SSG140 SECURE SERVICES GATEWAY

Product Overview

The SSG140 Secure Services Gateway is a purpose-built security appliance that delivers a perfect blend of performance, security, routing and LAN/WAN connectivity for medium sized branch offices and 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 security features that include stateful firewall, IPsec VPN, intrusion prevention system (IPS), antivirus (includes antispyware, antiadware, antiphishing), antispam and Web filtering.

Product Description

The Juniper Networks® SSG140 Secure Services Gateway is a high-performance security platform for branch offices and small/medium sized standalone businesses that want to stop internal and external attacks, prevent unauthorized access, and achieve regulatory compliance. The SSG140 is a modular platform that delivers more than 350 Mbps of stateful firewall traffic and 100 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 SSG140 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 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 SSG140 supports ten on-board interfaces (eight 10/100 plus two 10/100/1000) complemented by four I/O expansion slots that can house additional WAN interfaces (T1, E1, ISDN BRI S/T and Serial), making the SSG140 the most extensible security platform in its class. This broad array of I/O options coupled with WAN protocol and encapsulation support in its routing engine make the SSG140 a platform that can easily be deployed as a traditional branch office router or as a consolidated security and routing device to reduce CapEx and OpEx.

Access Control Enforcement: The SSG140 can act as an enforcement point in a Juniper Networks Unified Access Control (UAC) deployment with the simple addition of the

IC Series UAC appliance. The IC Series functions as a central policy management engine, interacting with the SSG140 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.
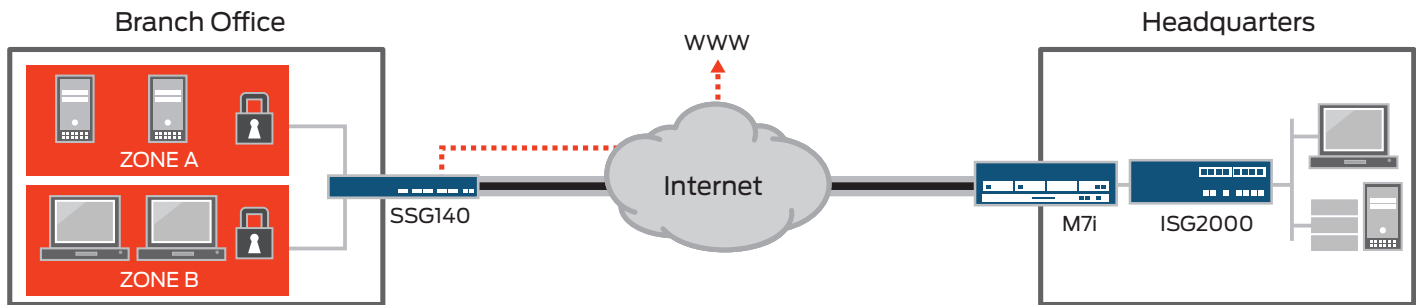
The SSG140 deployed at a branch office for secure Internet connectivity and site-to-site VPN to corporate headquarters. Internal branch office resources are protected with unique security policies for each security zone.

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, 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 IPS (Deep Inspection)	Annually licensed IPS engine.	Prevents application-level attacks from flooding the network.
Fixed Interfaces	Eight fixed 10/100 interfaces and two 10/100/1000 interfaces, one USB port, one console port, and one auxiliary port.	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.
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.
High interface density	Eight 10/100 plus two 10/100/1000 interfaces plus a console and an Aux interface for management.	Provides unmatched interface density when compared to competitive offerings.
Interface modularity	Four SSG140 interface expansion slots support optional T1, E1, ISDN BRI S/T, ADSL2+, G.SHDSL and serial physical interface modules (PIMs), and 10/100/1000 and SFP universal PIMs (uPIMs).**	Delivers LAN and WAN connectivity options on top of unmatched security to reduce costs and extend investment protection.
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.
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.
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.
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.

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

Product Options

OPTION	OPTION DESCRIPTION	APPLICABLE PRODUCTS
DRAM	The SSG140 is available with either 256 MB or 512 MB of DRAM.	SSG140
Unified Threat Management/ Content Security (high memory option required)	The SSG140 can be configured with any combination of the following best-in-class UTM and content security functionality: antivirus (includes antispyware, antiphishing), IPS (Deep Inspection), Web filtering, and/or antispam.	SSG140 high memory model only
I/O options	Four SSG140 interface expansion slots support optional T1, E1, ISDN BRI S/T, ADSL2+, G.SHDSL and serial physical interface modules (PIMs), and 10/100/1000 and SFP universal PIMs (uPIMs).	SSG140

SSG140

Specifications

Maximum Performance and Capacity[1]

