

JUNIPER NETWORKS ADAPTIVE THREAT MANAGEMENT SOLUTIONS

High-Performance Security Products That Work Together Across Your Distributed Enterprise

Challenge

Today's point security and networking products have formed a patchwork of devices resulting in ineffective and costly security. This problem has grown as the enterprise has become distributed where high performance is key and every location, user, and application poses a threat.

Solution

Juniper Networks Adaptive Threat Management Solutions provides best-in-class security products that cooperate to proactively prevent attacks that evade security point products while accelerating applications. They enable the network to dynamically adapt to risks and always with a full audit trail.

Benefits

- Security that identifies, mitigates, and reports on even the most sophisticated attacks Reduce cost of ownership
- Network-wide identity and application-aware security Dynamically provision security
- Flawless application delivery
- Real-time incident response
- Security and performance without tradeoff
- Network-wide, real-time visibility and control

Today's enterprise is at the center of a number of conflicting trends as exemplified by the changes in the network. Data centers are consolidating while enterprises are scaling beyond headquarters to regional, branch, and remote locations—and often the network functions as the primary connection between them. In order to be competitive, therefore, today's enterprise network must be open for business wherever business is done. Unfortunately, these highly pervasive networks can also open the network—and the enterprise itself—to threats that are motivated by everything from mischief to profit. Growing Internet use and user mobility mean that today's killer worm or virus is as likely to be inadvertently brought in by a telecommuter as planted by a hacker. Small remote offices are as vulnerable to threats as well-protected headquarters offices but usually do not have the same IT staff or budget to secure them. Individual users, many of whom access the network via unmanaged devices, often do not proactively manage their own security defenses on the daily basis that is required to ensure that the network as a whole remains safe.

Another factor of a distributed enterprise network is the ability to deliver a LAN-like experience, regardless of how far away from the headquarters LAN the users may physically be. Increasing numbers of business-critical online applications can strain the network, particularly in the case of remote users or branch offices. Poor performance or unplanned lapses that can result from security incidents, network-wide upgrades, changes to security policy, or even natural disasters, can directly and substantially impact bottom-line business.

Network and security managers are in the eye of the storm. The only way to identify, mitigate, and report on threats is with a cooperative security system that can provide real-time protection while correlating information about events occurring throughout the distributed enterprise. The system will also need to be able to sift actionable data from the deluge of log reports that are generated from regular business operation. Finally, a true distributed enterprise security solution would be able to proactively provide granular user-level protections and security without impacting speed and performance.

Juniper Networks® Adaptive Threat Management Solutions deliver a consistent and comprehensive approach to security while providing you with the freedom to deploy a best-in-class approach that is right for every user and location in your business. The products can be added incrementally, so there are no forklift upgrades required. With Juniper, you move from reactive to proactive, by deploying security that will protect your environment both today and tomorrow while allowing you to focus on securely growing your business.

The Challenge

As the enterprise has grown, so have the requirements for high performance regardless of user location. As enterprises have become increasingly reliant on the network, infrastructure has grown into a patchwork of point products, each of which solves a specialized problem. For example, a company may have added intrusion prevention to comply with legislation, firewalls to protect the data center, application acceleration to speed performance, SSL VPN to provide remote access without a client, application acceleration to speed performance, smaller firewalls to protect the branch—and may be considering overall LAN access control. Each product likely does its job well. Unfortunately, blended threats are designed to take advantage of the gaps between point products, which are typically not designed to communicate with each other. For example, an intrusion prevention system (IPS) may detect an application anomaly as a firewall logs reconnaissance activity and the access control devices capture a series of login attempts in the campus or across the VPN. While each product may be doing its individual job, if the products do not communicate and coordinate with each other it is easy to miss more complex attacks. By the time such a breach is detected, if at all, the damage is already done. As the enterprise becomes distributed, these issues are compounded. And because remote users and branch offices may not have dedicated IT staff, they may not be as well defended to begin with.

