Juniper Networks **SSG 5 and SSG 20**

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 office and small business deployments. Traffic flowing in and out of the branch office can be 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 rich set of UTM security features allows the SSG 5 and SSG 20 to be deployed as a stand alone network protection device. With its robust routing engine, the SSG 5 and SSG 20 can also be deployed as a traditional branch office router or as a combination security and routing device to help reduce IT capital and operational expenditures. The SSG 5 and SSG 20 provide customers with the following features and benefits:

- Extensible I/O architecture that delivers fixed LAN connectivity plus WAN I/O options on top of unmatched security to reduce costs and extend investment protection.
- UTM security features backed by best-in-class security partners to ensure that the network is protected against all manner of attacks.
- Advanced security features such as network segmentation allows administrators to deploy security policies to isolate guests, wireless networks and regional servers or databases to prevent unauthorized access and contain any attacks that may occur.
- Dedicated, security specific processing hardware and software platform delivers performance required to protect high speed LAN as well as lower speed WAN connections.

Used by enterprises, service providers and stand alone businesses alike, the SSG 5 and SSG 20 are ideally suited for locations that are smaller, with fewer employees yet still require advanced security and routing features to protect business critical traffic traversing the WAN and high speed internal networks. Typical deployments include small businesses, distributed branch offices, retail outlets, and fixed telecommuter environments.

SSG 5:
The SSG 5 is a fixed form factor platform that delivers 160 Mbps of Stateful firewall traffic and 40 Mbps of IPSec VPN throughput. The SSG 5 Series is equipped with seven on-board 10/100 interfaces with optional fixed WAN ports (ISDN BRI S/T, V.92 or RS-232 Serial/Aux). Optional support for 802.11 a/b/g and a broad array of wireless specific security allow the SSG 5 to consolidate security, routing and wireless access point into a single device.

SSG 20:
The SSG 20 is a modular platform that delivers 160 Mbps of Stateful firewall traffic and 40 Mbps of IPSec VPN throughput. The SSG 20 is equipped with five on-board 10/100 interfaces with two I/O expansion slots that support I/O cards, such as ADSL2+, T1, E1, ISDN BRI S/T, V.92 for additional WAN connectivity. Optional support for 802.11 a/b/g and a broad array of wireless specific security allow the SSG 20 to consolidate security, routing and wireless access point into a single device.

Security
Proven Stateful firewall and IPSec VPN combined with best-in-class UTM security features including IPS (Deep Inspection), Antivirus (includes Anti-Spyware, Anti-Adware, Anti-Phishing), Anti-Spam, and Web Filtering protects both LAN and WAN traffic from worms, Spyware, Trojans, malware and other emerging attacks.

LAN/WAN connectivity
The combination of LAN/WAN connectivity options and supporting protocols provides customers with the ability to deploy the SSG 5 or SSG 20 as a traditional LAN-based firewall or as a consolidated routing and security device, thereby reducing TCO.

Network segmentation
The SSG 5 and SSG 20 provide an advanced set of network segmentation features such as Security Zones, Virtual Routers and VLANs that allow administrators to deploy different levels of security to different user groups by dividing the network into distinct, secure domains, each with their own security policy.

Seamlessly transform your network
Whether you are deploying a few SSGs to your local offices or implementing thousands around the world, Juniper Networks Professional Services can help. From simple lab testing to major network implementations, we can identify the goals, define the deployment process, create or validate the network design, and manage the deployment. We collaborate with your team to transform your network infrastructure to ensure that it is flexible, scalable, reliable, and secure.

