



# Juniper Networks SSG 300 Series

## Product Description

The SSG 300 Series comprises high-performance security platforms that help businesses stop internal and external attacks, prevent unauthorized access, and achieve regulatory compliance. The SSG 350M provides 500 Mbps of stateful firewall performance and 225 Mbps of IPSec VPN performance, while the SSG 320M provides 400 Mbps of stateful firewall performance and 175 Mbps of IPSec VPN performance.

These products focus on three key disciplines:

**Security:** Protection against viruses, spam, and emerging malware is delivered by proven UTM security features that are backed by best-in-class partners. To address internal security requirements and facilitate regulatory compliance, the SSG 300 Series supports an advanced set of network protection features such as security zones, virtual routers, and VLANs that allow administrators to divide the network into distinct, secure domains, each with their own unique security policy. Policies protecting each security zone can include access control rules and inspection by any of the supported UTM security features.

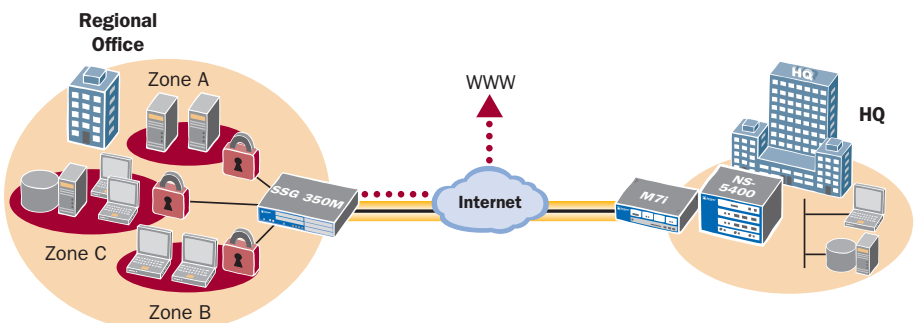
**Connectivity and Routing:** The SSG 300 Series provides four onboard 10/100/1000 interfaces complemented by I/O expansion slots that can house a mix of LAN or WAN interfaces, making the SSG 300 Series an extremely flexible platform. The broad array of I/O options coupled with WAN protocol and encapsulation support makes SSG 300 Series platforms easily deployable as traditional branch office routers or as consolidated security and routing devices, which can help reduce CapEx and OpEx.

**Access Control Enforcement:** The SSG 300 Series platforms can act as enforcement points in a Juniper Networks unified access control deployment with the simple addition of the Infranet Controller. The Infranet Controller functions as a central policy management engine by interacting with the SSG 300 Series to augment or replace the firewall-based access control. It grants/denies access based on more granular criteria, including endpoint state and user identity in order to accommodate the dramatic shifts in attack landscape and user characteristics.

In addition, Juniper Networks Professional Services will collaborate with your team to identify goals, define the deployment process, create or validate the network design, and manage the deployment to its successful conclusion. Whether it involves simple lab testing or a major network implementation, Juniper Networks Professional Services is there to help you ensure success.

*The Juniper Networks Secure Services Gateway 300 (SSG 300) Series consists of purpose-built security appliances that deliver the ideal blend of performance, security, routing, and LAN/WAN connectivity for large, regional branch offices and medium-size, standalone businesses. Traffic flowing in and out of a regional office or business is protected from worms, spyware, trojans, and malware by a complete set of Unified Threat Management (UTM) security features, including stateful firewall, IPSec virtual private network (VPN), Intrusion Prevention System (IPS), antivirus (includes anti-spyware, anti-adware, anti-phishing), anti-spam, and Web filtering. The SSG 300 Series comprises the SSG 350M and the SSG 320M offerings.*

The SSG 350M deployed at a branch office for secure Internet connectivity and site-to-site VPN to corporate headquarters. Internal branch office resources are protected with unique security policies applied to each Security Zone.



