WHITE PAPER

DYNAMIC SECURITY FOR THE NEW NETWORK DATA CENTER

Juniper Networks Delivers Comprehensive Security Capabilities to Meet the Needs of Next Generation Data Centers

Table of Contents

Table of Figures

Executive Summary

Starting with consolidation, trends such as virtualization, distributed applications, and a highly mobile workforce have made the data center more vulnerable to security breaches than ever before. IT must combat complex and rapidly evolving internal and external threats, make sense of a flood of logged events, and meet compliance mandates even as applications automatically migrate across virtual servers, and users connect to the data center from virtually anywhere with any type of device.

Research shows that many enterprises have a security architecture that looks much the same as it did 15 years ago. To address today's data center security challenges, enterprises need a network-based security solution that delivers unified, dynamic threat control across both physical and virtual systems. Specifically, enterprises need security solutions that combine high capacity, scalable platforms; application fluency; identity-based access enforcement; and centralized, automated management.

A leader in network security, Juniper Networks® has developed an innovative product portfolio with rich functionality designed to meet the security requirements of today's data center, and tomorrow's as well. With Juniper Networks SRX Series Services Gateways and the real-time provisioning of Juniper Networks SA Series SSL VPN Virtual Appliances, Juniper delivers enforcement that is tremendously scalable and dynamically expandable, enabling even the largest enterprises to control high volumes of traffic and accommodate growing resource usage without compromising security or performance.

Likewise, Juniper's AppSecure suite of applications, support for compound signatures, and virtual firewalling for virtual servers ensure that all application content in the data center is scanned, identified, tracked, and secured. With Juniper's application fluency, enterprises can secure a wide array of applications, including distributed, Web, client/server, and thin-client technologies—even content moving between virtual machines on a single host—and precisely define what actions are allowed.

Identity awareness is key to applying security consistently, regardless of user location or access method. Juniper Networks Junos® Pulse client works in conjunction with SA Series SSL VPN Appliances, Juniper Networks Unified Access Control, and other Juniper platforms to ensure that session data and security policies follow users wherever they go, no matter what type of device they use to connect to the network, whether desktop computer, laptop, netbook, smartphone, or PDA.

In addition, with its new Juniper Networks Junos Space platform, applications and streamlined threat and compliance management, Juniper is providing centralized, automated security management. Juniper's management tools reduce the burden on IT while ensuring consistent policy enforcement and compliance tracking across the enterprise.

With Juniper's dynamic security solutions, enterprises can easily secure their data centers today and well into the future, as they adopt new business models and technologies such as cloud computing.

Introduction

Trends ranging from consolidation and virtualization to distributed applications and user mobility are reshaping the data center, bringing enterprises significant benefits, but also creating new security vulnerabilities. Consolidating servers and other resources in data centers helps organizations boost efficiency, maximize resources, and reduce costs. At the same time, technologies such as server virtualization and distributed applications have enabled enterprises to increase business agility while also cutting CapEx and OpEx. Mobile workers extend an enterprise's geographic reach and allow for 24x7 operations.

But these trends create a range of security challenges. Consolidation results in high volumes of traffic to and from the data center, which can strain the security infrastructure so crucial to protecting enterprise assets, operations, and reputation. Virtualization results in a lack of visibility into and control over traffic passing between virtual machines (VMs) on the same server. As a result, malicious traffic can propagate unchecked between VMs and potentially onto the physical data center network. Similarly, by creating highly distributed communication patterns with multiple flows per transaction, distributed applications pose a variety of security risks as well as making it difficult to enforce access entitlements and data privacy.

Mobile workers need anytime, anywhere access to a broad array of applications, further taxing the data center security infrastructure. The ever expanding matrix of users, devices, locations, and applications makes it difficult for IT staff to ensure that access controls and other security mechanisms are applied consistently to the same user at all times. IT is also struggling to combat evolving internal and external threats, make sense of a flood of logged events, and meet compliance mandates.

