

# JUNIPER NETWORKS LAYERED SECURITY SOLUTION

## A Layered Security Stance for Empowering Higher Education

### Challenge

Higher education institutions today are faced with increasing demands for access to more and more network resources by students, faculty, staff and administration personnel. However, alongside these demands comes the need for better control of who is accessing what, and additional network security to counter a growing number of sophisticated threats that are hiding in common applications.

### Solution

The Juniper Networks layered security solution provides higher education IT managers with a complete set of security tools that can be deployed in layers to help achieve optimum security across their networks.

### Benefits

- Helping higher education institutions control what users have access to what resources in a structured environment
- Helping to protect campus resources and users from hidden security threats such as worms within normal-looking network traffic
- Protecting sensitive information such as personal student records during its transit across the network
- Detecting and eliminating harmful malware, like viruses and trojans, from email and Web servers before they propagate

At many higher education institutions, the infrastructure that helps everyone from students to faculty communicate and access information has evolved into a critical component of the daily operations for that organization. From Ethernet drops in student dorms to secure remote access for traveling staff and faculty around the globe, everyone is “plugged in” and expects the network to work any time, anywhere. These high-performance networks must be able to support daily academic functions in a timely, reliable and flexible manner. For example, many institutions are implementing a variety of sophisticated collaboration tools such as Web conferencing to help their users share resources productively. In addition, many traditional applications—like student registration and online course material—are evolving into Web-based applications, allowing easier access and manipulation for end users.

While this improved communications and information sharing has helped fulfill the academic mission of expanding knowledge, it is important to keep information resources and network communications secure and available. Security of this information and how it is carried across their networks continues to be a major concern for educational IT departments everywhere. This paper will outline some of these current trends and challenges and discuss how taking a structured approach to building up layers of security can help educational IT managers meet the needs of their customers.

### The Challenge

The traditional brick-and-mortar classroom is expanding “virtually” as students and faculty reach out to a global environment across high-performance education networks. Competitive pressures are also accelerating institutional offerings of alternative educational programs such as distance learning, online courses and outreach centers in remote locations. But, as with all changes, new challenges inevitably surface that require educational organizations to pay close attention to how they utilize electronic technology while also protecting sensitive information and users.

### Higher Education Security Threats

A widening range of both local and remote network access is being granted to students, faculty and staff, making the network increasingly vulnerable. The remote student, faculty or staff member will require different levels of access to campus resources, and appropriate measures must be taken to protect the campus network across these access levels. For example, a remote student may only need access to registration applications and class material, while an instructor working from home may require full access to all academic resources for both class and research efforts.

Increased Internet access from a myriad of connected and mobile devices has made every campus, dorm room and administrative office a potential entry point for a security attack. These sophisticated attacks can be launched by deliberate attackers or unknowingly by remote users logging in to the network. These network security attacks are increasing both in numbers and complexity, and include viruses and worms that are generally known as malicious programs or malware. Many forms of malware use common applications such as email to send messages to other users, while other types of malware use application vulnerabilities to replicate themselves via the network.

While stopping external attacks remains a constant challenge, equally troubling and difficult to defend against are the attacks that are perpetrated from inside the campus network by students and faculty who have full access to campus network resources. These internal attacks can range from the unintentional attacks from a user's laptop that is carrying an unknown virus to a disgruntled student destroying or stealing proprietary school information.