## Features and Benefits

Feature	Feature Description	Benefit
High performance	Purpose-built platform is assembled from custom-built hardware, powerful processing and a security-specific operating system.	Delivers performance headroom required to protect against internal and external attacks now and into the future.
Best-in-class UTM security features	UTM security features (antivirus, anti-spam, Web filtering, IPS) stop all manner of viruses and malware before they damage the network.	Ensures that the network is protected against all manner of attacks.
Integrated antivirus	Annually licensed antivirus engine, provided by Juniper, is based on Kaspersky Lab engine.	Stops viruses, spyware, adware and other malware.
Integrated anti-spam	Annually licensed anti-spam offering, provided by Juniper, is based on Symantec technology.	Blocks unwanted email from known spammers and phishers.
Integrated Web filtering	Annually licensed Web filtering solution, provided by Juniper, is based on SurfControl's technology.	Controls/blocks access to malicious Web sites.
Integrated Intrusion Prevention System (IPS) (Deep Inspection)	Annually licensed IPS engine is available with Juniper Networks' Deep Inspection Firewall Signature Packs.	Prevents application-level attacks from flooding the network.
Fixed Interfaces	Four fixed 10/100/1000 interfaces, two USB ports, one Console port and one Auxiliary port are standard on all SSG 300 Series models.	Provides high-speed LAN connectivity, future connectivity and flexible management.
Network segmentation	Bridge groups, security zones, virtual LANs and virtual routers allow administrators to deploy security policies to isolate guests, wireless networks and regional servers or databases.*	Powerful capabilities facilitate deploying security for various internal, external and DMZ sub-groups on the network, to prevent unauthorized access.
Interface modularity	Six interface expansion slots support optional T1, E1, Serial, ADSL/ADSL2/ADSL2+, G.SHDSL, 10/100/1000, and SFP connectivity.	Delivers combination of LAN and WAN connectivity on top of unmatched security to reduce costs and extend investment protection.
Robust routing engine	Proven routing engine supports OSPF, BGP and RIP v1/2 along with Frame Relay, Multilink Frame Relay, PPP, Multilink PPP and HDLC.	Enables the deployment of consolidated security and routing device, thereby lowering operational and capital expenditures.
Juniper Networks unified access control enforcement point	Interacts with the centralized policy management engine (Infranet Controller) to enforce session-specific access control policies using criteria such as user identity, device security state and network location.	Improves security posture in a cost-effective manner by leveraging existing customer network infrastructure components and best-in-class technology.
Management flexibility	Use any one of three mechanisms, CLI, WebUI or Juniper Networks NetScreen-Security Manager, to securely deploy, monitor and manage security policies.	Enables management access from any location, eliminating on-site visits thereby improving response time and reducing operational costs.
Auto-Connect VPN	Automatically sets up and takes down VPN tunnels between spoke sites in a hub-and-spoke topology.	Provides a scalable VPN solution for mesh architectures with support for latency-sensitive applications such as VoIP and video conferencing.
World-class professional services	From simple lab testing to major network implementations, Juniper Networks Professional Services will collaborate with your team to identify goals, define the deployment process, create or validate the network design and manage the deployment.	Transforms the network infrastructure to ensure that it is secure, flexible, scalable and reliable.

## Product Options

Option	Option Description	Applicable Products
Network Equipment Building Systems (NEBS) compliance	NEBS-compliant versions of the SSG 350M are available.	SSG 350M
DRAM	All SSG 300 Series models are available with 1 GB of DRAM. The SSG 320M and SSG 350M are also available in 256 MB-DRAM versions.	SSG 350M SSG 320M
UTM/Content Security (high memory option required)	With the addition of licensing keys, the Juniper SSG 300 Series can be configured with any combination of the following best-in-class UTM and content security functionality: antivirus (includes anti-spyware, anti-phishing), IPS (Deep Inspection firewall), Web filtering and/or anti-spam.	SSG 350M high-memory model only SSG 320M high-memory model only
I/O options	Three (SSG 320M) or five (SSG 350M) expansion slots support optional T1, E1, Serial, ADSL2+, G.SHDSL, 10/100/1000, and SFP.	SSG 350M SSG 320M

