



# Juniper Networks SSG 5 and SSG 20

## Portfolio Description

The SSG 5 and SSG 20 are high-performance security platforms for small branch office and standalone businesses that want to stop internal and external attacks, prevent unauthorized access and achieve regulatory compliance. Both the SSG 5 and SSG 20 deliver 160 Mbps of stateful firewall traffic and 40 Mbps of IPsec VPN traffic.

**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 SSG 5 and SSG 20 both support 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 its own unique security policy. Policies protecting each security zone can include access control rules and inspection by any of the supported UTM security features.

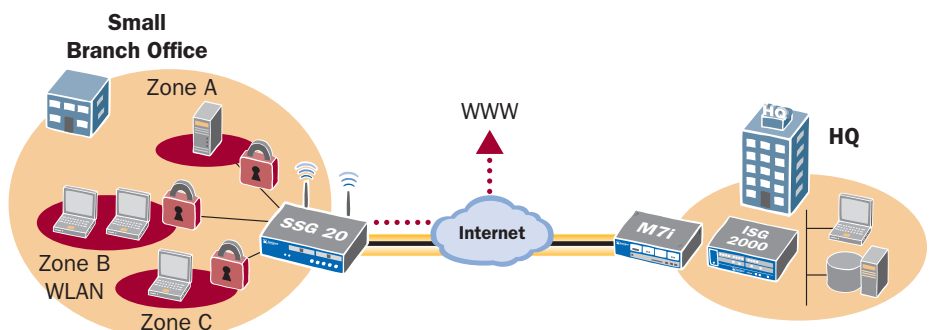
**Connectivity and Routing:** The SSG 5 has seven on-board 10/100 interfaces with optional fixed WAN ports. The SSG 20 has five 10/100 interfaces with two I/O expansion slots for additional WAN connectivity. The broad array of I/O options coupled with WAN protocol and encapsulation support in the routing engine make both the SSG 5 and the SSG 20 a solution that can easily be deployed as a traditional branch office router or as a consolidated security and routing device to reduce CAPEX and OPEX. Both the SSG 5 and SSG 20 support 802.11 a/b/g as a factory configured option supported by a wide array of wireless specific security features.

**Access Control Enforcement:** The SSG 5 and SSG 20 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, interacting with the SSG 5 or SSG 20 to augment or replace the firewall-based access control with a solution that grants/denies access based on more granular criteria that include 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 Juniper Networks™ Secure Services Gateway 5 (SSG 5) and Secure Services Gateway 20 (SSG 20) are purpose-built security appliances that deliver a perfect blend of performance, security, routing and LAN/WAN connectivity for small branch offices, fixed telecommuters and small standalone business deployments. Traffic flowing in and out of the branch office or business is protected from worms, spyware, trojans, and malware by a complete set of Unified Threat Management (UTM) security features that include stateful firewall, IP Security (IPsec) virtual private network (VPN), Intrusion Prevention System (IPS), antivirus (includes anti-spyware, anti-adware, anti-phishing), anti-spam and Web filtering.*