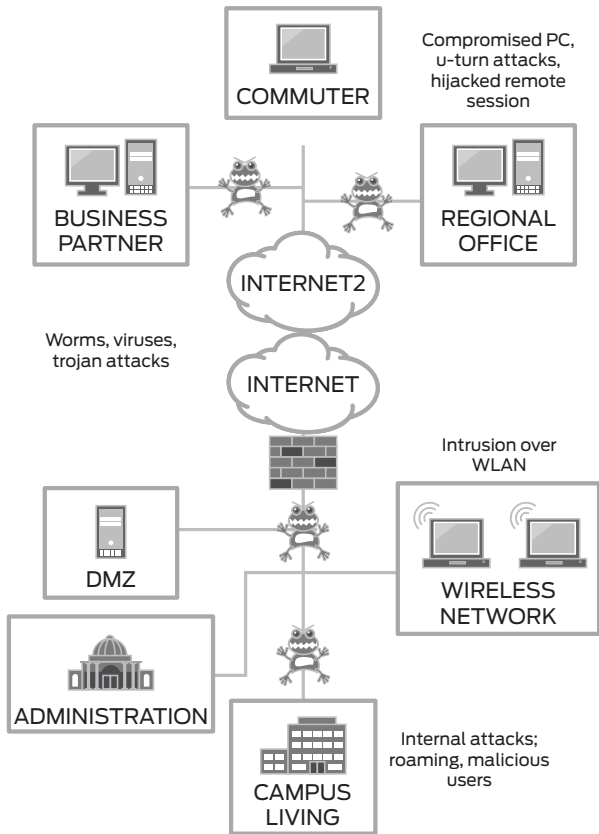


Figure 1: Higher education security threats

### Education Network IT Manager Challenges

While higher education institutions certainly want to strengthen the campus network against these security threats, they also want to retain the essence of an academic environment that promotes free expression and the exchange of ideas. This balancing act is one that IT departments at all higher education institutions are required to perform on a daily basis.

Within this open, yet secure environment, the major challenges for educational organizations can be summarized into three main categories:

- Maintaining a delicate balance between optimum network security that protects sensitive information, and flexible access control over students, faculty, staff and administration to help ensure that they can access what they need when they need it
- Building several lines of defense for higher education institutions that form a strong security stance through layers of access control, sensitive information protection and countermeasures against hidden security threats
- Providing campus IT departments with a complete set of security tools that they can deploy to help achieve end-to-end security all the way from remote locations to the main campus data center

### The Juniper Networks® Layered Security Solution

Layered security is a concept developed by Juniper Networks to help higher educational institutions strike this balance between strong network security and open network access for all campus users. This combination of security products provides educational organizations with a market-leading security solution that has been field proven in the networks of major service providers and enterprises around the globe.

This Juniper Networks layered security solution provides education IT managers with a complete set of security tools they can deploy in layers to help achieve optimized security across their networks.

### Features and Benefits

#### Features and Benefits

FEATURE	BENEFIT
Multiple standards-based access control and authentication security mechanisms	Helps higher educational institutions control what users have access to what resources in a structured environment
High-performance intrusion prevention resources	Helps protect campus resources and users from hidden security threats such as worms within normal-looking network traffic
Highly secure encryption technology	Protects sensitive information such as personal student records during its transit across the network
Deep application file-level security	Ensures early detection and elimination of harmful malware, including viruses and trojans in various email and Web servers before they can propagate

### Solution Components

The components of the Juniper Networks SecurED solution can be broken down into four main categories: (1) access control and authentication, (2) intrusion prevention, (3) encrypted communications and (4) unified threat management.

## Access Control and Authentication

1. **Firewalls:** A firewall helps to protect the education network from malicious content by performing a stateful inspection of incoming network packets. When examining the packet header (source and destination IP address/port numbers, packet sequence numbers) it determines whether or not to allow the packet through. In some cases, session-based firewalls also examine the “session” level to keep track of dynamic session protocols used in common client-server communications. Firewalls can also help provide denial-of-service (DoS) attack protection, where a malicious attacker can flood a network with packets to try and bring down the network. A firewall can quickly recognize this and automatically screen these packets.

It may also be important to identify and track applications to determine chatty users and servers. This capability, as well as many others, is available on the SRX Security Services Gateway. The SRX replaces numerous security solutions by providing a suite of services in one platform, including Firewall, Intrusion Prevention Systems (IPS) and Virtual Private Network (VPN) services. The SRX family is available in different performance form factors and can be deployed in a main campus, remote campus and data center.

