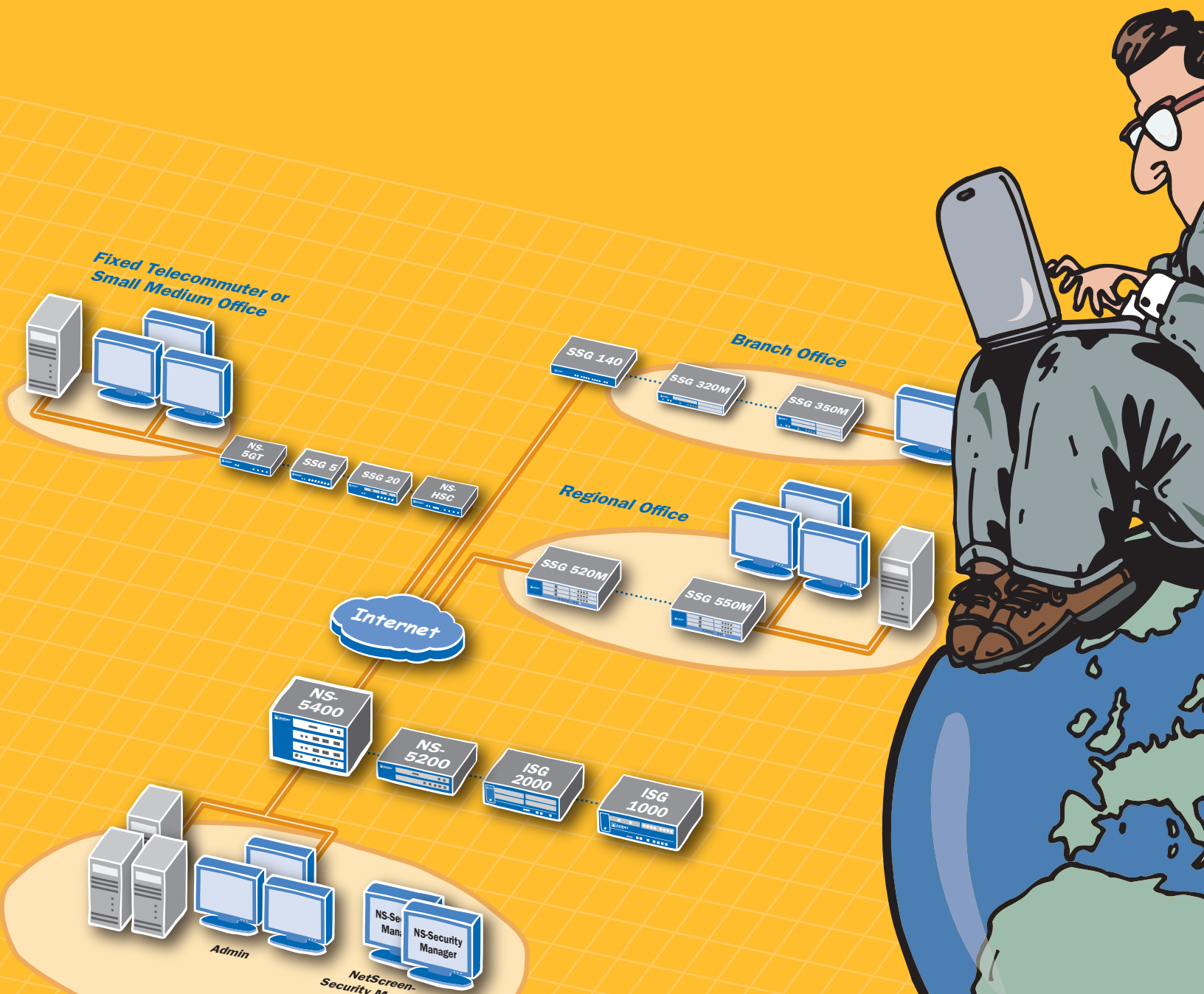


# Security Solutions Portfolio

Juniper Networks  
Integrated Firewall/VPN Solutions





Juniper Networks  
NetScreen-Hardware  
Security Client



Juniper Networks  
NetScreen-SGT and  
NetScreen-SGT ADSL



Juniper Networks  
NetScreen-SGT  
Wireless



Juniper Networks  
SSG 5



Juniper Networks  
SSG 5 Wireless



Juniper Networks  
SSG 20



Juniper Networks  
SSG 20 Wireless



Juniper Networks  
SSG 140



Juniper Networks  
SSG 320M



Juniper Networks  
SSG 350M



Juniper Networks  
SSG 520M



Juniper Networks  
SSG 550M



Juniper Networks  
ISG 1000



Juniper Networks  
ISG 2000



Juniper Networks  
NetScreen-5200



Juniper Networks  
NetScreen-5400

## Strong Security for Access Control, User Authentication, and Attack Protection at the Network and Application Level

As threats to the network grow more prevalent and destructive, securing the infrastructure is critical to maintaining a viable business. Attacks come from multiple sources in a variety of forms. Enterprises and service providers need more than just a security device; they require a comprehensive, reliable security solution backed by an industry leader.

The Juniper Networks integrated security devices are purpose-built to perform essential security functions. Optimized for maximum performance, they are controlled by a security-specific, real-time operating system, Juniper Networks ScreenOS. This operating system has been designed from the ground up to perform security functions without the overhead that can create vulnerabilities in other security products that rely on general-purpose operating systems.

With a range of purpose-built, high-performance platforms that deliver integrated security and LAN/WAN routing across high-density LAN/WAN interfaces, Juniper's integrated security devices address the needs of small to medium businesses, large distributed enterprises, and service providers. These integrated devices can protect the network from all manner of attacks and malware while simultaneously facilitating secure business-to-business communications.

### Product highlights:

- Complete set of Universal Threat Management (UTM) security features—including stateful firewall, intrusion prevention, antivirus (instant message scanning, anti-spyware, anti-adware, and anti-phishing), anti-spam, and Web filtering—stops worms, spyware, Trojans, malware, and other emerging attacks. (Note that not all UTM features are available on all platforms.)
- Centralized, policy-based management minimizes the chance of overlooking security holes by simplifying rollout and network-wide updates.
- Virtualization technologies make it easy for administrators to divide the network into secure segments for additional protection.