ScreenOS® version tested	ScreenOS 6.2
Firewall throughput (large packets)	350+ Mbps
Firewall throughput (IMIX)[2]	300 Mbps
Firewall packets per second (64 byte)	90,000 PPS
Advanced Encryption Standard (AES) 256+SHA-1 VPN throughput	100 Mbps
3DES encryption +SHA-1 VPN throughput	100 Mbps
Maximum concurrent sessions	48,000
New sessions/second	8,000
Maximum security policies	1,000
Maximum users supported	Unrestricted

Network Connectivity

Fixed I/O	8x10/100, 2x10/100/1000
Physical Interface Module (PIM) slots	4
Modular WAN/LAN interface options (PIMs/ uPIMs)	2xT1, 2xE1, 2xSerial, 1xISDN BRI S/T SFP, 10/100/1000

Firewall

Network attack detection	Yes
DoS and DDoS protection	Yes
TCP reassembly for fragmented packet protection	Yes
Brute force attack mitigation	Yes
SYN cookie protection	Yes
Zone-based IP spoofing	Yes
Malformed packet protection	Yes

Unified Threat Management[3]

IPS (Deep Inspection firewall)	Yes
Protocol anomaly detection	Yes
Stateful protocol signatures	Yes
IPS/DI attack pattern obfuscation	Yes
Antivirus	Yes

Unified Threat Management[3] (continued)

Signature database	200,000+
Protocols scanned	POP3, HTTP, SMTP, IMAP, FTP, IM
Antispyware	Yes
Antiadware	Yes
Anti-keylogger	Yes
Instant message AV	Yes
Antispam	Yes
Integrated URL filtering	Yes
External URL filtering[4]	Yes

VoIP Security

H.323. Application-level gateway (ALG)	Yes
SIP ALG	Yes
MGCP ALG	Yes
SCCP ALG	Yes
Network Address Translation (NAT) for VoIP protocols	Yes

IPsec VPN

Concurrent VPN tunnels	500
Tunnel interfaces	50
DES encryption (56-bit), 3DES encryption (168-bit) and AES (256-bit)	Yes
MD-5 and SHA-1 authentication	Yes
Manual key, Internet Key Exchange (IKE), IKEv2 with EAP public key infrastructure (PKI) (X.509)	Yes
Perfect forward secrecy (DH Groups)	1,2,5
Prevent replay attack	Yes
Remote access VPN	Yes
Layer 2 Tunneling Protocol (L2TP) within IPsec	Yes
IPsec Network Address Translation (NAT) traversal	Yes
Auto-Connect VPN	Yes
Redundant VPN gateways	Yes

User Authentication and Access Control

Built-in (internal) database user limit	250
Third-party user authentication	RADIUS, RSA SecureID, LDAP
RADIUS Accounting	Yes – start/stop
XAUTH VPN authentication	Yes
Web-based authentication	Yes
802.1X authentication	Yes
Unified Access Control (UAC) enforcement point	Yes

Specifications (continued)

PKI Support

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

Virtualization

Maximum number of security zones	40
Maximum number of virtual routers	6
Bridge groups*	Yes
Maximum number of VLANs	100

Routing

BGP instances	6
BGP peers	24
BGP routes	2,048
OSPF instances	3
OSPF routes	2,048
RIPv1/v2 instances	64
RIP v2 routes	2,048
Static routes	2,048
Source-based routing	Yes
Policy-based routing	Yes
Equal-cost multipath (ECMP)	Yes
Multicast	Yes
Reverse Forwarding Path (RFP)	Yes
Internet Group Management Protocol (IGMP) (v1, v2)	Yes
IGMP Proxy	Yes
Protocol Independent Multicast (PIM) single mode	Yes
PIM source-specific multicast	Yes
Multicast inside IPsec tunnel	Yes

Encapsulations

Point-to-Point Protocol (PPP)	Yes
Multilink Point-to-Point Protocol (MLPPP)	Yes
MLPPP max physical interfaces	4
Frame relay	Yes

Encapsulations (continued)

Multilink Frame Relay (MLFR) (FRF 15, FRF 16)	Yes
MLFR max physical interfaces	4
HDLC	Yes

IPv6

Dual stack IPv4/IPv6 firewall and VPN	Yes
IPv4 to/from IPv6 translations and encapsulations	Yes
Syn-Cookie and Syn-Proxy DoS Attack Detection	Yes
SIP, RTSP, Sun-RPC, and MS-RPC ALG's	Yes
RIPng	Yes
BGP	Yes
Transparent mode	Yes
NSRP	Yes
DHCPv6 Relay	Yes

Mode of Operation

Layer 2 (transparent) mode[5]	Yes
Layer 3 (route and/or NAT) mode	Yes

Address Translation

Network Address Translation (NAT)	Yes
Port Address Translation (PAT)	Yes
Policy-based NAT/PAT (L2 and L3 mode)	Yes
Mapped IP (MIP) (L3 mode)	1,500
Virtual IP (VIP) (L3 mode)	16
MIP/VIP Grouping (L3 mode)	Yes

