

INCREASING CYBER SECURITY READINESS WITH ADAPTIVE THREAT MANAGEMENT

Essential Insights for Strengthening the
Federal Response to Cyber Attacks

Table of Contents

Executive Summary	3
Introduction	3
Cyber Security Challenges	4
Shortcoming of Current Security Approaches	4
Juniper Networks Adaptive Threat Management Solutions	5
Multivendor Visibility and Event Correlation	5
Dynamic, Adaptive Threat Control	6
Consolidated Security and Compliance Reporting	6
Consolidated Policy Management	6
Adaptive Threat Management Solutions Benefits	6
Conclusion—Meeting the Cyber Security Challenge	8
Appendix A	8
About Juniper Networks	9

Table of Figures

Figure 1: Evolution of Threat Management Solutions to Address Government Cyber Security Requirements	4
Figure 2: Key Elements of an adaptive threat management solution	5
Figure 3: Integrated Adaptive Threat Management Solutions for Government	7

Executive Summary

The U.S. Federal Government depends on the vast array of systems and networks in cyberspace to support all aspects of their operations. Unfortunately, this dependence on cyberspace leaves agencies vulnerable to cyber attacks. Threats are growing in number and sophistication, originating from both domestic and foreign sources and encompassing intentional attacks as well as inadvertent causes. Despite ongoing investments in security products, many federal IT managers feel their infrastructure is inadequate for combating rapidly evolving threats and for ensuring compliance with government mandates and directives.

Security experts agree that a new approach to threat management is needed, one that adapts to threats and dynamically provides a coordinated response in real time. Juniper Networks® Adaptive Threat Management Solutions have been designed to deliver this new approach to cyber security. A set of dynamic and high-performance security platforms, the Adaptive Threat Management Solutions provide network-wide visibility and control capable of adapting to changing security risks. With Adaptive Threat Management Solutions, federal agencies can proactively protect data and boost compliance and continuity of operations, while reducing total cost of ownership for a greater return on their security investment.

Introduction

Recent news reports that a foreign entity has repeatedly hacked the White House computer network are a fresh reminder of the vulnerabilities posed by the global collection of networks and systems that make up “cyberspace.” Unfriendly nations, terrorist organizations, and criminals have been implicated in cyber espionage and attacks whose goals range from theft of intelligence, technology, and money to disruption of vital services and defense systems.

The U.S. Federal Government increasingly relies on cyberspace to support day-to-day activities, administrative services and mission-critical operations. The country’s national, economic, and homeland security are now fully dependent on the vitality of cyberspace. However, this array of computer networks and heterogeneous audience that requires network access poses security risks that threaten defense, intelligence and civilian agencies with data theft and corruption, compromised network performance, and unplanned downtime.

The number and sophistication of cyber threats continues to rise, originating from both domestic and foreign sources and encompassing intentional attacks as well as inadvertent causes. Consequently, concern about cyber security—the protection of information systems from ever-changing external and internal threats—is at an all-time high. The U.S. Government has invested heavily in security solutions to combat these threats as well as to comply with federal security mandates such as the Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), and Homeland Security Presidential Directive 12 (HSPD-12).

Unfortunately, many federal IT managers don’t feel their investment has made their agency more secure. They believe they need a new approach to cyber security to keep up with rapidly evolving threats, such as hard-to-identify blended attacks, accidental downloads of malicious code by insiders, and attacks by foreign entities and organized criminals. In a recent survey of federal IT decision makers, half of the respondents cited their agency’s existing, unintegrated security architecture as a major barrier to improved information security.¹

Security experts point to the need for an innovative approach to threat management that’s both dynamic, adaptive and leverage all security products that they have currently deployed. “The threat sources, the threat agents are changing constantly,” noted Dr. Ron Ross, a NIST senior computer scientist and information security researcher, in a recent edition of *Federal Computer Week*. “So we have to have a process that’s able to manage risk in the very dynamic and volatile environment that we see today” – a process that Ross calls “real time risk management.”²

As reported in *Dark Reading*, Gartner vice president and fellow Neil MacDonald has described an adaptive security infrastructure as a synchronized security system that adapts to threats in real time rather than in the aftermath of an attack. In addition to dynamically coordinating security and network gear, adaptive security solutions also provide consolidated logging, event correlation and alerting for troubleshooting and forensic purposes, according to MacDonald.³

These experts validate Juniper Networks’ approach in designing the Adaptive Threat Management Solutions, a set of dynamic, collaborative, and high-performance security solutions that provide network-wide visibility and control capable of adapting to changing security risks. With Adaptive Threat Management Solutions, government agencies can proactively protect data, manage federated access policies, more easily meet compliance requirements and boost continuity of operations while lowering total cost of ownership.