The SSG 20 deployed at a branch office for secure Internet connectivity and site-to-site VPN to corporate headquarters. Internal wired and wireless 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 is based on Kaspersky Lab engine.	Stops viruses, spyware, adware and other malware.
Integrated anti-spam	Annually licensed anti-spam offering is based on Symantec technology.	Blocks unwanted email from known spammers and phishers.
Integrated Web filtering	Annually licensed Web filtering solution is based on SurfControl's technology.	Controls/blocks access to malicious Web sites.
Integrated IPS (Deep Inspection)	Annually licensed IPS engine.	Prevents application-level attacks from flooding the network.
Fixed Interfaces	Seven fixed 10/100 interfaces on the SSG 5, and five fixed 10/100 interfaces on the SSG 20. The SSG 5 is factory configured with either RS232 Serial/AUX or ISDN BRI S/T or V.92 fixed WAN backup. Both models include one console port and one auxiliary port.	Provides high-speed LAN connectivity, redundant WAN connectivity and flexible management.
Network segmentation	Security zones, virtual LANs and virtual routers allow administrators to deploy security policies to isolate guests, wireless networks and regional servers or databases.	Facilitates deployment of internal security to prevent unauthorized access, contain attacks and assist in achieving regulatory compliance.
Interface modularity	Two interface expansion slots (SSG 20 only) supporting optional ADSL 2+, T1, E1, ISDN BRI S/T, Serial, SFP and v.92 Mini physical interface modules (Mini-PIMs).*	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.	Enables the deployment of a consolidated security and routing device, thereby lowering operational and capital expenditures.
802.11 a/b/g wireless-specific security features	Wireless-specific privacy and authentication features augment the UTM security capabilities to protect wireless traffic.	Provides additional device consolidation opportunities (WLAN access point, security, routing) for small office environment.
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, command line interface (CLI), WebUI or Network and Security Manager (NSM) to securely deploy, monitor and manage security policies.	Enables management access from any location, eliminating onsite visits thereby improving response time and reducing operational costs.
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
DRAM	The SSG 5 and SSG 20 are available with either 128 MB or 256 MB of DRAM.	SSG 5 and SSG 20
Unified Threat Management/Content Security (high memory option required)	The SSG 5 and SSG 20 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), Web filtering and/or anti-spam.	High memory SSG 5 or SSG 20 only
I/O options	Two interface expansion slots (SSG 20 only) supporting optional ADSL 2+, T1, E1, ISDN BRI S/T, Serial, SFP and v.92 Mini physical interface modules (Mini-PIMs).	SSG 5 and SSG 20
802.11 a/b/g connectivity	The SSG 5 and SSG 20 can be factory configured for 802.11 a/b/g wireless LAN connectivity.	SSG 5 and SSG 20
Extended license	Key capacities can be increased (sessions, VPN tunnels, VLANs) and stateful High Availability (HA) support for firewall and VPN can be added.	SSG 5 and SSG 20

\*Serial and SFP Mini-PIMs only supported in ScreenOS 6.0 or greater releases

## Specifications<sup>(1)</sup>

### SSG 5 Base/Extended

### SSG 20 Base/Extended

#### Maximum Performance and Capacity<sup>(2)</sup>

	SSG 5 Base/Extended	SSG 20 Base/Extended
ScreenOS version tested	ScreenOS 6.2	ScreenOS 6.2
Firewall performance (Large packets)	160 Mbps	160 Mbps
Firewall performance (IMIX) <sup>(3)</sup>	90 Mbps	90 Mbps
Firewall Packets Per Second (64 byte)	30,000 PPS	30,000 PPS
Advanced Encryption Standard (AES) 256+SHA-1 VPN performance	40 Mbps	40 Mbps
3DES encryption +SHA-1 VPN performance	40 Mbps	40 Mbps
Maximum concurrent sessions	8,000/16,000	8,000/16,000
New sessions/second	2,800	2,800
Maximum security policies	200	200
Maximum users supported	Unrestricted	Unrestricted

#### Network Connectivity

	SSG 5 Base/Extended	SSG 20 Base/Extended
Fixed I/O	7x10/100	5x10/100
Mini-Physical Interface Module (Mini-PIM) slots	0	2
WAN interface options	Factory configured: RS232 Serial AUX or ISDN BRI S/T or V.92	Mini-PIMs: 1xADSL 2+, 1xT1, 1xE1, V.92, ISDN BRI S/T, 1xSFP, 1xSerial

#### Firewall

	SSG 5 Base/Extended	SSG 20 Base/Extended
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<sup>(4)</sup>

	SSG 5 Base/Extended	SSG 20 Base/Extended
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
Instant message AV	Yes	Yes
Signature database	200,000+	200,000+
Protocols scanned	POP3, HTTP, SMTP, IMAP, FTP, IM	POP3, HTTP, SMTP, IMAP, FTP, IM
Anti-spyware	Yes	Yes
Anti-adware	Yes	Yes
Anti-keylogger	Yes	Yes
Anti-spam	Yes	Yes
Integrated URL filtering	Yes	Yes
External URL filtering <sup>(5)</sup>	Yes	Yes

#### Voice over IP (VoIP) Security

	SSG 5 Base/Extended	SSG 20 Base/Extended
H.323. Application-level gateway (ALG)	Yes	Yes
SIP ALG	Yes	Yes
MGCP ALG	Yes	Yes
SCCP ALG	Yes	Yes
Network Address Translation (NAT) for VoIP protocols	Yes	Yes

#### IPsec VPN

	SSG 5 Base/Extended	SSG 20 Base/Extended
Auto-Connect VPN	Yes	Yes
Concurrent VPN tunnels	25/40	25/40
Tunnel interfaces	10	10
DES encryption (56-bit), 3DES encryption (168-bit) and Advanced Encryption Standard (AES) (256-bit)	Yes	Yes