IP Address Assignment

Static	Yes
Dynamic Host Configuration Protocol (DHCP),Point-to-Point Protocol over Ethernet (PPPoE) client	Yes
Internal DHCP server	Yes
DHCP relay	Yes

Traffic Management Quality of Service (QoS)

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

High Availability (HA)

Active/active - L3 mode	Yes
Active/passive - Transparent & L3 mode	Yes
Configuration synchronization	Yes
Session synchronization for firewall and VPN	Yes
Session failover for routing change	Yes
VRRP	Yes
Device failure detection	Yes
Link failure detection	Yes
Authentication for new HA members	Yes
Encryption of HA traffic	Yes

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

Specifications (continued)

System Management

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

Administration

Local administrator database size	20
External administrator database support	RADIUS, RSA SecureID, LDAP
Restricted administrative networks	6
Root Admin, Admin, and Read Only user levels	Yes
Software upgrades	TFTP, WebUI, NSM, SCP, USB
Configuration roll-back	Yes

Logging/Monitoring

System log (multiple servers)	Yes – up to 4 servers
Email (2 addresses)	Yes
NetIQ WebTrends	Yes
SNMP (v2)	Yes
SNMP full custom MIB	Yes
Traceroute	Yes
VPN tunnel monitor	Yes

External Flash

Additional log storage	USB 1.1
Event logs and alarms	Yes
System configuration script	Yes
ScreenOS Software	Yes

Dimensions and Power

Dimensions (W x H x D)	17.5 x 1.8 x 15 in (44.5 x 4.5 x 38.1 cm)
Weight	10.2 lb (4.63 kg)
Rack mountable	Yes, 1RU
Power supply (AC)	100-240 VAC, AC Input line frequency 50 Hz or 60 Hz AC system current rating 2 A
Maximum thermal output	580 BTU/hour (170 W)
Noise Level	48.8 dB

Certifications

Safety certifications	UL, CUL, CSA, CB
Electromagnetic compatibility (EMC) certifications	FCC class B, CE class B
Network Equipment Building System (NEBS)	No
Mean time between failures (MTBF) (Bellcore model)	16 years

Security Certifications

Common Criteria: EAL4	Future
FIPS 140-2: Level 2	Future
ICSA Firewall and VPN	Yes

Operating Environment

Operating temperature	32º to 122º F (0º to 50º C)
Non-operating temperature	-4º to 158º F (-20º to 70º C)
Humidity	10% to 90% noncondensing

(1) 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 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.

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 SSG140:

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 (for example desktops)	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

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services and support, which are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to bring revenue-generating capabilities online faster so you can realize bigger productivity gains and faster rollouts of new business models and ventures. At the same time, Juniper Networks ensures operational excellence by optimizing your 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
SSG140	
SSG-140-SB	SSG140 with 256 MB memory, 0 PIM cards, AC power
SSG-140-SH	SSG140 with 512 MB memory, 0 PIM cards, AC power
SSG140 I/O Options	
JX-1BRI-ST-S	1-port ISDN BRI S/T PIM
JX-2E1-RJ48-S	2-port E1 PIM with integrated CSU/DSU
JX-2T1-RJ48-S	2-port T1 PIM with integrated CSU/DSU
JX-2Serial-S	2-port 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	1-port G.SHDSL PIM
JXU-6GE-SFP-S	6-port SFP Gigabit Ethernet Universal PIM*
JXU-1SFP-S	1-port SFP 100 Mbps or Gigabit Ethernet Universal PIM * (SFP sold separately)
JXU-8GE-TX-S	8-port Gigabit Ethernet 10/100/1000 Copper Universal PIM*
JXU-16GE-TX-S	16-port Gigabit Ethernet 10/100/1000 Copper Universal PIM*

* uPIMs are only supported in ScreenOS 6.0 or greater releases

MODEL NUMBER	DESCRIPTION
Unified Threat Management/Content Security (High Memory Option Required)	
NS-K-AVS-SSG140	Antivirus (antispyware, antiphishing)
NS-DI-SSG140	IPS (Deep Inspection)
NS-SPAM2-SSG140	Antispam
NS-WF-SSG140	Web filtering
NS-RBO-CS-SSG140	Remote Office Bundle (AV, IPS, WF)
NS-SMB2-CS-SSG140	Main Office Bundle (AV, IPS, WF, AS)

*uPIMs are only supported in ScreenOS 6.0 or greater releases

SSG140 Memory Upgrades, Spares and Communications Cables	
SSG-100-MEM-512	512 MB DIMM Memory upgrade
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, US
JX-Blank-FP-S	Blank I/O plate
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	35 cable (DTE)
JX-CBL-X21-DTE	X.21 cable (DTE)

Note: The appropriate power cord is included based upon the sales order "Ship To" destination

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**.

Printed on recycled paper