2. **Firewall Virtual Security Zones:** By using a single Juniper Networks firewall appliance, such as the SRX Security Services Gateways, higher educational institutions can create distinct “virtual” network segments and manage which users have access to those segments. By defining virtual security zones on the Juniper Networks firewall, the campus network is logically divided into separate service segments, each with its own rules. For example, a campus might use a single Juniper Networks firewall to create zones according to campus service types like “teachers zone,” “principals” or “parent or volunteer zone.” Please see figure 2. This allows educational organizations to easily create, manage and enforce rules whereby only users from one department, for example, can access that department’s applications and data.

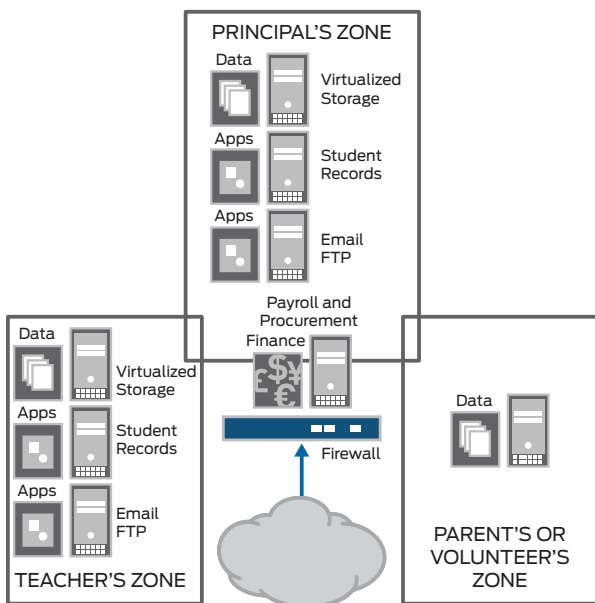


Figure 2: Firewall virtual security zones

3. **Unified Access Control:** Educational organizations need a centralized access policy manager on the LAN itself to ensure that only authorized users can get access, and LAN-based endpoints themselves are compliant with the campus network security policy. A LAN-based access control solution enables security policy enforcement and protects critical campus applications in a LAN environment. 802.1X is the standard from the IEEE for port-based network access control, protecting the campus network at the data link or access layer (Layer 2) by identifying and authenticating each LAN user before the network provides the user with an IP address.

Juniper Networks Unified Access Control (UAC) combines standards-based 802.1X access control technologies while leveraging existing campus investments and deployments. All policy is created and pushed by the IC Series UAC Appliance, a hardened centralized policy server. Juniper Networks UAC is compatible with multiple authentication and authorization databases, thereby allowing the combination of Microsoft Windows Active Directory user repositories, LDAP databases, Security Information Management Solutions (SIMS) and other popular security management tools. Endpoint control of user identity, device state and network location can be determined by a dynamically deployable Agent (UAC Agent), as well as via agentless mode when installing a software client is not feasible. Juniper designed UAC to interoperate with 802.1X-compliant enforcement points. Therefore, UAC is capable of instantiating a broad array of policies and associated enforcement actions on any 802.1X LAN switch. Unfortunately, many of the switches on the market today do not support the range of enforcement actions that UAC makes possible. Working in conjunction with UAC, each Juniper Networks EX Series Ethernet Switch supports the following enforcement actions:

- **Admission control:** The EX Series will permit or deny network access based on policies developed and distributed by UAC, including those policies based on user authentication status, endpoint posture compliance, user/device role and other policies. EX Series Ethernet Switches provide standards-based 802.1X port-level access control.
- **VLAN assignment:** An EX Series Ethernet Switch will assign an endpoint to a VLAN based on user/device identity, role or other policy parameter.
- **Bandwidth limiting:** The EX Series can constrain an endpoint to a specified maximum bandwidth based on policy created on and distributed by UAC, protecting network resources from over-consumption. Bandwidth limiting can be applied to every session an endpoint initiates (for example, a VoIP phone); by user identity or role (for example, certain users are rate limited to 1 Mbps while others have unlimited bandwidth); by destination (for example, limit traffic to/from the Internet to 10 Mbps); or other parameters.
- **Traffic marking:** Ethernet switches can apply QoS markings to traffic to ensure consistent handling throughout the network or within specific portions of the enterprise LAN. The EX Series will identify incoming traffic, match it against a QoS policy list, and mark it for appropriate handling by subsequent network devices. Marking can be based on user/

device identity or role, traffic type or other parameter. All EX Series Ethernet Switches support IEEE 802.1p marking at Layer 2 and IETF Differentiated Services (DiffServ) Code Point (DSCP) and IP Precedence marking at Layer 3.

