Datasheet

The Juniper Networks Secure Services Gateway 500 (SSG 500) Series consists of purpose-built security appliances that deliver the perfect blend of performance, security, routing and LAN/WAN connectivity for large, regional branch offices and medium-sized, standalone businesses. Traffic flowing in and out of the 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 VPN, IPS, antivirus (includes anti-spyware, anti-adware, anti-phishing), anti-spam and Web filtering. The SSG 500 Series comprises the SSG 550/SSG 550M and the SSG 520/SSG 520M.

Juniper Networks SSG 500 Series

Portfolio Description

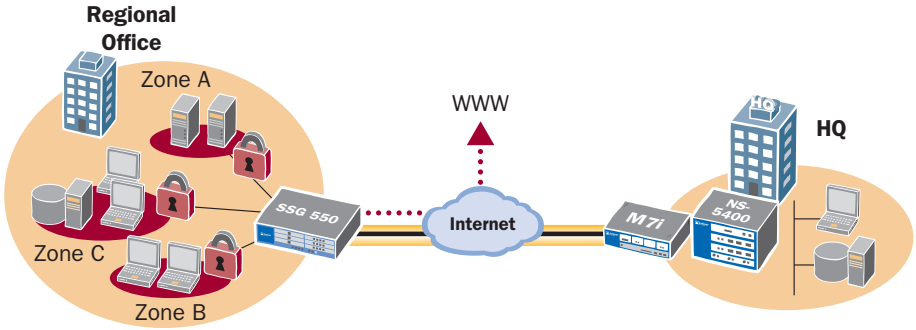
The SSG 500 Series consists of high-performance security platforms for regional branch office and medium-sized, standalone businesses that want to stop internal and external attacks, prevent unauthorized access and achieve regulatory compliance. The SSG 550/SSG 550M provides 1 + Gbps of stateful firewall performance and 600 Mbps of IPSec VPN performance, while the SSG 520/SSG 520M provides 650 Mbps of stateful firewall performance and 300 Mbps of IPSec VPN performance.

Security: Protection against viruses, 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 SSG 500 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 500 Series provides four onboard 10/100/1000 interfaces complemented by six I/O expansion slots that can house a mix of LAN or WAN interfaces, making the SSG 500 Series an extremely flexible platform. The broad array of I/O options coupled with WAN protocol and encapsulation support makes SSG 500 Series platforms easily deployable as traditional branch office routers or as consolidated security and routing devices to reduce CAPEX and OPEX.

Access Control Enforcement: The SSG 500 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 500 Series to augment or replace the firewall-based access control with a solution that 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.

World-Class Support: 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 to its successful conclusion.



The SSG 550 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 500 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, DS3, E3, 10/100/1000, 10/100 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
Single or redundant AC or DC power supplies	All SSG 500 series models are available with either AC or DC power supplies. The SSG 520 and SSG 520M offer a single power supply. The SSG 550 and SSG 550M are available with optional redundant power supplies.	SSG 550/SSG 550M SSG 520/SSG 520M
Network Equipment Building Systems (NEBS) compliance	NEBS-compliant versions of the SSG 520M and the SSG 550M are available.	SSG 550M SSG 520M
DRAM	All SSG 500 series models are available with 1 GB of DRAM. The SSG 520 and SSG 550 are also available in 512 MB-DRAM versions.	SSG 550/SSG 550M SSG 520/SSG 520M
Unified Threat Management/Content Security (high memory option required)	The Juniper SSG 500 series can be configured with any combination of the following best-in-class UTM and content security functionality: antivirus (includes snti-spyware, anti-phishing), IPS (Deep Inspection), Web filtering and/or anti-spam.	SSG 550 high-memory model only /SSG 550M SSG 520 high-memory model only /SSG 520M
I/O options	Six interface expansion slots support optional T1, E1, Serial, DS3, 10/100/1000, 10/100 and SFP connectivity.	SSG 550/SSG 550M SSG 520/SSG 520M

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

Specifications

	Juniper Networks SSG 520/SSG 520M	Juniper Networks SSG 550/SSG 550M
Maximum Performance and Capacity[1]		
Minimum ScreenOS version support*	ScreenOS 5.4	ScreenOS 5.4
Firewall performance (Large packets)	650+ Mbps	1+ Gbps
Firewall performance (IMIX)[2]	600 Mbps	1 Gbps
Firewall Packets Per Second (64 byte)	300,000 PPS	600,000 PPS
AES256+SHA-1 VPN performance	300 Mbps	500 Mbps
3DES+SHA-1 VPN performance	300 Mbps	500 Mbps
Maximum concurrent sessions	64,000	128,000
New sessions/second	10,000	15,000
Maximum security policies	1,000	4,000
Maximum users supported	Unrestricted	Unrestricted
Convertible to JUNOS 8.0	SSG 520M Only	SSG 550M Only
Network Connectivity		
Fixed I/O	4x10/100/1000	4x10/100/1000
Physical Interface Module (PIM) Slots	6 (2 ePIM/uPIM/PIM + 4 uPIM/PIM)	6 (4 ePIM/uPIM/PIM + 2 uPIM/PIM)
WAN interface options (PIMS)	Serial, T1, E1, DS3, E3, ADSL/ADSL2/ADSL2+, G.SHDSL	Serial, T1, E1, DS3, E3, ADSL/ADSL2/ADSL2+, G.SHDSL
LAN interface options (ePIMS and uPIMS)	10/100, 10/100/1000, and SFP	10/100, 10/100/1000, and SFP
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	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[4]	Yes	Yes
Voice over IP (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