## Specifications<sup>(1)</sup> (continued)

	SSG 5 Base/Extended	SSG 20 Base/Extended
<b>IPsec VPN (cont'd)</b>		
MD-5 and SHA-1 authentication	Yes	Yes
Manual key, Internet Key Exchange (IKE), IKEv2 with EAP public key infrastructure (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
Layer2 Tunneling Protocol (L2TP) within IPsec	Yes	Yes
IPsec Network Address Translation (NAT) traversal	Yes	Yes
Redundant VPN gateways	Yes	Yes
<b>User Authentication and Access Control</b>		
Built-in (internal) database - user limit	100	100
Third-party user authentication	RADIUS, RSA SecureID, LDAP	RADIUS, RSA SecureID, LDAP
RADIUS Accounting	Yes	Yes
XAUTH VPN authentication	Yes	Yes
Web-based authentication	Yes	Yes
802.1X authentication	Yes	Yes
Unified Access Control (UAC) enforcement point	Yes	Yes
<b>PKI Support</b>		
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
<b>Virtualization</b>		
Maximum number of security zones	8	8
Maximum number of virtual routers	3/4	3/4
Maximum number of VLANs	10/50	10/50
<b>Routing</b>		
BGP instances	3/4	3/4
BGP peers	10/16	10/16
BGP routes	1,024	1,024
OSPF instances	3	3
OSPF routes	1,024	1,024
RIP v1/v2 instances	16	16
RIP v2 routes	1,024	1,024
Static routes	1,024	1,024
Source-based routing	Yes	Yes
Policy-based routing	Yes	Yes
Equal-cost multipath (ECMP)	Yes	Yes
Multicast	Yes	Yes
Reverse Path Forwarding (RPF)	Yes	Yes
Internet Group Management Protocol (IGMP) (v1, v2)	Yes	Yes
IGMP Proxy	Yes	Yes
PIM single mode	Yes	Yes
PIM source-specific multicast	Yes	Yes
Multicast inside IPsec tunnel	Yes	Yes
ICMP Router Discovery Protocol (IRDP)	Yes	Yes

## Specifications<sup>(1)</sup> (continued)

	SSG 5 Base/Extended	SSG 20 Base/Extended
<b>Encapsulations</b>		
Point-to-Point Protocol (PPP)	Yes	Yes
Multilink Point-to-Point Protocol (MLPPP)	N/A	Yes
Frame Relay	Yes	Yes
Multilink Frame Relay (MLFR) (FRF 15, FRF 16)	Yes	Yes
HDLC	Yes	Yes
<b>IPv6</b>		
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
<b>Mode of Operation</b>		
Layer 2 (transparent) mode <sup>(6)</sup>	Yes	Yes
Layer 3 (route and/or NAT) mode	Yes	Yes
<b>Address Translation</b>		
Network Address Translation (NAT)	Yes	Yes
Port Address Translation (PAT)	Yes	Yes
Policy-based NAT/PAT (L2 and L3 mode)	Yes	Yes
Mapped IP (MIP) (L3 mode)	300	300
Virtual IP (VIP) (L3 mode)	4/5	4/5
MIP/VIP Grouping (L3 mode)	Yes	Yes
Dual untrust	Yes	Yes
Bridge groups	Yes	Yes
<b>IP Address Assignment</b>		
Static	Yes	Yes
DHCP, PPPoE client	Yes	Yes
Internal DHCP server	Yes	Yes
DHCP relay	Yes	Yes
<b>Traffic Management Quality of Service (QoS)</b>		
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
Differentiated Services stamping	Yes - per policy	Yes - per policy
<b>High Availability (HA)<sup>(7)</sup></b>		
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
Session failover for routing change	Yes	Yes
VRRP	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