- Built-in high-availability features allow pairs of devices to be deployed together to eliminate single points of failure.
- Rapid-deployment features, including Auto Connect VPN, help minimize repetitive tasks and the administrative burden associated with widespread deployments.

## Perimeter Defense Begins with Network-Level Protection

To protect against network-level attacks, Juniper Networks devices use a dynamic packet filtering method known as stateful inspection to unmask malicious traffic. With this method, firewalls collect information on various components in a packet header, including source and destination IP addresses, source and destination port numbers, and packet sequence numbers. When a responding packet arrives, the firewall will compare the information reported in its header with the state of its associated session. If they do not match, the packet is dropped.

Stateful inspection provides more security than other firewall technology such as packet filtering because it opens smaller “holes” through which traffic can pass. By default, the Juniper Networks firewall denies all traffic in all directions. Then, by using centralized, policy-based management, enterprises can create security policies that define the parameters of traffic that is permitted to pass from specified sources to specified destinations.

Secure, reliable WAN connectivity also plays an important role in network-level protection. By deploying robust virtual private networks (VPNs), remote sites can be securely connected to other remote sites and to centralized data and applications using high-bandwidth shared media such as the Internet. Juniper Networks ScreenOS features such as Auto Connect VPN can help ease the administration and management of VPNs, particularly in hub-and-spoke topologies, allowing secure connections to be automatically set up and taken down without manual configuration.

## Day-Zero Protection Against Application-Level Attacks

To help block malicious application-level attacks, Juniper Networks seamlessly integrates intrusion prevention across the entire product line. For central enterprise sites and data center environments with high volumes of throughput, the Juniper Networks Integrated Security Gateway (ISG) Series with IDP can be deployed for application-level protection. The ISG Series with IDP tightly integrates the same software found on the Juniper Networks IDP Platforms into ScreenOS to provide unmatched application-level protection against worms, Trojans, spyware, and malware. The ISG Series supports more than 60 protocols, including those used by advanced applications such as VoIP and streaming media.

