The Juniper Networks Secure Services Gateway 140 (SSG 140) 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 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 rich set of UTM security features allows the SSG 140 to be deployed as a stand alone network protection device. With its robust routing engine, the SSG 140 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 140 provides customers with the following features and benefits:

- Extensible I/O architecture that delivers LAN and WAN connectivity 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 140 is ideally suited for medium size offices that require advanced security and routing features to protect business critical traffic traversing the WAN and high speed LAN. Deployment examples include small to medium sized stand alone businesses and branch office environments.

The SSG 140 is a modular platform that delivers over 350 Mbps of Stateful firewall traffic and 100 Mbps of IPSec VPN. The SSG 140 supports 8 on-board 10/100 + 2 10/100/1000 interfaces and four I/O expansion slots that support T1, E1, ISDN BRI S/T, and Serial connectivity.

**Security**

Proven Stateful firewall and IPSec VPN combined with best-in-class UTM security features including IPS, 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 140 as a traditional LAN-based firewall or as a consolidated routing and security device, thereby reducing TCO.

**Network segmentation**

The SSG 140 provides 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.
**Juniper Networks Secure Services Gateway 140**

<table>
<thead>
<tr>
<th><strong>Maximum Performance and Capacity</strong>&lt;sup&gt;a,b&lt;/sup&gt;</th>
<th><strong>SSG 140</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>ScreenOS version support</td>
<td>ScreenOS 5.4</td>
</tr>
<tr>
<td>Firewall performance (Large packets)</td>
<td>350+ Mbps</td>
</tr>
<tr>
<td>Firewall performance (IMIX)</td>
<td>300 Mbps</td>
</tr>
<tr>
<td>Firewall packets per second (64 byte)</td>
<td>100,000 PPS</td>
</tr>
<tr>
<td>3DES + SHA-1 VPN performance</td>
<td>100 Mbps</td>
</tr>
<tr>
<td>Concurrent sessions</td>
<td>32,000</td>
</tr>
<tr>
<td>New sessions/second</td>
<td>8,000</td>
</tr>
<tr>
<td>Policies</td>
<td>500</td>
</tr>
<tr>
<td>Users supported</td>
<td>Unrestricted</td>
</tr>
</tbody>
</table>

**Network Connectivity**
- Fixed I/O: 8 10/100, 2 10/100/1000
- Physical Interface Module (PIM) Slots: 4
- WAN interface options: 2xT1, 2xE1, 1xISDN BRI S/T, 2xSerial

**Mode of Operation**
- Layer 2 (transparent) mode: 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: Yes
- Mapped IP: Yes
- Virtual IP: Yes

**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/Content Security**<sup>c</sup>
- IPS (Deep Inspection FW): Yes
- Protocol anomaly detection: Yes
- Stateful protocol signatures: Yes
- IPS/DI attack pattern obfuscation: Yes
- Antivirus: Yes
- Signature database: 100,000+
- Protocols scanned: POP3, SMTP, HTTP, IMAP, FTP
- Anti-Spyware: Yes
- Anti-Adware: Yes
- Anti-Keylogger: Yes
- Anti-Spam: Yes
- Integrated URL filtering: Yes
- External URL filtering: Yes

**VoIP Security**
- H.323 ALG: Yes
- SIP ALG: Yes
- MGCP: Yes
- SCCP: Yes
- NAT for VoIP protocols: Yes

**Firewall and VPN User Authentication**
- Built-in (internal) database - user limit: 250
- 3rd Party user authentication: RADIUS, RSA SecurID, and LDAP
- XAUTH VPN authentication: Yes
- Web-based authentication: Yes
- 802.1X authentication: Yes

**Routing**
- BGP: Yes
- OSPF: Yes
- RIPv1/v2: Yes
- Dynamic routing: Yes
- Static routes: Yes
- Source-based routing: Yes
- Policy-based routing: Yes
- ECMP: Yes
- Routes: 2048
- Multicast: Yes
- Reverse Forwarding Path (RFP): Yes
- IGMP (v1, v2): Yes
- IGMP Proxy: Yes
- PIM SM: Yes
- PIM SSM: Yes
- Mcast inside IPSec Tunnel: Yes