To date, security in data centers has been applied primarily at the perimeter using firewalls, and at the server level by installing host-based intrusion detection, identity enforcement, antivirus, and other software agents. With virtualization, applications on the same host can communicate without accessing the physical network, thereby circumventing traditional firewalls and breaking zones of trust. Server-based security isn't scalable, doesn't encompass the range of network-attached devices in the data center, and presents major operational challenges. To protect today's data center, enterprises need a unified security layer operating dynamically across the heterogeneous and ever changing data center infrastructure.

The network is ideally suited to provide visibility into the application traffic it carries and to act as an insertion point for policy enforcement devices. As a market leader in network security, Juniper Networks understands what's required to secure the data center environment. Juniper's comprehensive product portfolio combines high capacity and scalable platforms; application fluency; identity-based access enforcement; and centralized, automated management to deliver unified threat control across both physical and virtual systems. With Juniper's dynamic security solutions, enterprises can easily secure their data centers today and well into the future, as they adopt new business models and technologies such as cloud computing to fuel competitive advantage and their future success.

Requirements for Securing the Data Center

The data center is undergoing a dramatic transformation. As Nemertes Research has noted, workloads in today's data center move dynamically and start and stop based on real-time performance needs. Unfortunately, in many enterprises, the security architecture looks much the same as it did 15 years ago[1].

To keep pace with these changes, enterprises need new security and compliance controls that span physical and virtual environments and dynamically enforce policy regardless of application type or user location. In evaluating next-generation security solutions, enterprises should look for the following capabilities:

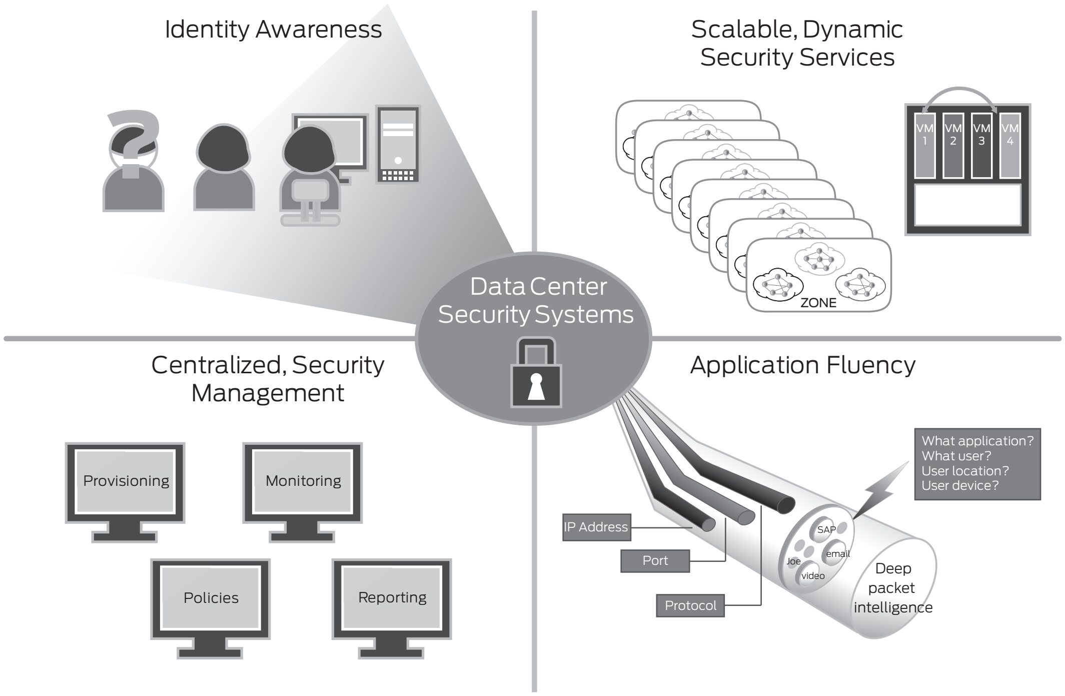

Figure 1: Security Systems for Data Center Networks

Scalable, Dynamic Security Enforcement: The data center is anything but static. The mix of applications in use changes over time, applications and VMs migrate from one server to another as application requirements change, and server and storage resources fluctuate. At the same time, the threat landscape is constantly shifting. Traditionally, enterprises added more devices when they needed more security, performance, and bandwidth as the data center grew. However, these approaches to scaling have created complexity and higher maintenance costs for IT.

