SSG320M AND SSG350M SECURE SERVICES GATEWAYS

Product Overview

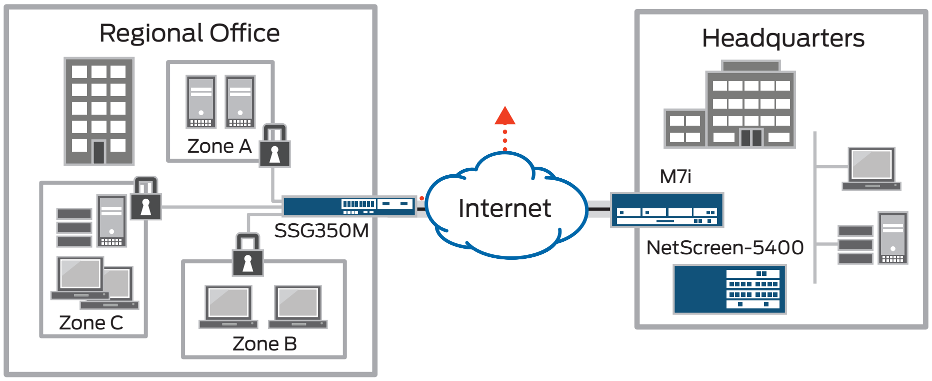
The Juniper Networks SSG300 line consists of purpose-built security appliances that deliver the ideal blend of performance, security, routing, and LAN/WAN connectivity for large, regional branch offices and medium-size, standalone businesses. Traffic flowing in and out of a regional office or business is protected from worms, spyware, trojans, and malware by a complete set of Unified Threat Management security features, including stateful firewall, IPsec VPN, intrusion prevention system (IPS), antivirus (includes antispyware, antiadware, antiphishing), antispam, and Web filtering. The SSG300 line comprises the SSG350M and the SSG320M Secure Services Gateways.

Product Description

The Juniper Networks® SSG300 line of secure services gateways comprises high-performance security platforms that help businesses stop internal and external attacks, prevent unauthorized access, and achieve regulatory compliance. The Juniper Networks SSG350M Secure Services Gateway provides 500 Mbps of stateful firewall performance and 225 Mbps of IPsec VPN performance, while the Juniper Networks SSG320M Secure Services Gateway provides 400 Mbps of stateful firewall performance and 175 Mbps of IPsec VPN performance.

These products focus on three key disciplines:

Security: Protection against worms, viruses, trojans, spam, and emerging malware is delivered by proven Unified Threat Management (UTM) security features that are backed by best-in-class partners. To address internal security requirements and facilitate regulatory compliance, the SSG300 line 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.



The SSG350M 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.

Connectivity and Routing: The SSG300 line 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 SSG300 line an extremely flexible platform. The broad array of I/O options coupled with WAN protocol and encapsulation support makes the SSG300 line of gateways 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 SSG300 line of gateways can act as enforcement points in a Juniper Networks Unified Access Control deployment with the simple addition of the Juniper Networks IC Series UAC Appliances. The IC Series functions as a central policy management engine by interacting with the SSG300 line 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.

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, antispam, 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 antispam	Annually licensed antispam offering, provided by Juniper, is based on Sophos technology.	Blocks unwanted email from known spammers and phishers.
Integrated Web filtering	Annually licensed Web filtering solution, provided by Juniper, is based on Websense SurfControl 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 SSG300 line 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 (IC Series) 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 Network and Security Manager (NSM), 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.

*Bridge groups supported only on uPIMs in Juniper Networks ScreenOS® Software 6.0 and higher releases.

Product Options

Option	Option Description	Applicable Products
Network Equipment Building Systems (NEBS) compliance	NEBS-compliant versions of the SSG350M are available.	SSG350M
DRAM	All models in the SSG300 line are available with 1 GB of DRAM. The SSG320M and SSG350M are also available in 256 MB-DRAM versions.	SSG350M SSG320M
UTM/Content Security (high memory option required)	With the addition of licensing keys, the SSG300 line can be configured with any combination of the following best-in-class UTM and content security functionality: antivirus (includes antispyware, antiphishing), IPS (Deep Inspection firewall), Web filtering and/or antispam.	SSG350M high-memory model only SSG320M high-memory model only
I/O options	Three (SSG320M) or five (SSG350M) expansion slots support optional T1, E1, Serial, ADSL2+, G.SHDSL, 10/100/1000, and SFP.	SSG350M SSG320M

SSG320M

SSG350M

Specifications

	SSG320M	SSG350M
Maximum Performance and Capacity[1]		
ScreenOS version tested	ScreenOS 6.3	ScreenOS 6.3
Firewall performance (Large packets)	450+ Mbps	550+ Mbps
Firewall performance (IMIX)[2]	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	64,000	128,000
New sessions/second	10,000	12,500
Maximum security policies	2,000	2,000
Maximum users supported	Unrestricted	Unrestricted
Convertible to Juniper Networks Junos® operating system 8.0 or higher	Yes	Yes
Network Connectivity		
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