**Encapsulations**
- PPP: Yes
- MLPPP: Yes
- MLPP max physical interfaces: 8
- Frame Relay: Yes
- MLFR (FRF 15, FRF 16): Yes
- MLFR max physical interfaces: 8
- HDLC: Yes

**Traffic Management (QoS)**
- Guaranteed bandwidth: Yes
- Maximum bandwidth: Yes, per physical interface
- Ingress Traffic Policing: Yes
- Priority-bandwidth utilization: Yes
- DiffServ stamp: Yes, per policy

**System Management**
- WebUI (HTTP and HTTPS): Yes
- Command Line Interface (console): Yes
- Command Line Interface (telnet): Yes
- Command Line Interface (SSH): Yes
- NetScreen-Security Manager: Yes
- All management via VPN tunnel on any interface: Yes
- SNMP full custom MIB: Yes
- Rapid deployment: No

**Logging and Monitoring**
- Syslog (multiple servers): Yes
- E-mail (2 addresses): Yes
- NetIQ WebTrends: External
- SNMP (v2): Yes
- Traceroute: Yes
- VPN tunnel monitor: Yes
Virtualization
Maximum number of security zones: 40
Maximum number of virtual routers: 3
Number of VLANs supported: 100

High Availability (HA)
Dedicated HA interfaces: No
Active/Passive: Yes
Configuration synchronization: Yes
Session synchronization for firewall and VPN: Yes
Session failover for routing change: Yes
Device failure detection: Yes
Link failure detection: Yes
Authentication for new HA members: Yes
Encryption of HA traffic: Yes

IP Address Assignment
Static: Yes
DHCP, PPPoE client: Yes
Internal DHCP server: Yes
DHCP relay: Yes

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

Administration
Local administrators database: 20
External administrators database: RADIUS/LDAP/SecureID
Restricted administrative networks: 6
Root Admin, Admin, and Read Only user levels: Yes
Software upgrades: Yes
Configuration roll-back: Yes

External Flash
Additional log storage: USB 1.1
Event logs and alarms: Yes
System config script: Yes
ScreenOS Software: Yes

Dimensions and Power
Dimensions (H/W/L): 1.75" x 17.5" x 15"
Weight: 10.2 lbs
Rack mountable: Yes, 1 RU
Power Supply (AC): AC input voltage, operating range: 90 to 240 VAC
AC input line frequency: 50 or 60 Hz
AC system current rating: 2 A
Maximum thermal output: 580 BTU/hour (170 W)

Certifications
Safety Certifications: UL, CUL, CSA, CB
EMC Certifications: FCC class B, CE class B
C-Tick, VCCI class A
Environment: Operational temperature: 32° to 122° F, 0° to 50° C
Non-operational temperature: 4° to 158° F, -20° to 70° C
Humidity: 10 to 90% non-condensing
MTBF (Bellcore model): 16 years

(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) NAT, PAT, policy based NAT, virtual IP, mapped IP, virtual systems, virtual routers, VLANs, OSPF, BGP, PIP, SecureFCA, and IP address assignment are not available in layer 2 transparent mode.

(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 to a secondary server and therefore entails purchasing a separate Web filtering license from either Websense or SurfControl.

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 140:

<table>
<thead>
<tr>
<th>Signature Pack</th>
<th>Target Deployment</th>
<th>Defense Type</th>
<th>Type of Attack Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base</td>
<td>Branch Offices, small medium businesses</td>
<td>Client/Server and worm protection</td>
<td>Range of signatures and protocol anomalies</td>
</tr>
<tr>
<td>Client</td>
<td>Remote/Branch Offices</td>
<td>Perimeter defense, compliance for hosts (desktops, etc)</td>
<td>Attacks in the server-to-client direction</td>
</tr>
<tr>
<td>Server</td>
<td>Small/Medium Businesses</td>
<td>Perimeter defense, compliance for server infrastructure</td>
<td>Attacks in the client-to-server direction</td>
</tr>
<tr>
<td>Worm Mitigation</td>
<td>Remote/Branch Offices of Large enterprises</td>
<td>Most comprehensive defense against worm attacks</td>
<td>Worms, Trojans, backdoor attacks</td>
</tr>
</tbody>
</table>
**Ordering Information**