- **Traffic scheduling and prioritization:** EX Series Ethernet Switches can queue and service traffic based on its priority setting. All EX Series Ethernet Switches provide eight queues per port and support 7,000 access control list (ACL) entries per switch, giving enterprises the flexibility to accommodate numerous classes of traffic and define very granular QoS policies. For example, when an 802.1X-enabled device authenticates to the network, with UAC a policy can be sent to the appropriate EX Series Ethernet Switch indicating it should give highest priority handling to traffic on that particular switch port. The port will mark the traffic and put it into a strict priority queue. All of this is done dynamically, eliminating the need for IT to configure QoS policies manually on each switch.
- **Policy-based routing:** Based on a specified policy created under UAC, the EX Series can forward traffic from one or more ports via a particular route. For example, a university can use this capability to ensure that IP telephony traffic is always forwarded over the lowest-latency path. This capability can also be used to route traffic from a guest or contractor through an IDP Series appliance before allowing it to other destinations.
- **Traffic mirroring:** Using Generic Routing Encapsulation (GRE) tunneling, an EX Series Ethernet Switch is able to mirror or copy a traffic flow to another EX Series Ethernet Switch. Universities can use this enforcement action in a number of ways. For example, IT could define a policy to mirror certain users' traffic to an IDP Series appliance or protocol analyzer in order to learn where those users go on the network and what applications and resources they use. Such information can be useful in refining access control policies or for tracking potentially suspicious users.

## Intrusion Prevention

The next layer of the layered security stance involves application-level protection technologies that monitor network traffic and dynamically analyze it for signs of attacks and intrusions. These devices are now searching for hidden security threats inside common applications like email and instant messaging (IM). These intrusion prevention system (IPS) devices examine control and data fields within the application flow to verify that the actions are allowed by the security policy and do not represent a threat to end systems. By determining application-level commands and primitives, they can identify content out of the norm and content that represents a known attack or exploit from worms, trojans, spyware and others. IPS devices can detect certain viruses or trojans by examining application service fields. For instance, IPS devices can examine the subject field, attachment name or attachment type within email traffic to detect characteristics of known viruses.

Juniper Networks IDP Series Intrusion Detection and Prevention Appliances detect both known and unknown application-layer threats within network traffic and eliminate those threats in

real time. The IDP Series also detect the use of unauthorized applications like instant messengers or file sharing. The IDP Series with its Multi-Method Detection (MMD) offers comprehensive coverage by leveraging multiple detection mechanisms. For example, by utilizing signatures as well as other detection methods that include protocol anomaly traffic detection, the IDP Series can thwart known attacks at all levels of the protocol stream as well as possible future variations of an attack.

## Encrypted Communications

The third layer of security involves setting up secure connections between locations that encrypt transmissions using technology called VPNs when running across untrusted mediums such as the Internet. While no one VPN solution is the "right" solution for every mobile student/faculty or for a distributed site situation, there are multiple VPN options from which to choose. For fixed remote campus locations, IPsec is the preferred method of deploying VPNs. IPsec can operate with low latency for applications that require high performance. Once they are configured and "in place" for fixed locations, they typically do not need to be reconfigured and can usually operate without manual intervention. Juniper has several purpose-built network security appliances that combine stateful inspection firewall capabilities with IPsec VPN functionality in one platform.