Network managers face the additional challenge of consolidating the information coming from a multitude of security devices into the reports that are required for internal, audit, or regulatory review. Because information must be correlated from device to device, the job of getting a network-wide view is both time consuming and subject to human error. Once this mass of data is compiled, it still must be sifted through to separate meaningful data from background noise. This challenge grows exponentially when one tries to identify the root cause of an attack, where reports and logs need to be looked at from multiple systems and several hundred devices, spread over many branch locations. Reactive forensic analysis becomes inconsistent and error prone, preventing businesses from taking a proactive view of their network as a whole. The result is that attacks are often discovered long after the damage has already been done.

Finally, scaling such a network to handle more users, new applications, or enhanced security further contributes to greater costs and complexities. The learning curve is steep, since each product has its own OS, management tools, and trouble-shooting techniques. The cycle is often repeated with the addition of each new product, since most point products are not created with incremental additions in mind. Total cost of ownership (TCO), therefore, must not only include the expense of the equipment itself, but also the less obvious disturbance to business required to deploy, test, troubleshoot, and manage new installations.

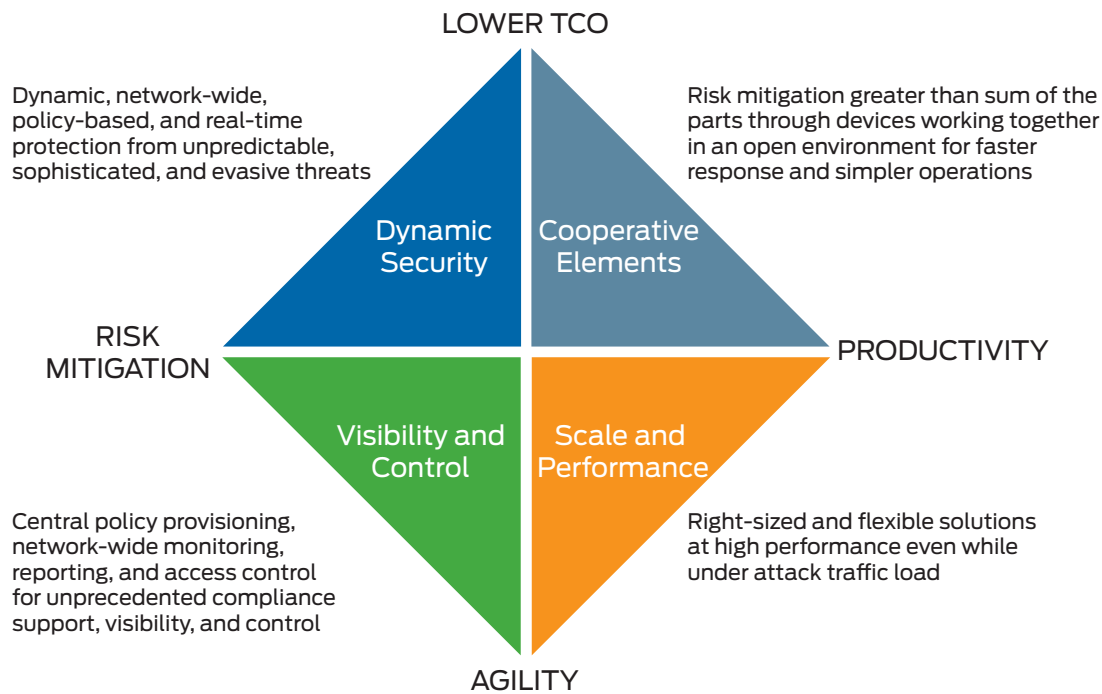


Figure 1: Juniper Networks Adaptive Threat Management Solutions remove legacy compromises around TCO, agility, risk mitigation, compliance, and productivity.

The Juniper Networks Adaptive Threat Management Solutions

Juniper Networks offers enterprises and service providers the industry's only high-performance adaptive threat management solution that leverages a dynamic, cooperative product portfolio. This solution provides both protection and performance enhancements, combined with network-wide visibility and control. The result is a suite of products designed to increase security and reduce the TCO associated with accelerating service and application delivery throughout the distributed enterprise.