[1] Source: Ritter, Ted. Nemertes Research. "Securing the Physical, Virtual, Cloud Continuum," 2009.

To keep up with the demands of today's data center, enterprises need next-generation security solutions with the following capabilities:

- Can easily scale in terms of overall capacities and throughput performance
- Can scale dynamically to accommodate shifting application and resource usage without disrupting network operations or requiring a network redesign
- Support rapid session setup and teardown for very large numbers of sessions
- Inspect and control high volumes of traffic crossing between different domains
- Eliminate the trade-off between security and performance

Application Fluency: Enterprises use a broad range of applications built around a variety of architectures. These include newer distributed application architectures such as service-oriented architecture (SOA) and mashups, as well as legacy client/server applications. At the same time, security threats have become more subtle. For example, attackers exploit the application logic itself in order to intercept data. And new application-level denial-of-service (DoS) attacks exploit legitimate application processes to disable applications by causing them to repeat one action over and over.

Properly securing all of these applications presents a major challenge. It is no longer sufficient to define or enforce security policies based on the TCP/IP "five tuple" (source and destination IP address, source and destination port, and protocol). With so many applications running over port 80, for example, it is impossible to distinguish between Salesforce.com traffic and BitTorrent. Enterprises need application fluent security solutions that:

- Support the spectrum of applications in use and easily adapt as the application mix shifts
- Can accurately identify common business and collaboration applications, nested applications and application instances, transactions, and actions based on internal characteristics such as protocol attributes
- Are intelligent enough to identify application context and conversations
- Allow IT to precisely define what actions are allowed within certain application instances
- Provide visibility into and tracking of application-level information, including application usage profiles

Identity Awareness: Today's highly mobile workforce connects to the data center from virtually anywhere in the world using a variety of connection methods via devices ranging from laptops, netbooks, and tablets, to smartphones and PDAs. At the same time, securing distributed applications requires the ability to correlate all of the flows and narrow them down to one user performing one transaction. Consequently, it is crucial to identify who is on the network, not just a user's IP address, and to tie security policies to user identity. Identity-based security is also necessary for location independence. Enterprises need identity-aware security solutions that:

- Allow IT to define policies based on user identity, role, location, and application
- Ensure that security policies follow users wherever they go
- Integrate with existing identity stores such as Active Directory or LDAP servers, or both
- Enable automated, coordinated threat management based on identity information
- Support standards such as the Interface for Metadata Access Point (IF-MAP) from the Trusted Network Connect (TNC) for sharing identity and privilege information across systems
- Report on unauthorized access attempts and violations for compliance, auditing, and record keeping purposes, tying them to specific users
- Provide common management for identity-based policies across security platforms

Centralized, Automated Management: Managing security is a significant challenge. IT must configure security policies on numerous platforms, both physical and virtual, sift through a flood of logged events to determine which require attention, and compile data to demonstrate compliance with government and industry-specific mandates. Today, staff must monitor multiple individual management consoles and create and maintain policy scripts for each different security platform—a manual and error prone process that makes it very difficult to apply policy consistently across the enterprise. Likewise, each security system typically generates its own logs, creating silos of event data. In addition, many solutions handle traffic flows and security events separately, and all of this makes it virtually impossible to spot network-wide threats and anomalies.

Given the complexity of today's data centers and the rapid evolution of threats, enterprises need security management solutions with the following capabilities:

- Automate security device and service provisioning
- Abstract and centralize policy definition
- Provide policy life cycle management
- Deliver a unified solution for managing traffic flow and security events
- Provide a single management interface for both physical and virtual systems
- Correlate data from diverse sources on the network
- Support multivendor security environments
- Simplify compliance reporting

Juniper's Data Center Solution

Juniper Networks continues to drive leadership in the network security market, investing in research and innovating to create a comprehensive product portfolio with rich functionality. In addition, Juniper is continually expanding its partnerships as well as making strategic financial investments in companies such as Altor. Juniper is also committed to supporting standards and delivering open platforms that enable customers to expand the capabilities of Juniper solutions without sacrificing ease of use or manageability.