## Specifications<sup>(1)</sup> (continued)

	S5G 5 Base/Extended	S5G 20 Base/Extended
<b>System Management</b>		
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	Yes	Yes
<b>Administration</b>		
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
<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)	8.8 x 1.6 x 5.6 in (22.2 x 4.1 x 14.3 cm)	11.6 x 1.8 x 7.4 in (29.5 x 4.5 x 18.7 cm)
Weight	2.1 lb (0.95 kg)	3.3 lb (1.5 kg)
Rack mountable	Yes	Yes
Power supply (AC)	100-240 VAC	100-240 VAC
Maximum thermal output	122.8 BTU/Hour	122.8 BTU/Hour
<b>Certifications</b>		
Safety certifications	CSA, CB	CSA, CB
EMC certifications	FCC class B, CE class B, A-Tick, VCCI class B	FCC class B, CE class B, A-Tick, VCCI class B
<b>Mean Time Between Failures (MTBF)</b>		
Non-wireless	40.5 years	35.8 years
Wireless	22.8 years	28.9 years
<b>Security Certifications</b>		
Common Criteria: EAL4	Yes	Yes
FIPS 140-2: Level 2	Yes	Yes
ICSA Firewall and VPN	Yes	Yes
<b>Operating Environment</b>		
Operating temperature	32° to 104° F (0° to 40° C)	32° to 104° F (0° to 40° C)
Non-operating temperature	-4° to 149° F (-20° to 65° C)	-4° to 149° F (-20° to 65° C)
Humidity	10% to 90% noncondensing	10% to 90% noncondensing

## Specifications<sup>(1)</sup> (continued)

	SSG 5 Base/Extended	SSG 20 Base/Extended
<b>Wireless Radio Specifications (Wireless Models Only)</b>		
Transmit power	Up to 200 mW	Up to 200 mW
Wireless standards supported	Dual Radio 802.11 a + 802.11b/g	Dual Radio 802.11 a + 802.11b/g
Site survey	Yes	Yes
Maximum configured SSIDs	16	16
Maximum active SSIDs	4	4
Atheros SuperG	Yes	Yes
Atheros eXtended Range (XR)	Yes	Yes
Wi-Fi CERTIFIED®	Yes	Yes

## Wireless Security (Wireless Models Only)

Wireless privacy	WPA, WPA2 (AES or TKIP), IPsec VPN, WEP	WPA, WPA2 (AES or TKIP), IPsec VPN, WEP
Wireless authentication	PSK, EAP-PEAP, EAP-TLS, EAP-TTLS over 802.1x	PSK, EAP-PEAP, EAP-TLS, EAP-TTLS over 802.1x
MAC access controls	Permit or Deny	Permit or Deny
Client isolation	Yes	Yes

## Antenna Option (Wireless Models Only)

Diversity antenna	Included	Included
Directional antenna	Optional	Optional
Omni-directional antenna	Optional	Optional

(1) Some features and functionality only supported in releases greater than ScreenOS 5.4.

(2) Performance, capacity and features listed are based upon systems running ScreenOS 6.2 and are the measured maximums under ideal testing conditions unless otherwise noted. Actual results may vary based on ScreenOS release and deployment. For a complete list of supported ScreenOS versions for SSG platforms, please visit the Juniper Customer Support Center (<http://www.juniper.net/customers/support/>) and click on ScreenOS Software Downloads

(3) 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.

(4) 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.

(5) 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.

(6) 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.

(7) Active/passive and active/active High Availability requires the purchase of an Extended License. In addition to the HA features, an Extended License key increases a subset of the capacities as outlined below. Active/active HA is only supported in ScreenOS 6.0 or greater releases.

## 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 5 and SSG 20:

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, etc.)	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

## Firewall Extended Licenses

Extended License Feature	SSG 20 and SSG 5
Sessions	Increases max from 8,000 to 16,000
VPN Tunnels	Increases max from 25 to 40
VLANs	Increases max from 10 to 50
VoIP Calls	Increases max from 64 to 96
High Availability	Adds support for stateful active/active or active/passive with ScreenOS 6.0 and above