Each of the Juniper products contributing to the Juniper Networks Adaptive Threat Management Solutions is best in class in its own right. But because the products are from Juniper, they offer something that other products don't—the ability to work together. The tight integration between devices enables Juniper Networks Adaptive Threat Management Solutions to provide value beyond the sum of its parts. These solutions empower the network itself to change based on parameters you set as variables within the network, user environment, application type, and threat landscape change. All policy creation and device configuration in the solution can be managed using a single platform—Juniper Networks Network and Security Manager. With only a single provisioning solution to learn, operating costs drop significantly, policy and configuration changes are faster, and there are fewer human errors. Juniper Networks STRM Series Security Threat Response Managers can take data from all of your network and security devices, regardless of vendor, to provide an “aerial” view of your network that gives you the perspective you need to be proactive. The STRM Series also comes prepackaged with over 1,300 different reports—and greatly simplifies generating the network security, trending, and compliance reports that you need.

Juniper Networks Adaptive Threat Management Solutions can be deployed incrementally, because each piece of the solution adds more value to the whole, regardless of the order in which devices are implemented. Because Juniper builds its products to industry standards, devices interoperate each other as well as other standards-based products, offering greater choice and flexibility than proprietary solutions that are designed to lock you in to a specific vendor. Together, Juniper solutions provide the product-specific security and application acceleration—as well as the network-wide visibility, mitigation, control and reporting—needed to adapt and protect the network against constantly evolving threats.

Key characteristics of this solution include:

- A highly integrated and collaborative security solution that proactively identifies, mitigates, and reports on security and compliance threats
- Application acceleration that ensures secure delivery of business-critical services
- Comprehensive and consistent solutions approach across all enterprise locations
- Application performance and security without trade-offs
- Identity- and application-aware services
- Full IPS capabilities throughout the network
- Consistent and granular policy-based access control regardless of the user location
- Centralized visibility and control reduces management complexity, false positive alarms, and overall costs
- Automatic and self-remediation options for noncompliant users and devices significantly increases user productivity, as well as overall network security
- Automation of mundane threat mitigation and reporting activities frees up IT staff

Reduce TCO While You Increase Agility

Juniper Networks Adaptive Threat Management Solutions feature unparalleled application acceleration, security, and compliance combined with a low TCO. This is achieved by reducing both obvious CapEx and OpEx.

Lower CapEx

Getting started with Juniper Networks Adaptive Threat Management Solutions can be done with minimal capital outlay, because Juniper products are designed to work together. Each product you buy can work with the ones you already have, for a solution that gives you more than the sum of its parts. Juniper offers a comprehensive solution that consistently scales from the smallest branch offices to the largest data center, so there is always a high-performance product at the right cost to meet your requirements. Solutions designed for branch/remote offices feature integrated functionality such as switching, routing, firewall, VPN, and full IPS capabilities. Consistency and simplicity are maintained with the products that are designed for the campus or data center. All elements of the solution are built on a pay-as-you-grow model that allows you to incrementally add network protection and application acceleration while maintaining compliance as your requirements and business evolve.

Lower OpEx

Provisioning any of the products within Juniper Networks Adaptive Threat Management Solutions is accomplished with Network and Security Manager. NSM supports routing, switching, and security products by default, so per-device applications don't need to be purchased and planned for. This means that you can simply grow device licenses as your network grows. The result is that ongoing maintenance costs begin to evaporate, learning is accelerated, and IT coverage is simplified, since administrators can easily manage different products using the tool with which they are already familiar. With Juniper Networks Adaptive Threat Management Solutions, NSM administrators can create policy across a network from a single console. For example, new access policies are pushed to both Juniper Networks Unified Access Control and SA Series SSL VPN Appliances for consistent policy and network entitlements no matter where the user is located. UAC enforcement on firewalls and Juniper Networks EX Series Ethernet Switches are also defined within NSM.