\*Bridge groups supported only on uPIMs in ScreenOS 6.0 and greater releases

## Specifications

	Juniper Networks SSG 320M	Juniper Networks SSG 350M
<b>Maximum Performance and Capacity<sup>(1)</sup></b>		
Minimum ScreenOS version support*	ScreenOS 6.0r2	ScreenOS 6.0r2
Firewall performance (Large packets)	450+ Mbps	550+ Mbps
Firewall performance (IMIX) <sup>(2)</sup>	400 Mbps	500 Mbps
Firewall Packets Per Second (64 byte)	175,000 PPS	225,000 PPS
AES256+SHA-1 VPN performance	175 Mbps	225 Mbps
3DES+SHA-1 VPN performance	175 Mbps	225 Mbps
Maximum concurrent sessions	48,000	48,000
New sessions/second	10,000	12,500
Maximum security policies	750	750
Maximum users supported	Unrestricted	Unrestricted
Convertible to JUNOS	Yes	Yes
<b>Network Connectivity</b>		
Fixed I/O	4x10/100/1000	4x10/100/1000
Physical Interface Module (PIM) Slots	3	5
WAN interface options (PIMS)	Serial, T1, E1, ADSL/ADSL2/ADSL2+, G.SHDSL	Serial, T1, E1, ADSL/ADSL2/ADSL2+, G.SHDSL
LAN interface options (uPIMS)	8x10/100/1000, 16x10/100/1000, and 6xSFP	8x10/100/1000, 16x10/100/1000, and 6xSFP
<b>Firewall</b>		
Network attack detection	Yes	Yes
DoS and DDoS protection	Yes	Yes
TCP reassembly for fragmented packet protection	Yes	Yes
Brute force attack mitigation	Yes	Yes
SYN cookie protection	Yes	Yes
Zone-based IP spoofing	Yes	Yes
Malformed packet protection	Yes	Yes
<b>Unified Threat Management<sup>(3)</sup></b>		
IPS (Deep Inspection firewall)	Yes	Yes
Protocol anomaly detection	Yes	Yes
Stateful protocol signatures	Yes	Yes
IPS/DI attack pattern obfuscation	Yes	Yes
Antivirus	Yes	Yes
Signature database	100,000+	100,000+
Protocols scanned	POP3, HTTP, SMTP, IMAP, FTP	POP3, HTTP, SMTP, IMAP, FTP
Anti-spyware	Yes	Yes
Anti-adware	Yes	Yes
Anti-keylogger	Yes	Yes
Instant message AV	Yes	Yes
Anti-spam	Yes	Yes
Integrated URL filtering	Yes	Yes
External URL filtering <sup>(4)</sup>	Yes	Yes
<b>Voice over IP (VoIP) Security</b>		
H.323 ALG	Yes	Yes
SIP ALG	Yes	Yes
MGCP ALG	Yes	Yes
SCCP ALG	Yes	Yes
NAT for VoIP protocols	Yes	Yes

\*Some features and functionality only supported in releases greater than ScreenOS 6.0

**Juniper Networks  
SSG 320M**
**Juniper Networks  
SSG 350M**
**IPSec VPN**

Concurrent VPN tunnels	250	350
Tunnel interfaces	100	200
DES (56-bit), 3DES (168-bit) and AES (256-bit)	Yes	Yes
MD-5 and SHA-1 authentication	Yes	Yes
Manual key, IKE, PKI (X.509)	Yes	Yes
Perfect forward secrecy (DH Groups)	1,2,5	1,2,5
Prevent replay attack	Yes	Yes
Remote access VPN	Yes	Yes
L2TP within IPSec	Yes	Yes
IPSec NAT traversal	Yes	Yes
Auto-Connect VPN	Yes	Yes
Redundant VPN gateways	Yes	Yes

**User Authentication and Access Control**

Built-in (internal) database - user limit	1,500	1,500
Third-party user authentication	RADIUS, RSA SecureID, LDAP	RADIUS, RSA SecureID, LDAP
RADIUS Accounting	Yes - start/stop	Yes - start/stop
XAUTH VPN authentication	Yes	Yes
Web-based authentication	Yes	Yes
802.1X authentication	Yes	Yes
Unified access control enforcement point	Yes	Yes