Cyber Security Challenges

Combating cyber threats is a significant challenge for government agencies that are also wrestling with flat security budgets, shifts in security policies, and a shortage of qualified IT staff.⁴ In implementing a cyber security plan, federal IT and network managers must address the dynamic nature of the cyberspace threat environment and must comply with a broad range of security and compliance directives. Meeting these objectives effectively and within budget is often a daunting task.

Malicious attacks are escalating, and include everything from hacking to bots and spyware infestations. According to the U.S. Department of Homeland Security (DHS), federal agencies identified some 37,000 reportable network intrusion incidents last year—and that number is only expected to grow.⁵ Beyond the sheer volume of attacks is their increasing complexity: viruses, worms, denial of service (DoS) and other threats evolve rapidly. Federal agencies must contend with ever more sophisticated, blended attacks as well as zero day viruses; malware planted in reputable web sites; remote access vulnerabilities; and targeted attacks against both known and unknown vulnerabilities.

Agencies also face internal threats, some of which – like unauthorized access – may be malicious in nature. Other internal vulnerabilities can result from oversight or accident, such as a firewall being misconfigured or a user not following security procedures (i.e., clicking on a phishing link and unwittingly downloading a Trojan). Loss or manipulation of agency data—and the resulting risk to assets, people, and privacy—can have serious consequences, even if accidental. These types of vulnerabilities can be hard to detect and correct especially when the user has been granted access to applications and network resources.

In addition to combating cyber threats, IT staff must also demonstrate compliance with a broad range of mandates, including FISMA, HIPAA, HSPD-12, National Security Presidential Directive 51/HSPD-20 and the Trusted Internet Connections (TIC) Initiative. (For more information on these mandates, see Appendix A.) To meet compliance requirements, network managers typically must document the controls they have in place as well as provide an audit trail and other metrics that confirm the effectiveness of these controls.

Shortcoming of Current Security Approaches

Federal IT departments have worked hard to build secure infrastructures. Too often, however, current infrastructures aren't achieving the desired outcomes because they're complex to manage, opaque, and uncoordinated. Agencies typically deploy a mix of security and network devices and applications from various vendors. This forces network staff to learn and maintain multiple management systems. The fact that each type of appliance is managed separately complicates security enforcement and regulatory compliance.

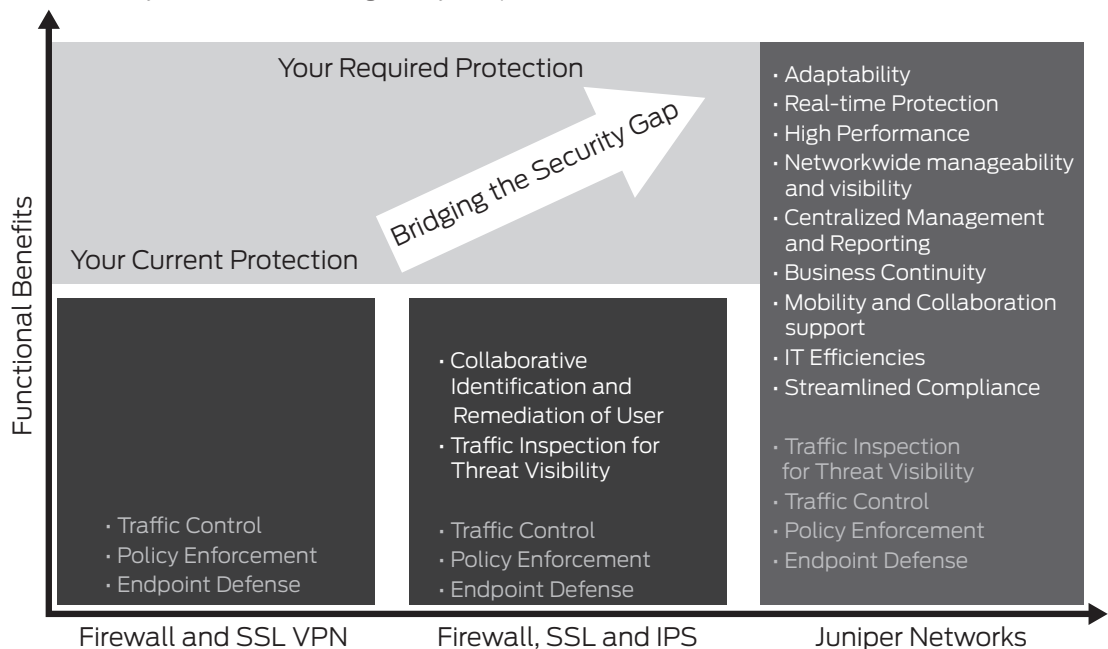


Figure 1: Evolution of Threat Management Solutions to Address Government Cyber Security Requirements

