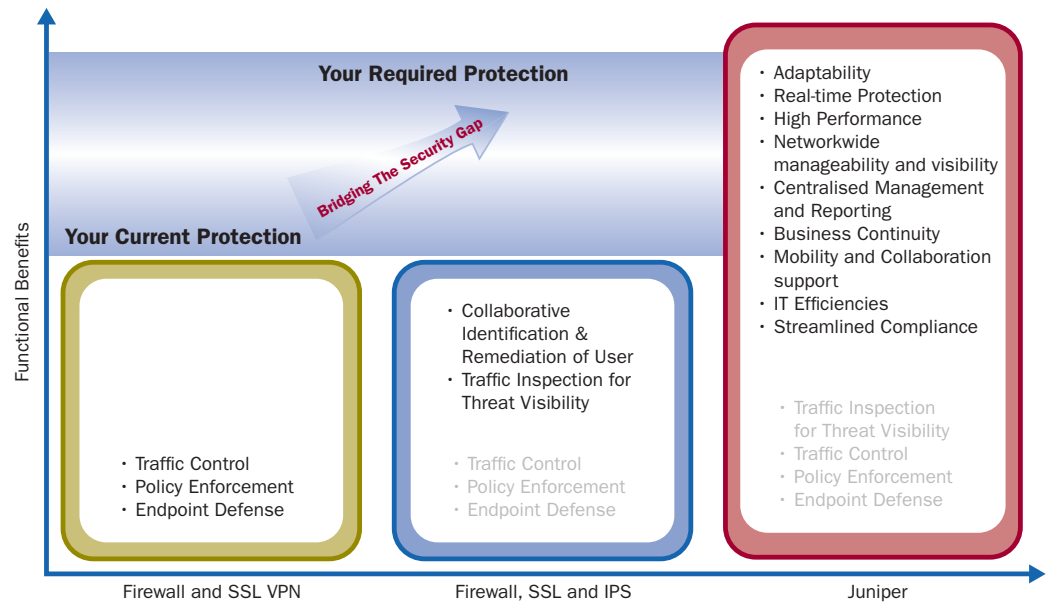


Figure 3. Solution Elements of Juniper Networks Adaptive Threat Management Solutions

Table 1. Solution Matrix

Product	Highlights
Firewall/VPN	<ul style="list-style-type: none"> • High performance purpose-built line of firewalls (SSG, ISG and NS-5000 systems) scaling from enterprise to service providers • Tightly integrated set of best-in-class unified threat management security features to protect against a wide range of worms, viruses, Trojans, spyware, denial-of-service, and blended or content based attacks • Secure site-to-site communication between distributed branch offices and corporate HQ locations
Intrusion Detection & Prevention (IDP)	<ul style="list-style-type: none"> • High performance with industry leading 10 Gbps throughput. • Comprehensive easy-to-use protection to stop network and application level attacks • Application visibility to ensure compliance to business practices and enforce application-based QoS
Secure Access (SA)	<ul style="list-style-type: none"> • Market leading SSL VPN features, including secure virtualization, access privilege management, host check, monitoring and reporting • Scalable to tens of thousands of concurrent users • Coordinated threat control (unique interoperability between Juniper Networks IDP and SA SSL VPN) enables automatic response to isolate specific users in case of network attacks
Juniper Networks NSM	<ul style="list-style-type: none"> • Centralized security policy management facilitates rapid deployment while minimizing ongoing operational costs
Security Threat Response Manager (STRM)	<ul style="list-style-type: none"> • Efficiently manages logs and flows, identifies prioritized offenses, and reduces operational complexity through a single appliance • Compliance support for monitoring reporting and auditing processes of regulatory and security standards • Provides a detailed view into the systems that are available remotely and suggest appropriate changes • Multi-vendor support for a wide range of network and security devices

Key Differentiators of Juniper Networks Adaptive Threat Management Solutions

Today's security market offers a dizzying array of products—often point products. Point products are costly to deploy and manage, fail to offer networkwide visibility and control, and do not offer the dynamic capabilities needed to support high-performance networks. Juniper Networks Adaptive Threat Management Solutions break the traditional mold of complex and costly point security products that solve only one security challenge, differentiating itself in the marketplace with its dynamic and high-performance security and visibility and control. Adaptive Threat Management Solutions are a solutions-based approach that delivers comprehensive security that keeps your business safe.