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

	Juniper Networks SSG 520/SSG 520M	Juniper Networks SSG 550/SSG 550M
IPSec VPN		
Concurrent VPN tunnels	500	1,000
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, 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	60	60
Maximum number of virtual routers	5	8
Bridge groups*	Yes	Yes
Maximum number of VLANs	125	150
Routing		
BGP instances	9	15
BGP peers	16	16
BGP routes	10,000	20,000
OSPF instances	3	8
OSPF routes	10,000	20,000
RIP v1/v2 instances	128	256
RIP v2 routes	10,000	20,000
Static routes	10,000	20,000
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 520/SSG 520M	Juniper Networks SSG 550/SSG 550M
Encapsulations		
PPP	Yes	Yes
MLPPP	Yes	Yes
MLPP max physical interfaces	12	12
Frame Relay	Yes	Yes
MLFR (FRF .15, FRF .16)	Yes	Yes
MLFR max physical interfaces	12	12
HDLC	Yes	Yes
Mode of Operation		
Layer 2 (transparent) mode[5]	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	6,000
Virtual IP	16	32
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 520/SSG 520M	Juniper Networks SSG 550/SSG 550M
Administration		
Local administrator database size	20	20
External administrator database support	RADIUS, RSA SecurID, LDAP	RADIUS, RSA SecureID, LDAP
Restricted administrative networks	6	6
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 (v2)	Yes	Yes
SNMP full custom MIB	Yes	Yes
Traceroute	Yes	Yes
VPN tunnel monitor	Yes	Yes
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 (HxWxD)	3.5" x 17.5" x 21.5" 8.51 cm x 44.45 cm x 54.61 cm	3.5" x 17.5" x 21.5" 8.51 cm x 44.45 cm x 54.61 cm
Weight	23.0 lbs (no interface modules) 10.43 Kg	25.0 lbs (no interface modules + one power supply) 11.34 Kg
Rack mountable	Yes, 2RU	Yes, 2RU
Power supply (AC)	100-240 VAC, 350 watts	100-240 VAC, 420 watts
Power supply (DC)	-48 to -60 VDC, 420 watts	-48 to -60 VDC, 420 watts
Redundant power supply (hot swappable)	No	Yes
Maximum thermal output	1,070 BTU/Hour (W)	1,145 BTU/Hour (W)
Certifications		
Safety certifications	UL, CUL, CSA, CB	UL, CUL, CSA, CB
EMC certifications	FCC class A, CE class A, C-Tick, VCCI class A	FCC class A, CE class A, C-Tick, VCCI class A
NEBS	Level 3 (SSG 520M only)	Level 3
MTBF (Bellcore model)	12 years	12 years
Security Certifications		
Common Criteria: EAL4 and EAL4+	Future	Future
FIPS 140-2: Level 2	Future	Future
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% non-condensing	10 to 90% non-condensing

(1) Performance, capacity and features listed are based upon systems running ScreenOS 5.4 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.

IPS (Deep Inspection firewall) Signature Packs

Signature Packs provide the ability to tailor the attack protection to the specific deployment and/or attack type. The following Signature Packs are available for the SSG 500 Series:

Signature Pack	Target Deployment	Defense Type	Type of Attack Object
Base	Branch offices, small/medium businesses	Client/server and worm protection	Range of signatures and protocol anomalies
Client	Remote/branch offices	Perimeter defense, compliance for hosts (desktops, and so on)	Attacks in the server-to-client direction
Server	Small/medium businesses	Perimeter defense, compliance for server infrastructure	Attacks in the client-to-server direction
Worm Mitigation	Remote/branch offices of large enterprises	Most comprehensive defense against worm attacks	Worms, trojans, backdoor attacks

Ordering Information

SSG 550M	Part Number
SSG 550M with 1 GB Memory, 0 PIM Cards, 1 AC Power Supply	SSG-550M-SH
SSG 550M with 1 GB Memory, 0 PIM Cards, 1 AC Power Supply, NEBS Compliant	SSG-550M-SH-N
SSG 550M with 1 GB Memory, 0 PIM Cards, 1 DC Power Supply, NEBS Compliant	SSG-550M-SH-DC-N