Network-wide monitoring, correlation from multiple feeds, and reporting from a single STRM Series console means that all device logs are correlated and consolidated—enabling identification, mitigation, and reporting of complex and blended attacks. No longer do you have to wait for a third party such as a credit agency, law enforcement agency, or the press to let you know about lost intellectual property, as you can proactively detect user misbehavior. Not only does the STRM Series allow you to be proactive, it also eases compliance reporting by including over 1,300 predefined and easy-to-customize reports. Like the other products in the solution, the STRM Series can be scaled up as you grow. All supported devices and reports are always included, so there are no management costs and complexity surprises as your network is required to support new demands and devices.

Increase Business Agility

The requirements of today's network—as well as what threatens it—change all the time. New opportunities demand new locations, audiences, and applications to be added to the network—which open new threat vectors. These new offerings also create new compliance headaches. The investments you make in your network today must enhance the business's agility in the face of such a dynamic business climate. Juniper Networks Adaptive Threat Management Solutions are designed to simplify fluid changes in scale, application delivery, threat response, and compliance. Juniper Networks IDP Series Intrusion Detection and Prevention Appliances functionality available via standalone or integrated devices across the entire enterprise enables “early warning beacons” and response to threats in real time. New applications—or access to them from remote locations—are accelerated with the Juniper Networks WX Client, included with the SA Series or UAC client. And the STRM Series features a breadth of reports to make new compliance requirements easier to meet.

Mitigate Risk and Raise Productivity

Secure Access by Organizational Roles and Responsibilities, Independent of Location

As access to an asset goes up, so does the risk. As the network and its applications have become mission critical, the risk associated with access to the network has also increased. Resources used to be protected by the network perimeter, much as a castle would be protected by a moat, and it was assumed that anyone who could get past that perimeter had a right to access the data and applications within. As the user community has become more varied and increasingly mobile, the conventional view of the network perimeter has dissolved. Users no longer know or care where an asset is housed and they require seamless access to key resources from anywhere in order to do their jobs. While this approach increases productivity, it also poses incredible risk for secure and assured application delivery. In today's enterprise, an attack could come from inside the LAN—from a branch office or from a remote location. A breach could originate from an unknowing employee, a guest, or a business partner.

This new paradigm is not supported with typical, location-specific security point products. Protection cannot be device-specific—a consistent security posture must be adopted and enforced throughout the network in order to be effective. Threats must be recognized and prevented from wherever they are detected, and the rest of the network must be alerted to prevent attack spread or data loss data. While this appears to be obvious, the fact is that based on a 2009 Verizon report, the average organization remains vulnerable for 104 days. In the 2008 Computer Security Institute (CSI) report, 49 percent of the responding companies had experienced a virus event. And attacks cost money—computer security incidents involving financial fraud had an average reported cost of close to \$550,000, while “bot” computers within the network are reported to cost an average of \$350,000 per respondent. Common sense shows that risk mitigation must be holistic, and strictures such as Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes-Oxley Act (SOX)—which require that access to regulated data be confined to certain departments and individuals—demand such protections. Unfortunately, the fact remains that most network managers are so overloaded with simply keeping the network running, that it is difficult to see how to add overarching security protection, application delivery, and access control that can be tailored to the user group or individual user—even given the compelling financial and security benefits.