**PKI Support**

PKI Certificate requests (PKCS 7 and PKCS 10)	Yes	Yes
Automated certificate enrollment (SCEP)	Yes	Yes
Online Certificate Status Protocol (OCSP)	Yes	Yes
Certificate Authorities supported	VeriSign, Entrust, Microsoft, RSA Keon, iPlanet (Netscape) Baltimore, DoD PKI	VeriSign, Entrust, Microsoft, RSA Keon, iPlanet (Netscape) Baltimore, DoD PKI
Self-signed certificates	Yes	Yes

**Virtualization**

Maximum number of security zones	40	40
Maximum number of virtual routers	5	8
Bridge groups*	Yes	Yes
Maximum number of VLANs	125	125

**Routing**

BGP instances	3	3
BGP peers	4	16
BGP routes	10,000	10,000
OSPF instances	3	3
OSPF routes	10,000	10,000
RIP v1/v2 instances	128	128
RIP v2 routes	10,000	10,000
Static routes	10,000	10,000
Source-based routing	Yes	Yes
Policy-based routing	Yes	Yes
ECMP	Yes	Yes
Multicast	Yes	Yes
Reverse Path Forwarding (RPF)	Yes	Yes
IGMP (v1, v2)	Yes	Yes
IGMP Proxy	Yes	Yes
PIM SM	Yes	Yes
PIM SSM	Yes	Yes
Multicast inside IPSec tunnel	Yes	Yes

\*Bridge groups supported only on uPIMs in ScreenOS 6.0 and greater releases

**Juniper Networks  
SSG 320M**
**Juniper Networks  
SSG 350M**
**Encapsulations**

PPP	Yes	Yes
MLPPP	Yes	Yes
MLPPP max physical interfaces	6	10
Frame Relay	Yes	Yes
MLFR (FRF .15, FRF .16)	Yes	Yes
MLFR max physical interfaces	6	10
HDLC	Yes	Yes

**Mode of Operation**

Layer 2 (transparent) mode <sup>(5)</sup>	Yes	Yes
Layer 3 (route and/or NAT) mode	Yes	Yes

**Address Translation**

Network Address Translation (NAT)	Yes	Yes
Port Address Translation (PAT)	Yes	Yes
Policy-based NAT/PAT	Yes	Yes
Mapped IP	1,500	1,500
Virtual IP	16	16
MIP/VIP Grouping	Yes	Yes

**IP Address Assignment**

Static	Yes	Yes
DHCP, PPPoE client	Yes	Yes
Internal DHCP server	Yes	Yes
DHCP relay	Yes	Yes

**Traffic Management Quality of Service (QoS)**

Guaranteed bandwidth	Yes - per policy	Yes - per policy
Maximum bandwidth	Yes - per policy	Yes - per policy
Ingress traffic policing	Yes	Yes
Priority-bandwidth utilization	Yes	Yes
DiffServ marking	Yes - per policy	Yes - per policy

**High Availability (HA)**

Active/Active	Yes	Yes
Active/Passive	Yes	Yes
Configuration synchronization	Yes	Yes
Session synchronization for firewall and VPN	Yes	Yes
Session failover for routing change	Yes	Yes
Device failure detection	Yes	Yes
Link failure detection	Yes	Yes
Authentication for new HA members	Yes	Yes
Encryption of HA traffic	Yes	Yes

**System Management**

WebUI (HTTP and HTTPS)	Yes	Yes
Command line interface (console)	Yes	Yes
Command line interface (telnet)	Yes	Yes
Command line interface (SSH)	Yes v1.5 and v2.0 compatible	Yes v1.5 and v2.0 compatible
NetScreen-Security Manager	Yes	Yes
All management via VPN tunnel on any interface	Yes	Yes
Rapid deployment	No	No