For the teleworker and mobile campus population, the ideal alternative is to use SSL VPNs. Since the SSL VPN uses technology embedded in all standard Web browsers, it uses a clientless platform and requires little or no manual configuration on behalf of the user or changes to internal servers. This makes VPN access seamless to the remote user. It is robust, and it combines security of communications with ease of use. Juniper Networks SA Series SSL VPN Appliances provide this segment of the educational population with a complete end-to-end security solution that includes endpoint client (checking the integrity of the end system before allowing any connection), device, data and server layered security controls.

For students and faculty accessing the network with mobile devices, Juniper Networks Junos® Pulse provides yet another layer of security.

Junos Pulse is a dynamic, standards based anytime/anywhere unified network client which builds on Juniper's market leading SA Series SSL VPN Appliance, UAC Solution and WXC Series WAN acceleration technology. The SA series SSL VPN Appliance can be provisioned to dynamically install Junos Pulse, which includes anti-spyware/anti-malware for the endpoint and removes the threat before access is granted. Junos Pulse's "location aware" capabilities allow a user—without any intervention—to automatically connect and to access authorized applications and data, based on their location. Access to network resources is also based on user identity and role.

## Unified Threat Management

The final layer of security involves file-level protection, which provides the ability to extract files within traffic and inspect them to detect malware, including viruses, worms or trojans. A common technology for file-level protection in a network is an antivirus