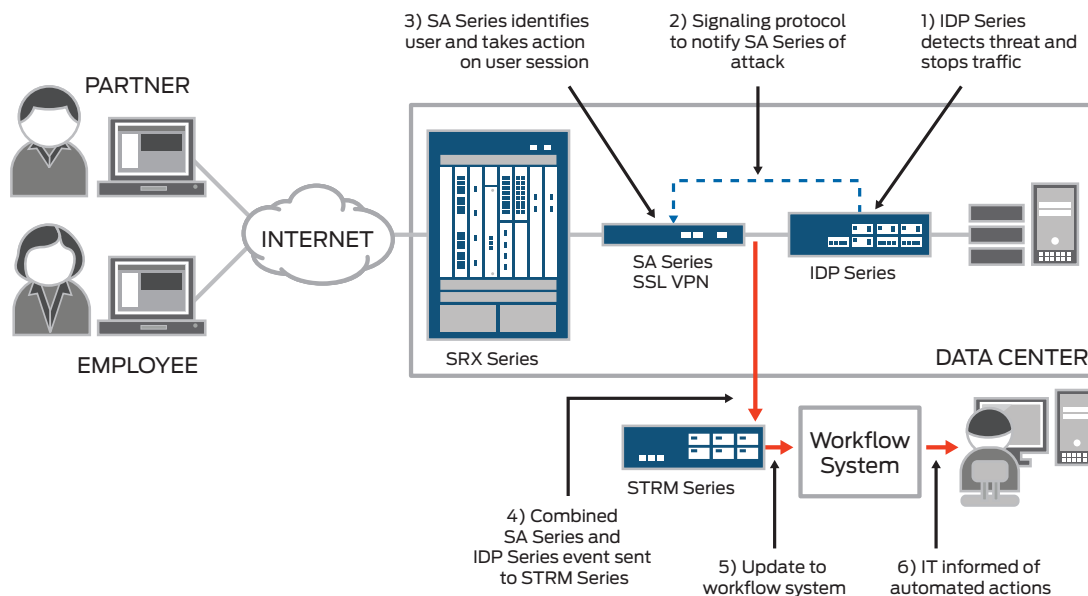


Figure 2: Juniper Networks Adaptive Threat Management Solutions in action: Malicious traffic or an out-of-policy action can be thwarted in real time, with a complete audit trail of events

Juniper Networks Adaptive Threat Management Solutions include the industry's only consistent enterprise-wide capabilities that focus on users and applications, no matter where they access the network. Role-based WX Client providing WAN acceleration functionality can be deployed via SA Series or UAC downloads, ensuring that the right users get the highest application performance possible, wherever they are. Juniper firewalls benefit from the application and threat information gleaned from the IDP Series, whether via integrated functionality or separate appliances. IDP Series alerts on malicious or noncompliant behavior trigger a change in access rights for a user throughout the network. Each individual device within the solution dynamically adds information and value to the whole, creating the dynamic risk mitigation you need.

Juniper Networks Adaptive Threat Management Solutions include the industry's only enterprise-wide access control capabilities that focus on users and applications, no matter where they access the network. Juniper firewalls can benefit from the application and threat information gleaned from the IDP Series appliances. The IDP Series alerts on malicious or noncompliant behavior triggers a change in access rights for a user throughout the network. Each individual device within the solution dynamically adds information to the whole, creating the dynamic risk mitigation you need.

Juniper Networks Adaptive Threat Management Solutions Phased Deployment Examples

- SA Series and UAC ensure consistent policy enforcement regardless of user location, while federated identity eliminates the need for multiple sign-ons across globally protected resources.
- SA Series and UAC downloads also provide a WX Client to speed application performance, as well as market-leading antivirus functionality.

- Juniper firewalls can be made identity aware and deployed as policy enforcers for the UAC solution, increasing choice and flexibility of where to deploy enforcement points.
- IDP Series capabilities are now deployable throughout the enterprise via integration into Juniper Networks SRX Series Services Gateways branch platforms, incremental addition to larger platforms, or deployment as a standalone platform. The IDP Series can monitor anomalous behaviors, malicious traffic, and the use of noncompliant applications on a per-user basis, and can then instruct a variety of products throughout the solution to drop, quarantine, or remediate the user/session.
- NSM provisions policies across the entire solution, greatly enhancing consistency and eliminating user errors.
- The STRM Series correlates all access and network usage information from Juniper firewalls, SA Series, UAC, IDP Series, networking products, and other vendor products—along with other corporate systems such as servers and applications. This completes the feedback loop required both for forensic activity and proactive planning. The STRM Series also eases compliance with over 500 reports that are prepackaged and very easy to customize.
- UAC also addresses the common problem of how to provide appropriate access to temporary guests, with an easy-to-use Web interface designed to be used by non-technical staff. These guests can be granted customizable, limited-time access privileges on the network during the duration of their stay.