	SSG 20	SSG 5
Maximum Performance and Capacity[1]		
ScreenOS version support	ScreenOS 5.4	ScreenOS 5.4
Firewall performance (Large packets)	160 Mbps	160 Mbps
Firewall performance[2] (IMIX)	90 Mbps	90 Mbps
Firewall Packets per second (64 byte)	30,000	30,000
VPN performance (3DES + SHA-1)	40 Mbps	40 Mbps
Concurrent sessions	4,000	4,000
New sessions/second	2,800	2,800
Policies	200	200
Users supported	Unrestricted	Unrestricted
Network Connectivity		
Fixed I/O	5x 10/100	7x 10/100
Physical Interface Module (Mini-PIM) Slots	2	0
WAN interface options	ADSL2 +, T1, E1, ISDN BRI S/T, V.92 (See Mini-PIM datasheets)	ISDN BRI S/T or RS-232 Serial/Aux or V.92 (factory configured)
LAN interface options	None	None
Wireless networking	Dual Radio 802.11a + 802.11b/g (factory configured)	
Firewall		
Network attack detection	Yes	Yes
DoS and DDoS protection	Yes	Yes
TCP reassembly for fragmented packet protection	Yes	Yes
Malformed packet protection	Yes	Yes
Unified Threat Management/Content Security[3]		
IPS (Deep Inspection FW)	Yes	Yes
Protocol anomaly detection	Yes	Yes
Stateful protocol signatures	Yes	Yes
Antivirus	Yes	Yes
Signature database	100,000 +	
Protocols scanned	POP3, SMTP, HTTP, IMAP, FTP	
Anti-Phishing	Yes	Yes
Anti-Spyware	Yes	Yes
Anti-Adware	Yes	Yes
Anti-Keylogger	Yes	Yes
Anti-Spam	Yes	Yes
Integrated URL filtering	Yes	Yes
External URL filtering[4]	Yes	Yes
VoIP Security		
H.323. ALG	Yes	Yes
SIP ALG	Yes	Yes
SCCP ALG	Yes	Yes
MGCP ALG	Yes	Yes
NAT for SIP, H.323, MGCP, SCCP	Yes	Yes
VPN		
Concurrent VPN tunnels	25	25
Tunnel interfaces	10	10
DES (56-bit), 3DES (168-bit) and AES encryptions	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
Redundant VPN gateways	Yes	Yes

	SSG 20	SSG 5
Firewall and VPN User Authentication		
Built-in (internal) database - user limit	Up to 100	Up to 100
3rd Party user authentication	RADIUS, RSA SecurID, and LDAP	
XAUTH VPN authentication	Yes	Yes
Web-based authentication	Yes	Yes
802.1X authentication	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	Yes	Yes
Virtual IP	Yes	Yes
Routing		
BGP	Yes	Yes
OSPF	Yes	Yes
RIPv1/v2	Yes	Yes
Static routes	Yes	Yes
Source-based routing	Yes	Yes
Policy-based routing	Yes	Yes
ECMP	Yes	Yes
Routes	1,024	1,024
Multicast	Yes	Yes
Reverse Forwarding Path (RFP)	Yes	Yes
IGMP (v1, v2)	Yes	Yes
IGMP Proxy	Yes	Yes
PIM SM	Yes	Yes
PIM SSM	Yes	Yes
Mcast inside IPSec Tunnel	Yes	Yes
Encapsulations		
PPP	Yes	Yes
MLPPP	Yes	N/A
Frame Relay	Yes	N/A
MLFR (FRF 15, FRF 16)	Yes	N/A
HDLC	Yes	N/A
Traffic Management (QoS)		
Guaranteed bandwidth	Yes	Yes
Maximum bandwidth	Yes	Yes
Ingress Traffic Policing	Yes	Yes
Priority-bandwidth utilization	Yes	Yes
DiffServ stamp	Yes, per policy	Yes, per policy
Wi-Fi Multi-Media (WMM)	Yes (with WLAN)	Yes (with WLAN)
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	
NetScreen-Security Manager	Yes	Yes
All management via VPN tunnel on any interface	Yes	Yes
SNMP full custom MIB	Yes	Yes
Rapid deployment	Yes	Yes
Logging and Monitoring		
Syslog (multiple servers)	External, up to 4 servers	
E-mail (2 addresses)	Yes	Yes
NetIQ WebTrends	External	External
SNMP (v2)	Yes	Yes
Traceroute	Yes	Yes
VPN tunnel monitor	Yes	Yes