As a result of these commitments, Juniper has the broadest set of security platforms available in the industry, and is uniquely positioned to deliver dynamic solutions that address the requirements of the data center environment.

Scalable, Dynamic Enforcement

To address the dynamic nature of today's data centers, Juniper has architected its data center security solutions to be highly scalable and dynamically expandable.

The Dynamic Services Architecture

Juniper's Dynamic Services Architecture (DSA) gives the Juniper Networks SRX Series Services Gateways a level of scalability and configurability that is unmatched in the industry, making them the ideal platform for today's data centers. Juniper's DSA uses a parallel computing model that simultaneously scales security and networking capabilities with performance. The key pieces of the DSA are the Switch Fabric Board (SFB) and Switch Control Board (SCB), and the Services Processing Card (SPC), which work together to produce phenomenal scalability. The SFB and SCB transform the chassis from a simple blade enclosure into a highly effective mesh network, allowing all blades in the chassis to send traffic at extremely high bandwidth.

The SPC functions as the brain for the SRX Series chassis. Multiple SPCs can be deployed to increase performance and capacity with no change to the system configuration. All SPCs in the system run the same services—such as firewall, VPN, intrusion prevention system (IPS), routing, quality of service (QoS), and Network Address Translation (NAT)—and have the same configuration, so there is no need for administrators to configure individual blades to perform specific tasks.

In addition, the DSA has a session distribution design that supports automatic load balancing of sessions across the shared pool of SPCs. There is no specific mapping from one I/O card (IOC) to one SPC; rather, each flow is mapped dynamically upon session creation. As a result, this revolutionary architecture ensures that SRX Series resources are fully optimized while administrative overhead is minimized.

Expandable Capacity and Performance

Security should never be a bottleneck in the data center. Already 10 Gbps is becoming the standard for connectivity within the data center; going forward, 40 Gbps and 100 Gbps links will be more popular within and between data centers. With its high-performance architecture, the SRX Series Services Gateways can grow with the requirements of the new data center, eliminating the need for forklift upgrades and preserving customer investment.

Real-Time Provisioning of SSL VPN Virtual Appliances

Today's mobile workforce is large and growing. Accommodating these users and their array of devices is a challenge for data center administrators. Through its SA Series SSL VPN Appliances, Juniper gives organizations the ability to increase the number of remote users they can support in real time. With this solution, enterprises use virtual appliance technology in lieu of traditional SSL VPN hardware and run the SA Series SSL VPN software as a service, either on a single large-scale server or distributed among multiple servers. In this way, organizations can scale remote access support rapidly and very cost effectively simply by turning on licensing options and adding more blades to servers as they are needed.

Application Fluency

Juniper understands that simple port-based security is no longer adequate. Malware attacks are getting more sophisticated, blending social engineering techniques with content-borne threat vectors. Understanding these threats requires technologies that diligently scan all content and identify the associated applications. Juniper delivers application fluency through the following products and capabilities.

Application Visibility and Control

Juniper's AppSecure suite of applications protects against application-oriented attacks by giving Juniper Networks SRX3000 line and SRX5000 line of gateways the ability to identify, defend, and track application traffic. By adding these sophisticated capabilities to its SRX Series platforms, Juniper ensures that enterprises have the tools they need to secure very high traffic loads in the data center.

AppID uses a combination of protocol decoding, application signature matching, and anomaly detection to identify hundreds of the most commonly used business and collaboration applications. Previously available only on the standalone Juniper Networks IDP Series Intrusion Detection and Prevention Appliances, AppID identifies both the context and characteristics of the traffic and makes that information available to the SRX Series for processing. Data center administrators can use this application information to better tune their security posture.