Features and Benefits

Only Juniper Networks Adaptive Threat Management Solutions offer such a rich set of application delivery, risk mitigation capabilities, and network-wide policy control in an open and standards-based environment. Organizations experience increased productivity by provisioning security, acceleration, access control, routing, and switching devices through a single management console. Additional benefits are gained by monitoring and detecting threats and non-compliant behaviors, consolidating and correlating logs, and reporting from a single console. Simplified management leads to less human error, faster troubleshooting, and the ability to detect a security breach that may have slipped through a legacy environment. Users with different business roles can safely share the same network infrastructure with less ability to spread viruses and worms, since their endpoints must always be compliant with security policy and their access is restricted to only job-role entitled data and applications. Single sign-on, federated identity capabilities, and consistent policy experiences across a global enterprise network with Juniper Networks Adaptive Threat Management Solutions mean users can access the network easily and securely from anywhere without placing a burden on IT to administer such productivity capabilities across the network.

Key features and benefits of this solution include:

- Comprehensive security that identifies, mitigates, and reports on even the most sophisticated attacks anywhere in the network
- Reduced cost of ownership with lower CapEx and OpEx
- Network-wide, identity-based, application-aware security that enables business while providing unparalleled protection and compliance
- Dynamically provisioned security to all audiences regardless of location or device
- Improved network performance and application delivery
- Improved response times to incidents while requiring less IT resources
- Eliminates the trade-off between security and performance
- Enhanced compliance via network-wide, real-time visibility and control

Solution Components

Juniper Networks is a leader in network security, with innovative products recognized as best in their category by analysts around the world. Security products that can be deployed as part of Juniper Networks Adaptive Threat Management Solutions across an entire network include the following.

PRODUCT	HIGHLIGHTS
A complete family of firewall/VPN solutions	This suite of firewalls and integrated security products is tailored for specific uses, including Juniper Networks ISG Series Integrated Services Gateways and Juniper Networks SSG Series Secure Services Gateways. A tightly integrated set of unified threat management (UTM) capabilities protects against malware, worms, viruses, trojans, denial of service (DoS), and blended attacks.
SRX Series Services Gateways	These gateways provide firewall, IPS, VPN, and other network and security services. They are based on Juniper's revolutionary Dynamic Services Architecture—a stable, scalable platform designed to allow you to build the network you need today, with all of the headroom you could want for tomorrow. SRX Series Services Gateways are available in a variety of form factors, enabling you to buy what you need for each location.
WXC Series Application Acceleration Platforms	The WX Client significantly accelerates application to ensure an unparalleled user experience. When combined with user credentials, the WXC Series can ensure personalized delivery options while maintaining the highest level of security regardless of location.
IDP Series Intrusion Detection and Prevention Appliances	High-performance devices with up to 30 Gbps throughput. Available as standalone devices or integrated functionality in select firewalls, including the ISG Series and SRX Series platforms.
End-to-end access control solutions	Market-leading Juniper Networks SA Series SSL VPN Appliances provide remote and granular access control to group or individual level. Juniper Networks Unified Access Control for users on the LAN. Federated identity management enables single sign-on (SSO) across both platforms.
Network and Security Manager	This enables centralized provisioning of Juniper Networks routing, switching, and security products.
STRM Series Security Threat Response Managers	These provide a single console for log, compliance, and reporting; event correlation across diverse data sources; application-level monitoring; and network-based anomaly detection for Juniper and other network and security vendors.

Summary: Intelligent Security and Performance for the Distributed Enterprise

Juniper Networks Adaptive Threat Management Solutions offer robust and highly cooperative, network-wide solutions consisting of tightly integrated network security products. They provide industry-leading security that is dynamic and optimized for high-performance businesses, as well as network-wide visibility and control that is essential in protecting your enterprise from today's highly volatile and damaging security threats. Juniper Networks Adaptive Threat Management Solutions help you achieve a sustainable competitive advantage that you can implement over time, realizing the benefits of superior point products that work better because they work together.

Next Steps

For more information on Juniper Networks Adaptive Threat Management Solutions, please visit us at www.juniper.net/adapt or contact your Juniper Networks representative. If you are interested in learning about financing offerings, please ask about Juniper Financing Advantage, provided by IBM Global Financing. We offer comprehensive funding options at very competitive rates.

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.

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.