SSG 550	Part Number
SSG 550 with 512 MB Memory, 0 PIM Cards, 1 AC Power Supply	SSG-550B-001
SSG 550 with 1 GB Memory, 0 PIM Cards, 1 AC Power Supply	SSG-550-001
SSG 550 with 1 GB Memory, 0 PIM Cards, 1 AC Power Supply, NEBS Compliant	SSG-550-001-NEBS
SSG 550 with 1 GB Memory, 0 PIM Cards, 1 DC Power Supply	SSG-550-001-DC

SSG 520M	Part Number
SSG 520M with 1 GB Memory, 0 PIM Cards, 1 AC Power Supply	SSG-520M-SH
SSG 520M with 1 GB Memory, 0 PIM Cards, 1 AC Power Supply, NEBS Compliant	SSG-520M-SH-N
SSG 520M with 1 GB Memory, 0 PIM Cards, 1 DC Power Supply, NEBS Compliant	SSG-520M-SH-DC-N

SSG 520	Part Number
SSG 520 with 512 MB Memory, 0 PIM Cards, AC Power	SSG-520B-001
SSG 520 with 1 GB Memory, 0 PIM Cards, AC Power	SSG-520-001
SSG 520 with 1 GB Memory, 0 PIM Cards, DC Power	SSG-520-001-DC

SSG 500 Series I/O Options	Part Number
1 Port Gigabit Ethernet 10/100/1000 Copper Enhanced PIM[1]	JXE-1GE-TX-S
1 Port Fiber Gigabit Ethernet Enhanced PIM (SFP sold separately)[1]	JXE-1GE-SFP-S
4 Port Fast Ethernet Enhanced PIM[1]	JXE-4FE-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
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 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
1 Port G.SHDSL PIM	JX-2SHDSL-S
1 Port DS3 PIM	JX-1DS3-S
1 Port E3 PIM	JX-1E3-S
6 Port SFP Gigabit Ethernet Universal PIM[2]	JXU-6GE-SFP-S
8 Port Gigabit Ethernet 10/100/1000 Copper Universal PIM[2]	JXU-8GE-TX-S
16 Port Gigabit Ethernet 10/100/1000 Copper Universal PIM[2]	JXU-16GE-TX-S

Unified Threat Management/Content Security (High Memory Option Required)	Part Number
Antivirus (includes anti-spyware, anti-phishing)	NS-K-AVS-SSG550 NS-K-AVS-SSG520
IPS (Deep Inspection)	NS-DI-SSG550 NS-DI-SSG520
Web filtering	NS-WF-SSG550 NS-WF-SSG520
Anti-spam	NS-SPAM-SSG550 NS-SPAM-SSG520
Remote Office Bundle (Includes AV, DI, WF)	NS-RBO-CS-SSG550 NS-RBO-CS-SSG520
Main Office Bundle (Includes AV, DI, WF, AS)	NS-SMB-CS-SSG550 NS-SMB-CS-SSG520

SSG 500 Series Memory Upgrades, Spares and Communications Cables	Part Number
Spare Power Supply for SSG 550, AC Power	SSG-PS-AC
Spare Power Supply for SSG 550, DC Power	SSG-PS-DC
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 500 series	SSG-500-MEM-1GB
Replacement air filter for SSG 550 Series	SSG-500-FLTR
EIA530 cable (DCE)	JX-CBL-EIA530-DCE
EIA530 cable (DTE)	JX-CBL-EIA530-DTE
RS232 cable (DCE)	JX-CBL-RS232-DCE
RS232 cable (DTE)	JX-CBL-RS232-DTE
RS449 cable (DCE)	JX-CBL-RS449-DCE
RS449 cable (DTE)	JX-CBL-RS449-DTE
V.35 cable (DCE)	JX-CBL-V35-DCE
V.35 cable (DTE)	JX-CBL-V35-DTE
X.21 cable (DCE)	JX-CBL-X21-DCE
X.21 cable (DTE)	JX-CBL-X21-DT
Blank I/O plate	JX-Blank-FP-S

[1] Enhanced Pluggable Interface Modules (Enhanced PIMs) are used in ePIM slots only (SSG 520 / SSG 520M / SSG 550 / SSG 550M / J4350 / J6350 only)

[2] Universal Pluggable Interface Modules (Universal PIMs) are used in either ePIM slots or regular PIM slots on the SSG and J-series platforms and are only supported in ScreenOS 6.0 or greater releases

Juniper Your Net™

About Juniper Networks

Juniper Networks develops purpose-built, high-performance IP platforms that enable customers to support a wide variety of services and applications at scale. Service providers, enterprises, governments and research and education institutions rely on Juniper to deliver a portfolio of proven networking, security and application acceleration solutions that solve highly complex, fast-changing problems in the world's most demanding networks. Additional information can be found at www.juniper.net.

Juniper® NETWORKS

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

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

100143-005 Mar 2007