Specifications (continued)

	SSG320M	SSG350M
Firewall		
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
Unified Threat Management[3]		
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	200,000+	200,000+
Protocols scanned	POP3, HTTP, SMTP, IMAP, FTP, IM	POP3, HTTP, SMTP, IMAP, FTP, IM
Antispyware	Yes	Yes
Antiadware	Yes	Yes
Anti-keylogger	Yes	Yes
Instant message AV	Yes	Yes
Antispam	Yes	Yes
Integrated URL filtering	Yes	Yes
External URL filtering[4]	Yes	Yes
VoIP Security		
H.323 ALG	Yes	Yes
SIP ALG	Yes	Yes
MGCP ALG	Yes	Yes
SCCP ALG	Yes	Yes
NAT for VoIP protocols	Yes	Yes
IPsec VPN		
Concurrent VPN tunnels	500	500
Tunnel interfaces	100	300
DES (56-bit), 3DES (168-bit) and AES (256-bit)	Yes	Yes
MD-5 and SHA-1 authentication	Yes	Yes
Manual key, IKE, IKEv2 with EAP, 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	500	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

Specifications (continued)

	SSG320M	SSG350M
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	8	8
Bridge groups*	Yes	Yes
Maximum number of VLANs	125	125
Routing		
BGP instances	8	8
BGP peers	36	48
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
Encapsulations		
PPP	Yes	Yes
MLPPP	Yes	Yes
MLPP 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
IPv6		
Dual stack IPv4/IPv6 firewall and VPN	Yes	Yes
IPv4 to/from IPv6 translations and encapsulations	Yes	Yes
Syn-Cookie and Syn-Proxy DoS Attack Detection	Yes	Yes
SIP, RTSP, Sun-RPC, and MS-RPC ALG's	Yes	Yes
RIPng	Yes	Yes
BGP	Yes	Yes
Transparent mode	Yes	Yes
NSRP	Yes	Yes
DHCPv6 Relay	Yes	Yes
Mode of Operation		
Layer 2 (transparent) mode[5]	Yes	Yes
Layer 3 (route and/or NAT) mode	Yes	Yes

*Bridge groups supported only on uPIMs in ScreenOS 6.0 and higher releases.

Specifications (continued)

	SSG320M	SSG350M
Address Translation		
Network Address Translation (NAT)	Yes	Yes
Port Address Translation (PAT)	Yes	Yes
Policy-based NAT/PAT (L2 and L3 mode)	Yes	Yes
Mapped IP (L3 mode)	4,000	4,000
Virtual IP (L3 mode)	32	32
MIP/VIP Grouping (L3 mode)	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 - L3 mode	Yes	Yes
Active/Passive - Transparent & L3 mode	Yes	Yes
Configuration synchronization	Yes	Yes
Session synchronization for firewall and VPN	Yes	Yes
VRRP	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
Network and Security Manager (NSM)	Yes	Yes
All management via VPN tunnel on any interface	Yes	Yes
Rapid deployment	No	No
Administration		
Local administrator database size	20	20
External administrator database support	RADIUS, RSA SecurID, LDAP	RADIUS, RSA SecureID, 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
Logging/Monitoring		
Syslog (multiple servers)	Yes - up to 4 servers	Yes - up to 4 servers
Email (two addresses)	Yes	Yes
NetIQ WebTrends	Yes	Yes
SNMP (v3)	Yes	Yes
SNMP full custom MIB	Yes	Yes
Traceroute	Yes	Yes
VPN tunnel monitor	Yes	Yes

Specifications (continued)

	SSG320M	SSG350M
External Flash		
Additional log storage	USB 1.1	USB 1.1
Event logs and alarms	Yes	Yes
System configuration script	Yes	Yes
ScreenOS Software	Yes	Yes
Dimensions and Power		
Dimensions (W x H x D)	17.5 x 1.8 x 15.1 in (44.5 x 4.5 x 38.3 cm)	17.5 x 2.6 x 15.1 in (44.5 x 6.6 x 38.3 cm)
Weight	15.0 lb (no interface modules) 6.8 kg	25.0 lb (no interface modules + one power supply) (11.34 kg)
Rack mountable	Yes, 1 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 – 75 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
Certifications		
Safety certifications	CSA, TUV, CB	CSA, TUV, CB
EMC certifications	FCC class A, CE class A, C-Tick, VCCI class B	FCC class A, CE class A, C-Tick, VCCI class B
NEBS	No	Level 3
MTBF (Bellcore model)	7.2 years	6.8 years
Security Certifications		
Common Criteria: EAL4	Yes (ScreenOS 6.2)	Yes (ScreenOS 6.2)
FIPS 140-2: Level 2	Yes	Yes
ICSA Firewall and VPN	Yes	Yes
Operating Environment		
Operating temperature	32° to 122° F (0° to 50° C)	32° to 122° F (0° to 50° C)
Non-operating temperature	-4° to 158° F (-20° to 70° C)	-4° to 158° F (-20° to 70° C)
Humidity	10% to 90% noncondensing	10% to 90% noncondensing

(1) Performance, capacity and features listed are based upon systems running ScreenOS 6.3 and are the measured maximums under ideal testing conditions unless otherwise noted. Actual results may vary based on ScreenOS release and by deployment. For a complete list of supported ScreenOS versions for SSG Series gateways, please visit the Juniper Customer Support Center (www.juniper.net/customers/support/) and click on ScreenOS Software Downloads.