For example, each network and security device tracks events and generates its own log within its own management console. Network managers must ping-pong between consoles and manually correlate security incident data in order to coordinate responses to attacks (for example, they must determine that a router and firewall are seeing an attack from the same IP address before they can take action). Given the huge volume of discrete management data that each device generates, manual review and correlation is impossible. IT staff can miss a security breach completely because the signs of an attack are evidenced piece-meal across multiple management consoles. Blended attacks, which are designed to evade traditional detection mechanisms, are particularly difficult for IT to identify and counter using discrete security and network management tools. As a result, people, critical applications and assets are at risk.

This management complexity drives up the cost of cyber security and increases the potential for failures due to misconfiguration, oversight, and leakage. It also limit IT's visibility into and control over resource usage, which makes it difficult to comply with government mandates. In addition to the lack of visibility across management systems, the various network devices themselves lack the necessary interfaces to coordinate threat response, which increases risk exposure. For example, an intrusion detection and prevention (IDP) device from Vendor A might identify anomalous traffic coming from a remote user, but has no feedback mechanism for alerting the remote access platform from Vendor B to shut down that user's traffic at the source.

Civilian, intelligence, and defense agencies need an adaptive threat management solution that's high performance, reliable and interoperates with current network appliances, allowing network managers to respond proactively in real time to constantly evolving cyber threats. Agency managers need an interoperable cyber security infrastructure that dynamically protects data availability, integrity and confidentiality, expedites risk resolution and compliance, and reduces total cost of ownership (TCO).

Juniper Networks Adaptive Threat Management Solutions

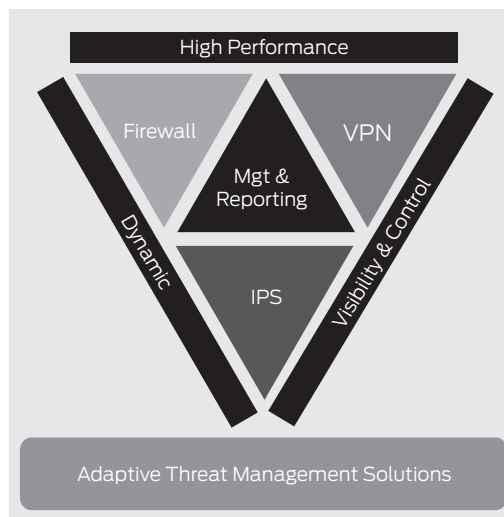


Figure 2: Key Elements of an adaptive threat management solution

Adaptive Threat Management Solutions address the challenges of cyber security by providing two strategic capabilities missing in current solutions: visibility and event correlation across a multi-vendor infrastructure, and a cooperative system of tightly integrated security products that interoperate with existing network security applications. By providing real-time, network-wide visibility into anomalous traffic and coordinating the actions taken by network and security devices, Juniper Networks Adaptive Threat Management Solutions accelerate the identification and mitigation of risks. Federal agencies benefit from greater overall security, asset protection and regulatory compliance, as well as a boost in IT's efficiency.

Adaptive Threat Management Solutions include high-performance firewalls, Juniper Networks SA Series SSL VPN Appliances, IDP Series Intrusion Detection and Prevention Appliances, SRX Series Services Gateways, Network and Security Manager, and STRM Series Security Threat Response Managers. These products work together to provide the following capabilities:

Multivendor Visibility and Event Correlation

The STRM Series is a security information event management (SIEM) system. The STRM Series gives IT visibility into activity across a multi-vendor network by consolidating, analyzing and correlating log and flow data from a wide range of vendors' security and network devices, desktops and servers. As a result, IT staff can quickly identify a threat, pinpoint its root cause, and take action.