Dynamic Security

Threats can sink your business, but your security solution should not. Building on a highly cooperative and integrated approach between security products, Adaptive Threat Management Solutions use advanced threat detection techniques to proactively identify, mitigate, and report threats before they affect your business. Tactics used by Adaptive Threat Management Solutions to address today's business risks include addition of new signatures, signatureless attack detection, access control adjustments on a per-group or per-user basis, and end-point policy checking and enforcement. Self-remediation and autoremediation help reduce the drain on IT resources and time.

Collaboration between devices such as the Juniper Networks Intrusion Detection and Prevention (IDP) and Secure Access (SA) SSLVPN automatically take action against users who are not complying with set security policies by forcing the users to remediate, dropping violating traffic, or notifying IT so IT staff can deal with the users who are not in compliance. The Juniper Networks NetScreen-Security Manager (NSM) and Security Threat Response Manager (STRM) devices track changes and can report on them in real time or historically.

High-Performance Security

A successful business requires compromises, but network security and performance should not. The performance and throughput of security devices are not generally put to the test under normal business conditions. In the event of a new virus or worm outbreak or distributed-denial-of-service (DDoS) attack, security devices such as the intrusion prevention system (IPS), firewall, SSL VPN, or security information and event manager (SIEM) must be able to support the increased traffic load without compromising security or performance. Otherwise, the hacker wins.

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

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.
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, 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 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Additionally, in the event of a physical disaster such as an earthquake, the number of remote logins will likely spike upward. If the SSL VPN device cannot support the additional load, the business cannot securely operate. Adaptive Threat Management Solutions are a high-performance security solution that enables enterprises to protect critical assets that reside in the network core, data center, and branch offices without the traditional performance trade-off. Juniper prides itself on delivering outstanding security without sacrificing performance. Each individual solution element is highly scalable to accommodate growth in network traffic, and with its collaborative nature, Adaptive Threat Management Solutions have been proven to scale even in the most demanding networks with the highest rates of throughput.

Visibility and Control

You cannot control what you cannot see. Juniper offers comprehensive and innovative centralized management, monitoring, and reporting capabilities with STRM and NSM devices. Adaptive Threat Management Solutions offer exceptional visibility and support for previously deployed third-party devices, giving you the freedom to select new or build on existing products that are right for you. Moreover, IT departments gain a networkwide view for monitoring, trending, and reporting. The cooperative approach between the security products that form the Adaptive Threat Management Solutions enable IPS inspection, deep packet inspection, anomaly detection, and application inspection all correlated to the user and the relevant user group. In combination with SSL VPN host checker capability, firewall inspection, and reporting by the STRM device, the Adaptive Threat Management Solutions protect both managed and unmanaged devices. Sophisticated correlation methods can uncover the true attacks that can bring down the business while reducing the false positives that can needlessly waste IT time.

Summary: Adaptive Threat Management Solutions – Ensuring the Security of Your High Performance Network

Juniper is committed to delivering a dynamic and high-performance security solution—Adaptive Threat Management Solutions – that provides networkwide visibility and control to address the constantly evolving security landscape. Business benefits include proactive data protection, business continuity, and reduced TCO. IT benefits include fewer network disruptions, IT resources freed from mundane tasks, and support for compliance requirements.

As threats change, Adaptive Threat Management Solutions will continue to adapt to ensure proactive protection, business continuity, and security compliance while reducing costs.

To learn more about Juniper Networks Adaptive Threat Management Solutions, contact your Juniper Networks representative for more information. Additional information can be found at www.juniper.net/adapt.

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.

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