With the application identity information from AppID, AppDoS performs behavioral and heuristic analysis on application traffic to identify bots and other malware. Specifically, AppDoS monitors session activity to see if it varies from established norms or thresholds; for example, by performing the same task repeatedly. AppDoS can determine if client traffic is coming from an approved user or an automated botnet and trigger appropriate action, such as blocking that session, quarantining the client, or both.

AppTrack adds the application identification and visibility information from AppID to the IPS session log, providing a detailed log of actual network traffic patterns and applications. With this historical information, data center administrators can better manage their security risks. AppTrack records a range of application usage information that includes bandwidth consumption and the volume of traffic within and between zones, which administrators can use to establish appropriate bandwidth and QoS policies for applications to ensure application availability.

Secure, Single Access to Diverse Applications, VDI

Data center administrators must support a wide array of application types, including distributed, Web, client/server, legacy, and thin-client technologies such as virtual desktop infrastructure (VDI). It is not feasible to maintain a separate security infrastructure per protected application. However, using Juniper technologies such as SA Series SSL VPN Appliances, Juniper Networks IC Series Unified Access Control Appliances, and Junos Pulse, administrators can streamline application access control by allowing the different enforcement systems to connect with identity stores and enforce policy on the full spectrum of enterprise applications. SA Series appliances interoperate with leading VDI products, including VMware's View Manager and Citrix's XenDesktop, giving enterprises vendor choice and deployment flexibility.

Compound Signatures Support

Juniper's Compound Signatures technology leverages information about the context of network traffic to make complex determinations of what represents truly malicious intent. Nine different mechanisms are combined in Compound Signatures, including protocol anomaly detection and stateful signatures. In addition, administrators have the ability to chain together events and look for multiple anomalies and attack patterns, either sequentially or in parallel.

Previously available on the standalone IDP Series, Juniper has added Compound Signatures support to the SRX Series platform to provide the largest data centers with complex attack detection capabilities. Security operations on the SRX Series are handled very efficiently in Juniper Networks Junos operating system, which ensures that each packet is opened and a set of services, including AppID, firewalling, and IPS services such as Compound Signatures, are applied once, rather than having each service individually opening each packet.

Virtual Server Support

Server virtualization often creates blind spots for inter-VM traffic that traditional network-based security devices can't cover effectively. Virtual firewalls are key to securing VM environments and the distributed applications that run across them. Juniper has partnered with Altor to integrate its virtual firewall (VF) with Juniper's security products to deliver a comprehensive data center security solution that is vendor agnostic, eliminates blind spots from the network, and allows administrators to apply the same policy across both physical and virtual environments.

Combining a stateful virtual firewall with a virtual intrusion detection service (IDS), Altor's VF complements physical infrastructure security by providing visibility and control over VM traffic, enforcing policies at the VM level, securing live migration, and preventing inter-VM malware propagation. A hypervisor-neutral solution, Altor's VF inspects all traffic to and from each VM and enforces policies at the global, group, and per-VM level, ensuring isolation between and within trust levels, and allowing for precise micro-segmentation. In addition, the Altor VF supports compliance reporting by tracking all access attempts into VM-based applications and collecting historical application usage data.

Identity Awareness

Juniper has infused identity awareness across much of its product line. As a result, enterprises benefit from the following capabilities.

Consistent Client Access with Junos Pulse

Data center administrators must support a wide array of user access methods and devices. Applying a consistent set of network access controls, security policies, encryption, and other security mechanisms across a variety of clients and devices is a major challenge that can strain data center staff. To address this challenge, Juniper has developed Junos Pulse, a location-aware, identity-enabled client that allows administrators to apply granular security policy consistently across all users, anytime, from anywhere, regardless of access method or device.

Combining remote access, application acceleration, and network access control (NAC) in a single unified client, Junos Pulse eliminates the expense and overhead of deploying, configuring, and maintaining separate clients for each function, user device, and access method. Junos Pulse works in conjunction with Junos Pulse platforms such as the SA Series SSL VPN Appliances and Juniper Networks WXC Series Application Acceleration Platforms to support remote users, and with UAC to support LAN-attached users. In addition, Junos Pulse supports industry standards such as the TNC specifications, including IF-MAP to ensure multivendor NAC support.