Using correlation rules, IT staff can detect individual as well as sequential events, enabling them to recognize, for example, that a router and firewall are seeing an attack from the same IP address. Rather than having to sort through dozens of logs and alerts to identify a single incident, the network manager sees one consolidated event alert. This expedites troubleshooting and remediation, thus minimizing the impact of an attack. As a collaborative solution, the STRM Series also can identify complex and blended attacks that non-collaborative tools miss. Similarly, the highly advanced correlation system of the STRM Series reduces false positives, enabling IT and security staff to concentrate on actual security incidents – increasing IT's efficiency along with an agency's security.

Dynamic, Adaptive Threat Control

Time is of the essence when a security breach occurs. The more quickly a threat can be contained, the less damage it will do. Juniper has tightly integrated its industry-leading security products with each other and with the STRM Series and Network and Security Manager to create a real-time, adaptive threat response system. The STRM Series correlates event information from all network and security devices and alerts IT about specific events. In addition, the STRM Series can automatically trigger Network and Security Manager to take mitigating actions based on an administrator-defined threat response.

For example, a Juniper Networks SA Series SSL VPN Appliance can cooperate with an IDP Series system to shut down anomalous traffic from a remote user. In a typical scenario, the IDP Series detects a worm and blocks it, then contacts the remote SA Series appliance and informs it that malware was detected, as an example, on flow number 47. The SA Series knows flow 47 belongs to user “Joe” and automatically disconnects him from the network. At the same time, the SA Series appliance displays a screen on Joe’s laptop informing him that malware was detected on his machine and will be quarantined until the problem is fixed. The screen directs Joe to a URL for remediation and indicates that his network privileges will be restored once his laptop is clean. Network and Security Manager also informs the network manager of the actions taken.

Consolidated Security and Compliance Reporting

Federal agencies must comply with numerous security directives and other regulations. Compiling the necessary audit data in a multi-vendor environment can be time consuming and error prone. In addition to providing a single network-wide view for threat identification and mitigation, the STRM Series delivers real-time and historical views of security events as well as comprehensive reporting.

The STRM Series provides accountability information—who did what and when – as well as visibility into the business applications and assets being protected by security controls. As a result, IT can get detailed logging and accounting reports on the activities of users. The STRM Series supports numerous out-of-the-box compliance reports and compliance-focused regulation workflow information, enabling federal agencies to meet reporting and auditing requirements for FISMA, HIPAA, and other regulations.

Consolidated Policy Management

Lack of consistent policy enforcement can create security holes. NSM serves as security management console for all Juniper products within the Adaptive Threat Management Solutions, ensuring that security policy is centrally managed and a single security policy is applied. Centralized policy management boosts protection of critical resources throughout an agency’s information infrastructure and reduces IT’s administrative burden.

Adaptive Threat Management Solutions Benefits

Combining the security event information management of the STRM Series with a tightly integrated, cooperative set of industry leading security platforms, Adaptive Threat Management Solutions deliver the following benefits to federal government agencies:

Interoperates with existing infrastructure – Adaptive Threat Management Solutions interoperate with network and security equipment from multiple vendors so can be deployed easily in existing multi-vendor environments to boost cyber security.

Provides network wide visibility and control – The STRM Series advanced multi-vendor event and log correlation capability enables IT to rapidly identify, mitigate, and report on complex attacks that other solutions miss, thus minimizing the impact an attack has on an agency. By giving IT one consolidated event alert, the STRM Series successfully addresses the task that John Slye, principal analyst at INPUT, describes as “turning tons of data about network and application activity into useful, actionable information.”⁶

Proactively identifies and mitigates new and complex threats – Leveraging sophisticated security incident analysis and auto-remediation capabilities, Adaptive Threat Management Solutions are able to identify and respond in real time to evolving cyber threats. Juniper Networks Adaptive Threat Management Solutions give IT the ability to automate threat management—for example, by enabling automatic device quarantining—which reduces risk exposure as well as IT operations overhead.

Delivers reliable, consistent threat response – With Adaptive Threat Management Solutions, the network can be trusted to respond appropriately to prevent attacks, thus ensuring the integrity, availability, and confidentiality of data.

Simplifies compliance reporting – By consolidating logs and event data network-wide and providing numerous report templates and auditing tools, the STRM Series dramatically simplifies and streamlines the job of documenting compliance with federal directives and regulations.

Reduces operations overhead – Manually correlating security incident data is a time-consuming and error-prone task. Adaptive Threat Management Solutions relieve IT of that burden, reducing complexity. In addition, its highly integrated security capabilities and auto-remediation features address security breaches without constant IT intervention, lowering TCO and freeing IT staff to focus on other pressing tasks.