<table>
<thead>
<tr>
<th>Product</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSG 140 System, 256 MB memory, 0 PIM cards, AC power</td>
<td>SSG-140-SB</td>
</tr>
<tr>
<td>SSG 140 System, 512 MB memory, 0 PIM cards, AC power</td>
<td>SSG-140-SH</td>
</tr>
<tr>
<td><strong>SSG 140 I/O Options</strong></td>
<td></td>
</tr>
<tr>
<td>1 Port ISDN BRI S/T Interface</td>
<td>JX-1BRI-ST-S</td>
</tr>
<tr>
<td>2 Port E1 PIM with integrated CSU/DSU</td>
<td>JX-2E1-RJ48-S</td>
</tr>
<tr>
<td>2 Port T1 PIM with integrated CSU/DSU</td>
<td>JX-2T1-RJ48-S</td>
</tr>
<tr>
<td>2 Port Serial PIM</td>
<td>JX-2Serial-S</td>
</tr>
<tr>
<td><strong>Unified Threat Management/Content Security</strong> (High Memory Option Required)</td>
<td></td>
</tr>
<tr>
<td>Antivirus (Anti-Spyware, Anti-Phishing)</td>
<td>NS-K-AVS-SSG140</td>
</tr>
<tr>
<td>IPS (Deep Inspection)</td>
<td>NS-DI-SSG140</td>
</tr>
<tr>
<td>Anti-Spam</td>
<td>NS-SPOM-SSG140</td>
</tr>
<tr>
<td>Web Filtering</td>
<td>NS-WF-SSG140</td>
</tr>
<tr>
<td>Remote Office Bundle (AV, IPS, WF)</td>
<td>NS-ROBO-CS-SSG140</td>
</tr>
<tr>
<td>Main Office Bundle (AV, IPS, WF, AS)</td>
<td>NS-SMB-CS-SSG140</td>
</tr>
<tr>
<td><strong>SSG 140 Memory Upgrades, Spares and Communications Cables</strong></td>
<td></td>
</tr>
<tr>
<td>512 MB memory upgrade for the SSG 140</td>
<td>SSG-100-MEM-512</td>
</tr>
<tr>
<td>Power Cable, Australia</td>
<td>CBL-JX-PWR-AU</td>
</tr>
<tr>
<td>Power Cable, China</td>
<td>CBL-JX-PWR-CH</td>
</tr>
<tr>
<td>Power Cable, Europe</td>
<td>CBL-JX-PWR-EU</td>
</tr>
<tr>
<td>Power Cable, Italy</td>
<td>CBL-JX-PWR-IT</td>
</tr>
<tr>
<td>Power Cable, Japan</td>
<td>CBL-JX-PWR-JP</td>
</tr>
<tr>
<td>Power Cable, UK</td>
<td>CBL-JX-PWR-UK</td>
</tr>
<tr>
<td>Power Cable, US</td>
<td>CBL-JX-PWR-US</td>
</tr>
<tr>
<td>Blank I/O plate</td>
<td>JX-Blank-FP-S</td>
</tr>
<tr>
<td>EIA530 cable (DCE)</td>
<td>JX-CBL-EIA530-DCE</td>
</tr>
<tr>
<td>EIA530 cable (DTE)</td>
<td>JX-CBL-EIA530-DTE</td>
</tr>
<tr>
<td>RS252 cable (DCE)</td>
<td>JX-CBL-RS252-DCE</td>
</tr>
<tr>
<td>RS252 cable (DTE)</td>
<td>JX-CBL-RS252-DTE</td>
</tr>
<tr>
<td>RS449 cable (DCE)</td>
<td>JX-CBL-RS449-DCE</td>
</tr>
<tr>
<td>RS449 cable (DTE)</td>
<td>JX-CBL-RS449-DTE</td>
</tr>
<tr>
<td>V.35 cable (DCE)</td>
<td>JX-CBL-V35-DCE</td>
</tr>
<tr>
<td>V.35 cable (DTE)</td>
<td>JX-CBL-V35-DTE</td>
</tr>
<tr>
<td>X.21 cable (DCE)</td>
<td>JX-CBL-X21-DCE</td>
</tr>
<tr>
<td>X.21 cable (DTE)</td>
<td>JX-CBL-X21-DTE</td>
</tr>
</tbody>
</table>

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