Junos Pulse leverages existing authentication stores and methods—including multifactor authentication—along with the identity awareness of Juniper platforms to obtain and apply policies based on a user's identity and role within the organization. Junos Pulse can also determine whether the user's endpoint device is corporate owned; measures the health of the endpoint device both pre- and post-authentication; and, if necessary, quarantines and remediates unhealthy or offending endpoints.

Junos Pulse gives users a simple, intuitive, consistent experience and allows them to seamlessly migrate from one access method to another. Data center staff are able to provision secure, accelerated, anytime/anywhere network and application access using a single client, ensuring that security policies are applied consistently across physical and virtual environments regardless of a user's location or access method. Using the Junos Pulse client, administrators can grant users one of three levels of access from mobile devices: core, which encompasses Web access or Web intranet access; client/server access; or a Layer 3 connection for full access to applications and resources.

Define Policies by Role

Juniper security platforms share identity entitlement information with each other, which makes it possible for administrators to define a set of role-based policies that are enforced regardless of a user's location, access method, or device. For example, when used in conjunction with UAC, Juniper firewalls become identity aware and can be deployed as policy enforcers, giving enterprises greater choice and flexibility as to where to deploy enforcement points.

Likewise, because IDP Series capabilities are integrated into SRX Series Services Gateways, the SRX Series can monitor anomalous behaviors, malicious traffic, and the use of noncompliant applications on a per user basis. The SA Series SSL VPN or UAC gateways can also instruct devices acting as enforcement points to drop, quarantine, or remediate users and their sessions if they are deemed out of policy or are acting in an anomalous fashion.

Juniper management tools make it easy to implement identity- and role-based policies. With Junos Space Security Design, for example, IT can provision identity-based policies across the entire network. Junos Space Security Design uses an innovative approach that abstracts the network security policy and then applies it to a group—effectively protecting an entire security domain. Security Design has an easy to use wizard-driven interface, granular configuration options, and predefined profiles for rapidly deploying devices and security services. Using Security Design, data center staff can easily provision complex identity-based policies across the entire network, greatly improving operational scale and efficiency and enhancing overall policy consistency and security due to minimal operator error.

In addition, the Juniper Networks STRM Series Security Threat Response Managers provide intelligent correlation between all security and network information from Juniper firewalls, SA Series appliances, UAC, the IDP Series, networking products, and other vendor products—along with other corporate systems such as servers and applications. This enables security operators to quickly and accurately identify the source of anomalous behavior and take proactive action.

Securely Share Policy with IF-MAP

In addition to sharing identity information, Juniper platforms share user session and policy information using the Interface for Metadata Access Point protocol (IF-MAP), a standard from the Trusted Network Connect, which is a workgroupof the Trusted Computing Group (TCG). As a result, user session data and policies follow users wherever they go, ensuring that they are applied consistently across the organization and around the globe. A user connected to the LAN at headquarters who logs into an HQ-based data center application via a desktop computer will have seamless access rights, without re-authenticating, to remote data centers. The same mechanism is applied when the user travels overseas to a remote office and accesses the same application via an SA Series SSL VPN appliance using a smartphone.

Juniper supports IF-MAP on the SA Series SSL VPN Appliances and IC Series UAC Appliances. In addition, because IF-MAP is a standard, Juniper devices can share policy information with, or leverage information from, third-party platforms that support the IF-MAP standard, enabling more comprehensive, identity-enabled integrated data center security and control.

Centralized, Automated Security Management

Juniper offers a suite of intuitive, multivendor security management solutions that ease the operations burden on IT, while ensuring consistent policy enforcement and compliance tracking across the enterprise. Juniper more than meets enterprise requirements for centralized, automated security management with the following products and capabilities.

Automated, Single Pane Management

The Junos Space network application platform provides an open, programmable platform for developing and deploying network infrastructure automation applications.