Increases return on security investment – Adaptive Threat Management Solutions operate within an existing information infrastructure to provide more robust cyber security than other solutions. This enables federal agencies to achieve a higher return on their cyber security investment.

Improves continuity of operations (COOP) – By providing correlated security information instantly and empowering IT to automate threat response, Adaptive Threat Management Solutions ensure that cyber attacks are shut down as quickly as possible, before they can ripple through the network and compromise data, impact performance or trigger downtime.

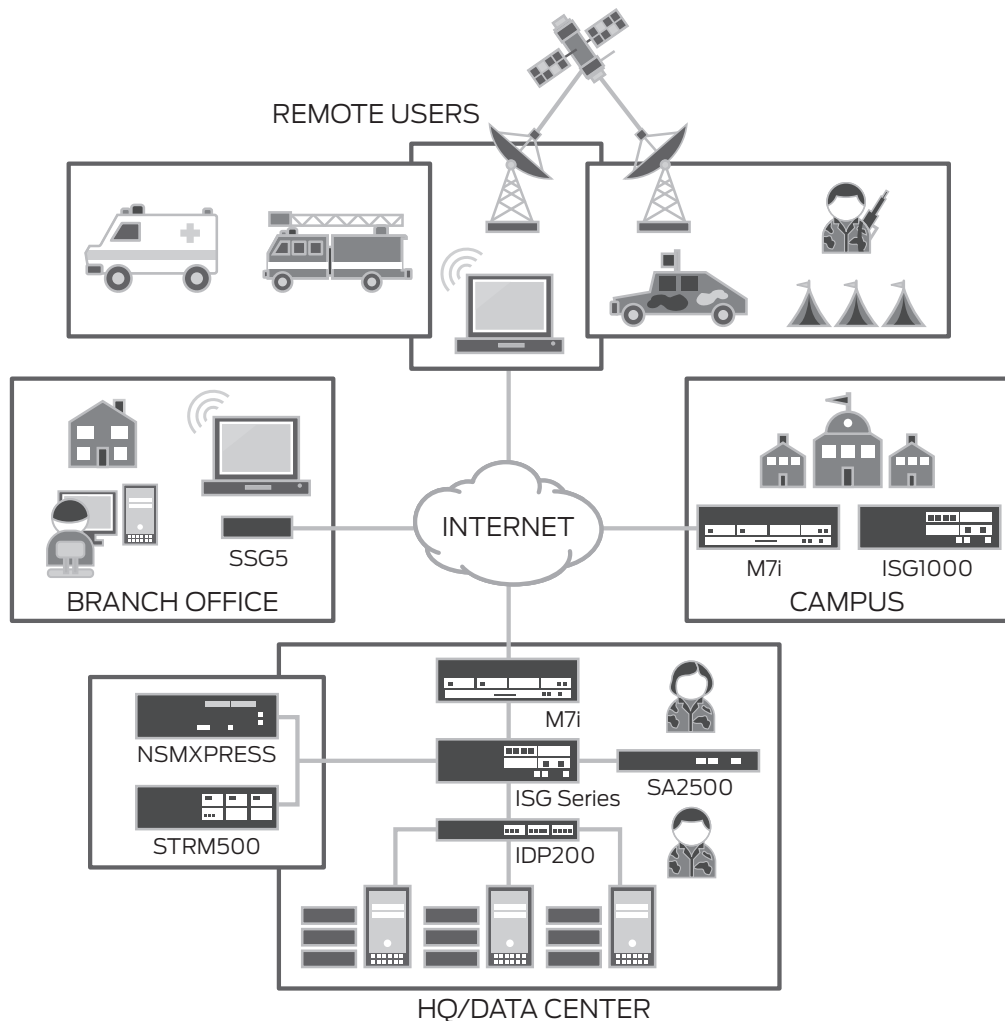


Figure 3: Integrated Adaptive Threat Management Solutions for Government

Conclusion—Meeting the Cyber Security Challenge

Cyberspace is critical to the U.S. Federal Government but is the source of constantly changing security threats. Juniper Networks Adaptive Threat Management Solutions provide the dynamic and coordinated threat response missing from current solutions. With its network-wide visibility and integrated set of market-leading security platforms, Juniper Networks enables defense, intelligence and civilian agencies to counter cyber attacks in real time, limiting their impact on people and assets.