Unmatched security processing power and network segmentation features allow the ISG Series to protect critical high-speed networks against the penetration and proliferation of existing and emerging application-level threats. With multiple attack detection mechanisms, including stateful signatures and protocol anomaly, the ISG Series with IDP performs in-depth analysis of application protocol, context, and state to deliver Zero-day protection from application level attacks

On all other models, security administrators can deploy IPS capability using the Deep Inspection firewall to block application-level attacks. Deep Inspection utilizes two of the eight attack-detection mechanisms available on the standalone IDP platforms and integrates them with the stateful inspection firewall. The result is that the Deep Inspection firewall can apply a deeper level of application understanding to the network traffic to make access control decisions based on the intent of that traffic. If the packet's contents are inappropriate for the application it seeks, the packet can be dropped. Deployed in perimeter locations such as the branch office, a Deep Inspection firewall can block application-level attacks before they infect the network and inflict any damages.

### Integrated Antivirus Protects Remote Locations

For remote offices or smaller locations without full-time IT staff, integration and simplicity are an absolute must in any security solution. Juniper Networks currently provides integrated file-based antivirus protection on the Secure Services Gateway (SSG) family, the NetScreen-5GT Series, and NetScreen-HSC. These products combine firewall and VPN capabilities with an antivirus engine to provide a comprehensive security solution in a single device.

These integrated appliances scan for viruses imbedded in both e-mail and Web traffic by scrutinizing IMAP, SMTP, FTP, POP3, and HTTP protocols. They provide the most advanced protection from today's fast-spreading network viruses such as MSBlast, Sobig, and CodeRed. With its ability to uncompress files using common protocols, the engine scans deep inside attachments to detect viruses hidden in multiple levels of compression.

### Controlling Access to Known Malware and Phishing Web Sites

Employees who access inappropriate Web sites from the corporate network risk bringing malicious software into the organization. Worse, their errors in judgment could also expose the company to litigation for not having adequate controls in place. Juniper Networks integrated security devices are the ideal solution to help organizations devise and enforce responsible Web usage policies.

Two approaches are available: external and integrated Web filtering. External Web filtering, available on all Juniper Networks firewall and VPN devices, redirects traffic from the device to a dedicated SurfControl or Websense Web filtering server for enforcement of the organization's policies.

Integrated Web filtering, available on Juniper Networks NetScreen-HSC, NetScreen-5GT Series, NetScreen-25 and NetScreen-50, and the SSG family, enables enterprises to build their own Web access policies by selectively blocking access to sites listed in a continuously updated database. Maintained by SurfControl, a Juniper Networks security alliance partner, the database lists more than 13 million URLs organized into more than 54 categories of potentially problematic content.

Customers can rapidly deploy integrated or external Web filtering using default configurations based on the SurfControl database. Web filtering profiles can be customized by using black lists or white lists, plus a number of predefined and user-defined categories.

### Blocking Inbound Spam and Phishing Attacks

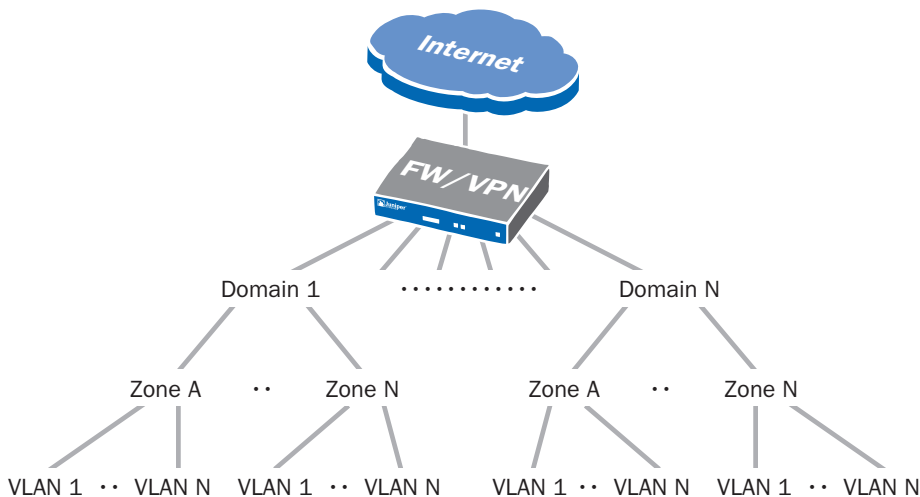
Juniper Networks has teamed with Symantec Corporation to leverage Symantec's market-leading AntiSpam solution and reputation service for Juniper's small-to-medium office platforms to help limit unwanted e-mails and the potential attacks they carry. Installed on the Juniper Networks firewall/VPN gateway, the AntiSpam engine filters incoming e-mail from known spam and phishing users, acting as a first line of defense. When a known malicious e-mail arrives, it is blocked and/or flagged so that the e-mail server can take appropriate action. Integrated anti-spam is available on NetScreen-HSC, NetScreen-5GT Series, NetScreen-25 and NetScreen-50, and Juniper's entire SSG family.