## Ordering Information

Part Number	SSG 5
SSG-5-SB	SSG 5 with 128 MB Memory, RS232 Serial backup interface
SSG-5-SB-BT	SSG 5 with 128 MB Memory, ISDN BRI S/T backup interface
SSG-5-SB-M	SSG 5 with 128 MB Memory, v.92 backup interface
SSG-5-SB-W-xx	SSG 5 with 128 MB Memory, RS232 Serial backup interface, 802.11a/b/g Wireless
SSG-5-SB-BTW-xx	SSG 5 with 128 MB Memory, ISDN BRI S/T backup interface, 802.11a/b/g Wireless
SSG-5-SB-MW-xx	SSG 5 with 128 MB Memory, v.92 backup interface, 802.11a/b/g Wireless
SSG-5-SH	SSG 5 with 256 MB Memory, RS232 Serial backup interface
SSG-5-SH-BT	SSG 5 with 256 MB Memory, ISDN BRI S/T backup interface
SSG-5-SH-M	SSG 5 with 256 MB Memory, v.92 backup interface
SSG-5-SH-W-xx	SSG 5 with 256 MB Memory, RS232 Serial backup interface, 802.11a/b/g Wireless
SSG-5-SH-BTW-xx	SSG 5 with 256 MB Memory, ISDN BRI S/T backup interface, 802.11a/b/g Wireless
SSG-5-SH-MW-xx	SSG 5 with 256 MB Memory, v.92 backup interface, 802.11a/b/g Wireless
Part Number	SSG 20
SSG-20-SB	SSG 20 with 128 MB Memory, 2-port Mini-PIM slots
SSG-20-SB-W-xx	SSG 20 with 128 MB Memory, 2-port Mini-PIM slots, 802.11a/b/g Wireless
SSG-20-SH	SSG 20 with 256 MB Memory, 2-port Mini-PIM slots
SSG-20-SH-W-xx	SSG 20 with 256 MB Memory, 2-port Mini-PIM slots, 802.11a/b/g Wireless
Part Number	SSG 20 I/O Options
JXM-1SERIAL-S	1-port Serial Mini Physical Interface Module*
JXM-1SFP-S	1-port SFP Mini Physical Interface Module**
JXM-1T1-S	1-port T1 Mini Physical Interface Module
JXM-1E1-S	1-port E1 Mini Physical Interface Module
JXM-1ADSL2-A-S	1-port ADSL2+ Annex A Mini Physical Interface Module
JXM-1ADSL2-B-S	1-port ADSL2+ Annex B Mini Physical Interface Module
JXM-1V92-S	1-port v.92 Mini Physical Interface Module
JXM-1BRI-ST-S	1-port ISDN S/T BRI Mini Physical Interface Module
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

\* The Serial Mini-PIM is only supported in ScreenOS 6.0 or greater releases

\*\* The SFP Mini-PIM is only supported in ScreenOS 6.0 or greater releases



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 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  
 Fax: 35.31.8903.601

Copyright 2008 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. JUNOSe is a trademark 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.

100176-010 Dec 2008

Part Number	SSG 20 I/O Options (cont'd)
JX-SFP-1GE-T	Small Form Factor Pluggable 1000BASE-T Gigabit Ethernet Copper Transceiver Module
JX-SFP-1FE-FX	Small Form Factor Pluggable 100BASE-FX Fast Ethernet Optical Transceiver Module

Part Number	SSG 5 / SSG 20 Accessories & Upgrades
SSG-5-ELU	Extended License Upgrade Key for SSG 5
SSG-20-ELU	Extended License Upgrade Key for SSG 20
SSG-5-20-MEM-256	SSG 5 and SSG 20 256 MB Memory Upgrade Module
SSG-5-RMK	SSG 5 Rack Mount Kit - holds 2 units
SSG-20-RMK	SSG 20 Rack Mount Kit
SSG-ANT	SSG Wireless Replacement Antenna
SSG-ANT-DIR	SSG 5 and SSG 20 Dual Band Directional Antenna
SSG-ANT-OMNI	SSG 5 and SSG 20 Dual Band Omni-Directional Antenna
SSG-CBL-ANT-10M	10 meters (30 feet) Low Loss Cable for SSG-ANT-XXX

Part Number	Unified Threat Management/Content Security (High Memory Option Required)
NS-K-AVS-SSG5	Antivirus (incl. anti-spyware, anti-phishing)
NS-K-AVS-SSG20	
NS-DI-SSG5	IPS (Deep Inspection)
NS-DI-SSG20	
NS-WF-SSG5	Web Filtering
NS-WF-SSG20	
NS-SPAM-SSG5	Anti-spam
NS-SPAM-SSG20	
NS-RBO-CS-SSG5	Remote Office Bundle (Includes AV, DI, WF)
NS-RBO-CS-SSG20	
NS-SMB-CS-SSG5	Main Office Bundle (Includes AV, DI, WF, AS)
NS-SMB-CS-SSG20	

- Note: The appropriate power cord is included based upon the sales order "Ship To" destination.
- Note: XX denotes Region Code for Wireless devices. Not all countries are supported. Please see Wireless Country Compliance Matrix for certified countries. <http://www.juniper.net/products/integrated/dsheet/800003.pdf>
- Note: For renewal of Content Security Subscriptions, add "-R" to above SKUs.
- Note: For 2 year Content Security Subscriptions, add "-2" to above SKUs.
- Note: For 3 year Content Security Subscriptions, add "-3" to above SKUs.

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