By leveraging existing network infrastructures, Adaptive Threat Management Solutions enable federal agencies to realize a greater return on their security investment, reducing TCO while boosting cyber security, compliance and continuity of operations. An adaptive, proactive solution, Juniper Networks gives organizations the tools they need to operate securely in cyberspace.

Appendix A

CAC—Common Access Card – The CAC is a United States Department of Defense (DoD) smartcard issued as standard identification for active duty military personnel, reserve personnel, civilian employees, and eligible contractor personnel. The CAC is used as a general identification card as well as for authentication to enable access to DoD computers, networks, and certain DoD facilities. The CAC enables encrypting and cryptographically signing email, facilitating the use of public key infrastructure (PKI) authentication tools, and establishes an authoritative process for the use of identity credentials.

FISMA—Federal Information Security Management Act – FISMA was passed by Congress and signed into law by the President as part of the Electronic Government Act of 2002. Its goals include development of a comprehensive framework to protect the government's information, operations and assets. The Act assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) in order to strengthen information system security. In particular, FISMA requires the head of each agency to implement policies and procedures that cost-effectively reduce information technology security risks to an acceptable level. To ensure the adequacy and effectiveness of information security controls, FISMA requires agency program officials, Chief Information Officers and Inspector Generals (IGs), to conduct annual reviews of their agency's information security program and report the results to OMB. OMB uses this data to assist in its oversight responsibilities and to prepare an annual report to Congress on agency compliance with the Act. The report is based primarily on agency and IG reports submitted to OMB in October of every year.

HIPAA—Health Insurance Portability and Accountability Act – HIPAA was enacted by the U.S. Congress in 1996. It protects health insurance coverage for workers and their families when they change or lose their jobs, and requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. HIPAA also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the U.S. health care system.

HSPD-12—Homeland Security Presidential Directive 12 – In August 2004, the President signed Homeland Security Presidential Directive Twelve (HSPD-12). This directive requires that all federal agencies follow a common standard when issuing, utilizing and maintaining physical and logical security access mechanisms. The access mechanisms must be interoperable between agencies. The National Institute of Standards (NIST) was tasked with developing the standard, named FIPS Publication 201. Collectively, implementation of FIPS 201 is referred to as "Personal Identity Verification of Federal Employees and Contractors" or PIV. HSPD-12 defines "secure and reliable forms of identification" as identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process.]⁷

NSPD-51—National Security Presidential Directive 51/HSPD-20 – Homeland Security Presidential Directive 20

– This directive establishes a comprehensive national policy on the continuity of Federal Government structures and operations and a single National Continuity Coordinator responsible for coordinating the development and implementation of Federal continuity policies. This policy establishes “National Essential Functions,” prescribes continuity requirements for all executive departments and agencies, and provides guidance for State, local, territorial, and tribal governments, and private sector organizations in order to ensure a comprehensive and integrated national continuity program that will enhance the credibility of our national security posture and enable a more rapid and effective response to and recovery from a national emergency.

TIC—Trusted Internet Connections Initiative – The TIC program is a component of the Comprehensive National Cyber Security Initiative. The goal of TIC is to decrease the number of connections from federal agencies to external computer networks to 100 or fewer. The idea is that the fewer connections agencies have, the easier it will be to monitor them and detect security incidents.

¹ Source: “The State of Federal Government Information Security, 2007”

² Source: “Security Directives and Compliance” – custom supplement to Federal Computer Week; www.fcw.com/industry_insights/cs_09222008_Index.html

³ Source: Dark Reading : A New Spin on Adaptive Security Gartner’s next-generation security model has its roots in other efforts -- June 5, 2008 By Kelly Jackson Higgins, Senior Editor, www.darkreading.com/document.asp?doc_id=155734]

⁴ Source: INPUT – Top Opportunities in Federal Information Security Market - www.researchandmarkets.com/reports/648992/top_opportunities_in_federal_information

⁵ Source: NextGov – “DHS cites steps to detect increasing network intrusions” www.nextgov.com/nextgov/ng_20080425_8753.php

⁶ Source: Security Magazine – www.securitymagazine.com/CDA/Articles/Breaking_News/BNP_GUID_9-5-2006_A_1000000000000426514

⁷ Source: www.whitehouse.gov/news/releases/2004/08/20040827-8.html

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
Airsides 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.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, 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.

2000297-002-EN Mar 2010

 Printed on recycled paper