## Virtualization Boosts Security by Dividing the Network into Multiple Network Segments

Virtualization technologies in the Juniper Networks integrated firewall/VPN security solutions enable users to segment their network into many separate compartments, all controlled through a single appliance. Administrators can simply segment traffic bound for different destinations, or they can further divide the network into distinct, secure segments with their own firewalls and separate security policies.

The firewall/VPN devices support the following virtualization technologies:

- **Security Zones:** Supported on every product, security zones represent virtual sections of the network, segmented into logical areas. Security zones can be assigned to a physical interface or, on the larger devices, to a virtual system. When assigned to a virtual system, multiple zones can share a single physical interface which lowers ownership costs by effectively increasing interface densities.
- **Virtual Systems (VSYS):** Available on the NetScreen-500 and above, virtual systems are an additional level of partitioning that creates multiple independent virtual environments, each with its own set of users, firewalls, VPNs, security policies, and management interfaces. By providing administrators with the ability to quickly segment networks into multiple secure environments managed through a single device, VSYS enables network operators to build multi-customer solutions with fewer physical firewalls and reduced administrative attention. This reduces both capital and operational expenses.
- **Virtual Routers (VR):** Supported on all products, virtual routers enable administrators to partition a single device so it functions like multiple physical routers. Each VR can support its own domains, ensuring that no routing information is exchanged with domains established on other VRs. This enables a single device to support multiple customer environments, lowering total cost of ownership.
- **Virtual LANs (VLAN):** Supported on the NetScreen-200 and above, VLANs are a logical – not physical – division of a subnetwork that enables administrators to identify and segment traffic at a very granular level. Security policies can specify how traffic is routed from each VLAN to a security zone, virtual system or physical interface. This makes it easy for administrators to identify and organize traffic from multiple departments and define what resources each can access.

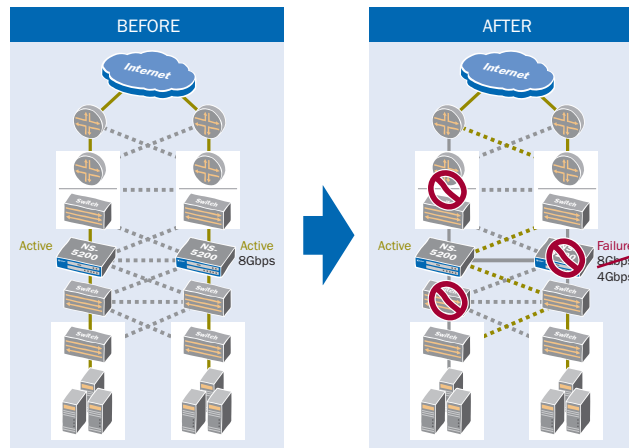


Networks are segmented into hierarchies of secure compartments using virtual technology.

## Comprehensive High-Availability Solutions Ensure Uptime

A security system is only as good as its reliability and uptime. Juniper Networks security solutions include reliable, high-availability systems based on the NetScreen Redundancy Protocol (NSRP). Firewalls and VPNs can be synchronized between high availability pairs to provide subsecond failover to a backup device. Configuration options include:

### System Redundancy Active/Active/Full Mesh



Full-mesh high availability configurations maintain service despite device failures

- **Active/Passive:** Master device shares all network, configuration setting, and current session information with the backup so that, in the event of a failure, the backup can take over in a seamless manner. Juniper Networks NetScreen-Security Manager provides centralized, policy-based control.

- **Active/Active:** Both devices are active, sharing an approximate equal amount of the load. If one fails, the other unit takes over to maintain traffic flow and security.

- **Active/Active/Full Mesh:** Both devices are configured to be active, with traffic flowing through each. Should one device fail, the other device becomes the master and continues to handle 100 percent of the traffic. The redundant physical paths provide maximum resiliency and uptime.