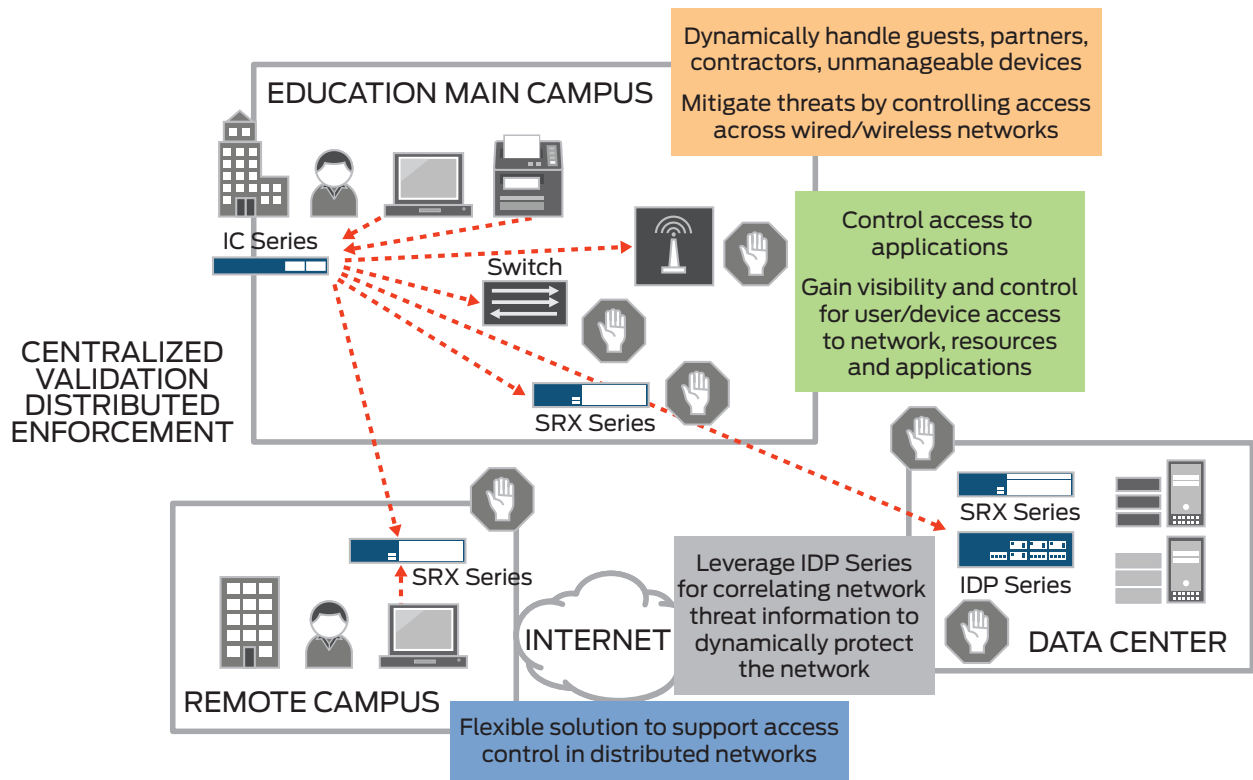


Figure 3: Unified Access Control

gateway. Antivirus systems typically scan files in email and Web traffic, mainly inspecting communication from servers to clients. Viruses are aimed at damaging enduser systems, but use various email and Web servers to propagate. Consequently, it is important to detect viruses while they are being uploaded to or downloaded from servers.

An antivirus system searches for virus signatures—a unique string of bytes that identifies a virus—and zaps the virus from the file. Most antivirus scanning systems catch not only the initial virus but also many of its variants, since the signature code usually remains intact. Gateway antivirus systems scan files that are embedded in network traffic, including files in HTTP traffic (Web downloads) and files in email traffic (attachments). If an infected file is detected, a gateway antivirus system removes it from the traffic, so that it does not affect other users. To scan files within network traffic, the gateway antivirus must detect a broad range of file-encoding protocols (for example, MIME, uucode, Base64) and file compression algorithms.

Juniper Networks family of integrated firewall/VPN solutions includes a complete set of UTM security features—such as stateful firewall, intrusion prevention, antivirus (instant message scanning, anti-spyware, anti-adware and anti-phishing), anti-spam and Web filtering—to stop worms, spyware, trojans, malware and other emerging attacks.

### Network Orchestration

Provisioning any of the products within Juniper Networks Layered Security Solution for Higher Education 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. With Juniper Networks Layered Security for Higher Education, 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.

<b>ORGANIZATION:</b>	ISLE OF WRIGHT (IOW) COLLEGE OFF THE SOUTH COAST OF ENGLAND
<b>Situation:</b>	Needed a secure, flexible remote access solution at the right price for teaching staff when abroad, working from home or at the outreach centres.
<b>Solution:</b>	Juniper Networks SA Series
<b>Results:</b>	For more than 50 key staff members, key work resources are readily, yet securely available any time, from anywhere. The entire network is protected while providing remote access and cost savings of IT budget and management resources.
<b>Customer Quote:</b>	<p>"Juniper Networks solution is exactly what IoW needs, at the right price. It is flexible and easily scales, allowing us to provide remote access to more staff members without incurring significant capital or management overhead costs."</p> <p>- Rosie Quelch, network manager, Isle of Wright College</p>

## Summary—A Layered Security Solution for Optimum Protection

With the growing need for open access to campus information and resources by students, faculty and staff, higher education networks will remain the target of increasingly sophisticated types of security attacks. The challenge will be how to protect the major assets of the campus while still fostering open communication and the exchange of ideas throughout the academic enterprise. Juniper Networks can help education IT departments build up a layered security solution that is designed to (1) control who has access to what through the use of firewalls, virtualization and access control technologies, (2) protect against application-level attacks from worms with IPS devices, (3) facilitate encrypted communications with an IPsec or SSL/VPN platform and (4) detect and deny deep file-level viruses or spyware using a UTM solution. For more information on Juniper Networks solutions for higher education, please visit [www.juniper.net/us/en/solutions/public-sector/research-education/](http://www.juniper.net/us/en/solutions/public-sector/research-education/) or contact your Juniper Networks representative today.

Layer Four Protection	File-Level Protection	Unified Threat Management
Layer Three Protection	Encrypted Communications	IPsec VPN SSL VPN
Layer Two Protection	Intrusion Prevention	Intrusion Detection and Prevention (IPS) Application Level
Layer One Protection	Access Control and Authentication	Firewalls Virtual Security Zones Unified Access Control

Figure 4: Layered security solution

## About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at [www.juniper.net](http://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](http://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 2012 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.