	SSG 20	SSG 5
Virtualization		
Maximum number of configurable security zones	8	8
Maximum number of virtual routers	3	3
Maximum number of 802.1q VLANs	10	10
High Availability (HA)[6]		
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
IP Address Assignment		
Static	Yes	Yes
DHCP, PPPoE client	Yes	Yes
Internal DHCP server	Yes	Yes
DHCP relay	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	
Administration		
Local administrators database size	20	20
External administrator database	RADIUS/LDAP/SecurID	
Root Admin, Admin, and Read Only user levels	Yes	Yes
Software upgrades	TFTP / WebUI / NSM / SCP / USB	
Configuration Roll-back	Yes	Yes
External Flash		
Additional log storage	via USB	
Event logs and alarms	Yes	Yes
System config script	Yes	Yes
ScreenOS Software	Yes	Yes
Dimensions and Power		
Dimensions (W/L/H)	11 5/8" x 7 3/8" x 1 3/4" 29.5cm x 18.7cm x 4.5cm	8 3/4" x 5 5/8" x 1 5/8" 22.2cm x 14.3cm x 4.1cm
Weight	3.3 lbs (1.5 kg)	2.1 lbs (0.95 kg)
Rack mountable	Yes	Yes
Power Supply (AC)	100-240 VAC	100-240 VAC
Certifications		
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
Environment		
Temp and Humidity		
Operating Temp	0 to 40 Deg C (32 to 104 Deg F)	0 to 40 Deg C (32 to 104 Deg F)
Non-Operating Temp	-20 to 65 Deg C (-4 to 149 Deg F)	-20 to 65 Deg C (-4 to 149 Deg F)
Humidity	10 to 90% non-condensing	10 to 90% non-condensing
MTBF (Bellcore model)		
Non-Wireless	35.8 Yrs	40.5 Yrs
Wireless	28.9 Yrs	22.8 Yrs

	SSG 20	SSG 5
Wireless Radio Specifications (Wireless Models Only)		
Transmit Power	Up to 200mW	
Wireless Standards supported	Dual Radio 802.11 a + 802.11b/g	
Site Survey	Yes	
Maximum Configured SSIDs	16	
Maximum Active SSIDs	4	
Atheros SuperG	Yes	
Atheros eXtended Range (XR)	Yes	
Wi-Fi CERTIFIED®	Yes	
Wireless Security (Wireless Models Only)		
Wireless Privacy	WPA, WPA2 (AES or TKIP), IPSEC VPN, WEP	
Wireless Authentication	PSK, EAP-PEAP, EAP-TLS, EAP-TTLS over 802.1x	
MAC Access Controls	Permit or Deny	
Client Isolation	Yes	
Antenna Option (Wireless Models Only)		
Diversity Antenna	Included	
Directional Antenna	Future	
Omni-directional Antenna	Future	

(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 to a secondary server and therefore entails purchasing 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.

(6) Active Passive and HA Lite require 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.

Extended License Feature	SSG 20 and SSG 5
Sessions	Increases max from 4000 to 8000
VPN Tunnels	Increases max from 25 to 40
VLANS	Increases max from 10 to 50
VoIP Calls	Increases max from 32 to 48
High Availability	Adds support for Stateful Active/Passive and/or HA Lite

IPS (Deep Inspection FW) 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 SG 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

Ordering Information

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

Product	Part Number
SSG 5 / SSG 20 Accessories & Upgrades	
Extended License Upgrade Key for SSG 5	SSG-5-ELU
Extended License Upgrade Key for SSG 20	SSG-20-ELU
SSG 5 and SSG 20 256MB Memory Upgrade Module	SSG-5-20-MEM-256
SSG 5 Rack Mount Kit - holds 2 units	SSG-5-RMK
SSG 20 Rack Mount Kit	SSG-20-RMK
SSG Wireless Replacement Antenna	SSG-ANT
Unified Threat Management/Content Security (High Memory Option Required)	
Anti-Virus (Anti-Spyware, Anti-Phishing)	NS-K-AVS-SSG5
	NS-K-AVS-SSG20
IPS (Deep Inspection)	NS-DI-ISG-SSG5
	NS-DI-ISG-SSG20
Web Filtering	NS-WF-SSG5
	NS-WF-SSG20
Anti-Spam	NS-SPAM-SSG5
	NS-SPAM-SSG20
Remote Office Bundle (Includes AV, DI, WF)	NS-RBO-CS-SSG5
	NS-RBO-CS-SSG20
Main Office Bundle (Includes AV, DI, WF, AS)	NS-SMB-CS-SSG5
	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. www.jnpr.net/products/integrated/ssg_5_20.html
- Note: For 2nd year renewal of Content Security Subscriptions add "-R" to above SKUs.

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

100176-002 Oct 2006