	Juniper Networks SSG 320M	Juniper Networks SSG 350M
<b>Administration</b>		
Local administrator database size	20	20
External administrator database support	RADIUS, RSA SecurID, LDAP	RADIUS, RSA SecurID, LDAP
Restricted administrative networks	50	50
Root Admin, Admin and Read Only user levels	Yes	Yes
Software upgrades	TFTP, WebUI, NSM, SCP, USB	TFTP, WebUI, NSM, SCP, USB
Configuration rollback	Yes	Yes
<b>Logging/Monitoring</b>		
Syslog (multiple servers)	Yes - up to 4 servers	Yes - up to 4 servers
Email (two addresses)	Yes	Yes
NetIQ WebTrends	Yes	Yes
SNMP (v2)	Yes	Yes
SNMP full custom MIB	Yes	Yes
Traceroute	Yes	Yes
VPN tunnel monitor	Yes	Yes
<b>External Flash</b>		
Additional log storage	USB 1.1	USB 1.1
Event logs and alarms	Yes	Yes
System configuration script	Yes	Yes
ScreenOS Software	Yes	Yes
<b>Dimensions and Power</b>		
Dimensions (W x H x D)	17.5 in x 1.75 in x 150.1 in 44.45 cm x 8.51 cm x 54.61 cm	17.5 in x 2.61 in x 15.1 in 44.5 cm x 6.62 cm x 38.3 cm
Weight	15 lbs (no PIMs) 6.8 Kg	25.0 lbs (no PIMs) 11.34 Kg
Rack mountable	Yes, 2 RU	Yes, 1.5 RU
Power Supply (AC) 100-240 VAC	275 W	300 W
Average Power Consumption	80 W (No PIMs)	80 W (No PIMs)
Maximum Power Consumption	320 W	350 W
Input Frequency	47-63 Hz	47-63 Hz
Maximum Current Consumption	100 - 240 VAC, 3.2 A - 1.3 A	100 - 240 VAC, 3.5 A - 1.5 A
Maximum Inrush Current	100 - 240 VAC, 42 A - 62 A	100 - 240 VAC, 13 A - 32 A
Average Heat Dissipation	273 BTU (No PIMs)	273 BTU (No PIMs)
Maximum Heat Dissipation	1091 BTU	1195 BTU
Power Supply (DC)*	N/A	-48 to -60 VDC, 300 watts
Noise Level	40.0 dB	59.2 dB
<b>Certifications</b>		
Safety certifications	CSA, TUV, CB	CSA, TUV, CB
EMC certifications	FCC class A, CE class A, C-Tick, VCCI class A	FCC class B, CE class B, C-Tick, VCCI class B
NEBS**	No	Level 3 Q3, 2007
MTBF (Bellcore model)	7.2 years	6.8 years
<b>Security Certifications</b>		
Common Criteria: EAL4 and EAL4+	Future	Future
FIPS 140-2: Level 2	Future	Future
ICSA Firewall and VPN	Yes	Yes

\*SSG 350M with DC power supply available Q4, 2007

\*\*SSG 350M NEBS compliant version available Q3, 2007

## Operating Environment

<b>Operating temperature</b>	32° to 122° F, (0° to 50° C)	32° to 122° F, (0° to 50° C)
<b>Non-operating temperature</b>	-4° to 158° F -20° to 70° C	-4° to 158° F -20° to 70° C
<b>Humidity</b>	10 to 90% non-condensing	10 to 90% non-condensing

- (1) Performance, capacity and features listed are based upon systems running ScreenOS 6.0r2 and are the measured maximums under ideal testing conditions unless otherwise noted. Actual results may vary based on ScreenOS release and by deployment.
- (2) IMIX stands for Internet mix and is more demanding than a single packet size as it represents a traffic mix that is more typical of a customer's network. The IMIX traffic used is made up of 58.33% 64 byte packets + 33.33% 570 byte packets + 8.33% 1518 byte packets of UDP traffic.
- (3) UTM Security features (IPS/Deep Inspection, antivirus, anti-spam and Web filtering) are delivered by annual subscriptions purchased separately from Juniper Networks. Annual subscriptions provide signature updates and associated support. The high memory option is required for UTM security features.
- (4) Redirect Web filtering sends traffic from the firewall to a secondary server. The redirect feature is free. However, it does require the purchase of a separate Web filtering license from either Websense or SurfControl.
- (5) NAT, PAT, policy-based NAT, virtual IP, mapped IP, virtual systems, virtual routers, VLANs, OSPF, BGP, RIPv2, Active/Active HA and IP address assignment are not available in Layer 2 transparent mode.