The Junos Space application portfolio includes innovative network security automation solutions that help maximize security through sophisticated policy abstraction and optimization technology; improve operational efficiencies through prebuilt configuration templates, workflow automation, and Juniper best practices; and control compliance costs through out-of-box templates and reports. With Junos Space, enterprises can improve their organization's security posture, lower security risk, and scale their security services cost effectively.

Juniper has announced several Junos Space applications, including:

Junos Space Security Design, which gives administrators the ability to rapidly provision thousands of devices and security services such as firewalls, IDPs, and VPNs with minimal human intervention; intuitively define and apply common policies across diverse devices and services; and create domains of protected resources such as networks, users, IP addresses, servers, even files, applying policies to those domains. All entities and sub-domains within a domain automatically inherit the security policies and other properties of the domain, eliminating the need for administrators to configure policy controls individually for each entity.

Junos Space Virtual Control, which delivers common management across both virtual and physical connections. Virtual Control provides end-to-end topology, inventory, and visualization capabilities across physical and virtual connections; orchestrates configuration, events, and failures between both environments; and lets network operators define network policies and parameters that server administrators can associate with VMs on the fly. By enabling network administrators to configure physical and virtual devices from the same screen, Virtual Control simplifies virtual server, VLAN, and virtual I/O management, reducing the number of devices that must be managed and overall OpEx, while providing operating consistency and visibility throughout the network.

Junos Space Security Insight, which abstracts, aggregates, and correlates network and security intelligence such as network inventory, configuration, traffic and log information, as well as security events, and presents it as services, enabling enterprises and service providers to have network-wide visibility and control of all network elements. By leveraging Security Insight, enterprises can maximize their security posture, proactively address increasingly sophisticated threats, and rapidly scale their security infrastructure in response to business dynamics.

Security Insight includes flow analysis that intelligently correlates traffic flows and security events for proactive threat detection and mitigation; security risk analysis to enable predictive threat modeling and simulation; automated compliance and policy verification; heterogeneous network configuration monitoring and auditing; and advanced threat visualization and impact analysis. Junos Space Security Insight correlates real-time network flow information and real-time log-based events to create a snapshot of the data center security state, giving enterprises a precise view of their security exposure at all times.

Streamlined Threat and Compliance Management

The STRM Series integrates best-in-class security information and event management (SIEM), network behavior analysis, and log management in a single console. With STRM Series, enterprises get a unified view of what are otherwise silos of network and security data. By centralizing management of network and security events, network and application flow data, vulnerability data, and identity information, STRM Series significantly reduces false positives and helps enterprises detect complex threats and aberrant activities that other systems miss.

An open platform, STRM Series integrates data and log management from a broad array of third-party networking and security equipment, operating systems, applications, and security map utilities. The STRM Series provides long-term collection, archiving, search, and reporting of event logs, flow logs, and application data. In addition, the distributed architecture of the STRM Series scales to provide event and flow log management in any size enterprise network.

Juniper has created more than 1,500 out-of-the-box report templates, including events and time-series reports, vendor-specific reports, and compliance reporting packages for Payment Card Industry (PCI), Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), and Gramm-Leach-Bliley Act (GLBA). By streamlining compliance reporting, the STRM Series helps enterprises more accurately and cost-effectively comply with government and industry mandates.

Conclusion—Securing the Data Center with Juniper

Juniper Networks is in a unique position to help enterprises secure today's dynamic data center. With its comprehensive approach to security, history of innovation, robust and scalable product line, and support for open, expandable systems, Juniper can deliver security solutions that address the requirements of even the largest organizations.

With Juniper security solutions, enterprises can minimize threats across both physical and virtual environments, improve their security posture, gain greater insight and visibility into their network and its users, and better meet compliance mandates. In addition, Juniper's focus on centralizing and automating security and network management helps enterprises rapidly deploy new services while driving down costs. And Juniper's ability to embed new technologies in its open platforms ensures that the company can continue to meet enterprise data center security needs as they evolve.

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.

2000351-001-EN May 2010

Printed on recycled paper