## Device Integration Made Easy

Networks are never static. Potentially costly and time-consuming changes and additions occur all the time. When the network topology changes, or as new offices, business partners, and customers are added to the network, network interoperability becomes especially important. To simplify network integration and help minimize administrative effort when changes are required, Juniper Networks integrated security solutions can operate in three different modes:

- **Transparent mode** affords the simplest way to add security to the network. In transparent mode, organizations can deploy a Juniper Networks firewall/VPN appliance without making any other changes to the network: firewall, VPN, and denial-of-service (DoS) mitigation functions work without an IP address, making the device “invisible” to the user.
- **Route mode** enables the security device to actively participate in network routing by supporting both static and dynamic routing protocols, including BGP, OSPF, RIPv1, RIPv2, and ECMP. Route mode enables administrators to quickly deploy multilayer security solutions with a minimum of manual configuration.
- **NAT mode** automatically translates an IP address or a group of IP addresses to a single address to hide an organization’s private addresses from public view.

Juniper Networks integrated security devices support both static and dynamic address assignment through DHCP or PPPoE, enabling Juniper Networks solutions to operate in any network environment.

### **NetScreen-Security Manager Provides Centralized, Policy-Based Control**

NetScreen-Security Manager takes a new approach to security management by providing IT departments with an easy-to-use solution that controls all aspects of the firewall/VPN security device, including device configuration, network settings, and security policy.

Unlike solutions that require administrators to use multiple management tools to control a single device, NetScreen-Security Manager enables IT departments to control the device throughout its life cycle with a single, centralized dashboard. It is designed specifically to foster teamwork among device technicians, network administrators, and security personnel.

The intuitive user interface of NetScreen-Security Manager streamlines the process of configuring devices, creating security policies, and setting up VPNs. It is easy to delegate administrative roles so that everyone who plays a role has access to the information and controls they need, while comprehensive logging tracks who performs each action. Dramatic reductions in operating costs are common because NetScreen-Security Manager promotes organizational efficiency like no other product on the market.

### **For Low-Cost Rapid Deployment, Drop Ship Devices—Not Administrators**

To avoid the high cost of sending administrators to configure systems at remote sites, Juniper Networks integrated security devices can be installed by nontechnical users. With the NetScreen-Security Manager Rapid Deployment functionality, network administrators do not need to preconfigure the devices or handle them in any way.

At the remote site, the new device simply needs to be cabled up and loaded with a small configuration file, which a central administrator has either e-mailed or sent on CD to the remote location. The initial configuration file establishes a secure connection to NetScreen-Security Manager, which then pushes the complete configuration files to the new device.

### **Juniper Networks Service and Support**

Juniper Networks delivers comprehensive service and support solutions. With our support portfolio, you benefit from the economy and simplicity of a single service solution to maintain your network's day-to-day operation. Key services include the delivery of around the clock technical assistance, online tools, software support, and options for parts delivery and onsite support. You receive the support you need and the value you deserve. For complete details, please visit us at: [www.juniper.net/products/services](http://www.juniper.net/products/services).

### **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](http://www.juniper.net).

To purchase Juniper Networks integrated security systems, please contact a Juniper Networks sales representative or authorized reseller.

CORPORATE HEADQUARTERS  
AND SALES HEADQUARTERS  
FOR NORTH AND SOUTH AMERICA

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
Phone: 888.JUNIPER (888.586.4737)  
or 408.745.2000  
Fax: 408.745.2100  
[www.juniper.net](http://www.juniper.net)

EAST COAST OFFICE

Juniper Networks, Inc.  
10 Technology Park Drive  
Westford, MA 01886-3146 USA  
Phone: 978.589.5800  
Fax: 978.589.0800

ASIA PACIFIC REGIONAL  
SALES HEADQUARTERS

Juniper Networks (Hong Kong) Ltd.  
Suite 2507-11, 25/F  
ICBC Tower  
Citibank Plaza, 3 Garden Road  
Central, Hong Kong  
Phone: 852.2332.3636  
Fax: 852.2574.7803

EUROPE, MIDDLE EAST, AFRICA  
REGIONAL SALES HEADQUARTERS

Juniper Networks (UK) Limited  
Building 1  
Aviator Park  
Station Road  
Addlestone  
Surrey, KT15 2PG, U.K.  
Phone: 44.(0).1372.385500  
Fax: 44.(0).1372.385501

Copyright 2007 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