## Ordering Information

Description	Part Number
SSG 320M, ScreenOS, Base Memory (256 MB), HW Security, AC Power Supply	SSG-320M-SB
SSG 320M, ScreenOS, High Memory (1 GB), HW Security, AC Power Supply	SSG-320M-SH
SSG 350M, ScreenOS, Base Memory (256 MB), HW Security, AC Power Supply	SSG-350M-SB
SSG 350M, ScreenOS, High Memory (1 GB), HW Security, AC Power Supply	SSG-350M-SH

SSG 300 Series I/O Options	Part Number
2 Port T1 PIM with integrated CSU/DSU	JX-2T1-RJ48-S
2 Port E1 PIM with integrated CSU/DSU	JX-2E1-RJ48-S
2 Port Synchronous Serial PIM	JX-2Serial-S
1 Port ADSL 2/2+ Annex A PIM	JX-1ADSL-A-S
1 Port ADSL 2/2+ Annex B PIM	JX-1ADSL-B-S
2-Port 2-wire or 1-Port 4-wire G.SHDSL PIM	JX-2SHDSL-S
6 Port SFP Gigabit Ethernet Universal PIM2	JXU-6GE-SFP-S
8 Port Gigabit Ethernet 10/100/1000 Copper Universal PIM2	JXU-8GE-TX-S
16 Port Gigabit Ethernet 10/100/1000 Copper Universal PIM2	JXU-16GE-TX-S
Small Form Factor Pluggable 1000Base-LX Gigabit Ethernet Optical Transceiver Module	JX-SFP-1GE-LX
Small Form Factor Pluggable 1000Base-SX Gigabit Ethernet Optical Transceiver Module	JX-SFP-1GE-SX

## Unified Threat Management/Content Security (High Memory Option Required)

	Part Number
Antivirus (includes anti-spyware, anti-phishing)	NS-K-AVS-SSG350 NS-K-AVS-SSG320
IPS (Deep Inspection)	NS-DI-SSG350 NS-DI-SSG320
Web filtering	NS-WF-SSG350 NS-WF-SSG320
Anti-spam	NS-SPAM-SSG350 NS-SPAM-SSG320
Remote Office Bundle (Includes AV, DI, WF)	NS-RBO-CS-SSG350 NS-RBO-CS-SSG320
Main Office Bundle (Includes AV, DI, WF, AS)	NS-SMB-CS-SSG350 NS-SMB-CS-SSG320

## SSG 300 Series Memory Upgrades, Spares and Communications Cables

	Part Number
Power cable, Australia	CBL-JX-PWR-AU
Power cable, China	CBL-JX-PWR-CH
Power cable, Europe	CBL-JX-PWR-EU
Power cable, Italy	CBL-JX-PWR-IT
Power cable, Japan	CBL-JX-PWR-JP
Power cable, UK	CBL-JX-PWR-UK
Power cable, USA	CBL-JX-PWR-US
1 Gigabyte Memory Upgrade for the SSG 300 Series	SSG-300-MEM-1GB
Replacement air filter for SSG 300 Series	SSG-350-FLTR
EIA530 cable (DTE)	JX-CBL-EIA530-DTE
RS232 cable (DTE)	JX-CBL-RS232-DTE
RS449 cable (DTE)	JX-CBL-RS449-DTE
V.35 cable (DTE)	JX-CBL-V35-DTE
X.21 cable (DTE)	JX-CBL-X21-DTE
Blank I/O plate	JX-Blank-FP-S

## 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).



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.