(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, antispam 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.

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit **www.juniper.net/us/en/products-services**.

Ordering Information

Model Number	Description
SSG320M	
SSG-320M-SB	SSG320M, ScreenOS, base memory (256 MB), HW security, AC power supply
SSG-320M-SH	SSG320M, ScreenOS, base memory (1 GB), HW security, AC power supply
SSG350M	
SSG-350M-SB	SSG350M, ScreenOS, base memory (256 MB), HW security, AC power supply
SSG-350M-SH	SSG350M, ScreenOS, base memory (1 GB), HW security, AC power supply
SSG-350M-SB-TAA	SSG350M gateway, ScreenOS, base memory (256 MB), 5 PIM slots, HW Crypto, AC power supply, TAA, 19" rack mount
SSG-350M-SH-TAA	SSG350M gateway, ScreenOS, base memory (1 GB), 5 PIM slots, HW Crypto, AC power supply, TAA, 19" rack mount
SSG-350M-SB-DC-N-TAA	SSG350M gateway, ScreenOS, base memory (256 MB), 5 PIM slots, HW Crypto, DC power supply, fan filter, NEBS, TAA, 19" rack mount
SSG-350M-SH-DC-N-TAA	SSG350M gateway, ScreenOS, base memory (1 GB), 5 PIM slots, HW Crypto, DC power supply, fan filter, NEBS, TAA, 19" rack mount
SSG300 Line I/O Options	
JX-2T1-RJ48-S	2-port T1 PIM with integrated CSU/DSU
JX-2E1-RJ48-S	2-port E1 PIM with integrated CSU/DSU
JX-2Serial-S	2-port Synchronous Serial PIM
JX-1ADSL-A-S	1-port ADSL 2/2+ Annex A PIM
JX-1ADSL-B-S	1-port ADSL 2/2+ Annex B PIM
JX-2SHDSL-S	2-port 2-wire or 1-port 4-wire G.SHDSL PIM
JX-1BRI-ST-S	1-port ISDN BRI S/T PIM
JXU-6GE-SFP-S	6-port SFP Gigabit Ethernet Universal PIM2
JXU-8GE-TX-S	8-port Gigabit Ethernet 10/100/1000 Copper Universal PIM2
JXU-16GE-TX-S	16-port Gigabit Ethernet 10/100/1000 Copper Universal PIM2
JX-SFP-1GE-LX	Small form factor pluggable 1000BASE-LX Gigabit Ethernet Optical Transceiver Module
JX-SFP-1GE-SX	Small form factor pluggable 1000BASE-SX Gigabit Ethernet Optical Transceiver Module
Unified Threat Management/Content Security (High Memory Option Required)	
NS-K-AVS-SSG350 NS-K-AVS-SSG320	Antivirus (includes antispyware, antiphishing)
NS-DI-SSG350 NS-DI-SSG320	IPS (Deep Inspection)
NS-WF-SSG350 NS-WF-SSG320	Web filtering
NS-SPAM2-SSG350 NS-SPAM2-SSG320	Antispam
NS-RBO-CS-SSG350 NS-RBO-CS-SSG320	Remote Office Bundle (includes AV, DI, WF)
NS-SMB2-CS-SSG350 NS-SMB2-CS-SSG320	Main Office Bundle (includes AV, DI, WF, AS)
SSG300 Line Memory Upgrades, Spares and Communications Cables	
CBL-JX-PWR-AU	Power cable, Australia
CBL-JX-PWR-CH	Power cable, China
CBL-JX-PWR-EU	Power cable, Europe
CBL-JX-PWR-IT	Power cable, Italy
CBL-JX-PWR-JP	Power cable, Japan
CBL-JX-PWR-UK	Power cable, UK
CBL-JX-PWR-US	Power cable, USA
SSG-300-MEM-1GB	1 Gigabyte memory upgrade for the SSG300 line
SSG-350-FLTR	Replacement air filter for SSG300 line
JX-CBL-EIA530-DTE	EIA530 cable (DTE)
JX-CBL-RS232-DTE	RS232 cable (DTE)
JX-CBL-RS449-DTE	RS449 cable (DTE)
JX-CBL-V35-DTE	V.35 cable (DTE)
JX-CBL-X21-DT	X.21 cable (DTE)
JX-Blank-FP-S	Blank I/O plate

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**.

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 and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: 31.0.207.125.700
Fax: 31.0.207.125.701

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

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.

1000203-009-EN Sept 2013

Printed on recycled paper