Juniper Networks ISG Series

Juniper Networks™ Integrated Security Gateways (ISG) are ideally suited for securing enterprise, carrier, and data center environments where advanced applications, such as voice over IP (VoIP) and streaming media, demand consistent, scalable performance. The Juniper Networks ISG 1000 and ISG 2000 solutions are purpose-built security solutions that leverage a fourth-generation security ASIC, the GigaScreen3, along with high-speed microprocessors to deliver unmatched firewall and virtual private network (VPN) performance. Integrating best-in-class firewall, VPN, and optional Intrusion Detection and Prevention (IDP), the ISG 1000 and ISG 2000 enable secure, reliable connectivity along with network-and application-level protection for critical, high-traffic network segments.

Product Description

The Juniper Networks ISG 1000 and ISG 2000 are fully integrated firewall/VPN systems that offers multi-gigabit performance, modular architecture and rich virtualization capabilities. They are an ideal security solution for large enterprise, data center and service provider networks.

The ISG Series firewall/VPN-based systems deliver security features such as Intrusion Prevention System (IPS), anti-spam, Web filtering, and Internet Content Adaptation Protocol (ICAP) antivirus redirection support. The advanced system is further expandable with optionally integrated IDP or as a General Packet Radio Service (GPRS) firewall/VPN for mobile network service provider environments.

The ISG Series firewall/VPN modular architecture enables deployment with a wide variety of copper and fiber interface options. Highly flexible segmentation and isolation of traffic belonging to different trust levels can be achieved using advanced features such as virtual systems, virtual LANs, and security zones. The ISG Series firewall/VPN allows multiple, separate firewall inspection or routing policies to simplify network design. This enables the enforcement of security policies to traffic streams—even in highly complex environments—without significant impact on the network itself.

The flexibility and efficiency offered by the ISG Series architecture provides state-of-the-art performance and best-in-class functionality as a firewall/VPN or integrated firewall/VPN/IDP solution with optional security modules. The ISG 1000 supports up to two security modules, while the ISG 2000 can support up to three security modules. The security modules maintain their own dedicated processing and memory, and incorporate technology designed to accelerate IDP packet processing. This reduces the number of separate security devices and management applications, and simplifies deployment effort and network complexity. The result? Higher cost savings.

The ISG Series firewall/VPN with IDP utilizes the same award-winning software found on Juniper Networks IDP platforms. The IDP security module supports multi-method detection, combining eight different detection mechanisms—including stateful signatures and protocol anomaly detection. In addition to helping businesses defend against security threats such as worms, trojans, malware, spyware, and hackers, the ISG with IDP can provide information on rogue servers as well as types and versions of the applications and operating systems that may have inadvertently been added to the network. Application signatures go a step further by enabling administrators to maintain compliance and enforce corporate business policies with accurate detection of application traffic.

The ISG 1000 and ISG 2000 can be deployed in a number of different configurations to protect both the perimeter and internal network resources. When deployed in a mobile operator network, the ISG 1000 and ISG 2000 GPRS solutions are GPRS Tunneling Protocol (GTP) aware and fully support GTP functionality in virtual systems. The ISG Series firewall/VPN can be deployed at the Gp interface connection between two Public Land Mobile Networks (PLMN), the Gn interface connection between the SGSN and the GGSN support nodes, and the Gi interface connection between the GGSN and the Internet.

In addition to countering sophisticated threats, denial of service (DoS) attacks, and malicious users, the ISG Series GPRS firewall/VPN can limit messages, throttle bandwidth-hungry applications that consume uplink/downlink traffic, and perform 3GPP R6 IE removal to help retain interoperability in roaming between 2G and 3G networks.

Features and Benefits

Feature	Feature Description	Benefit
Purpose-built platform	Dedicated, security-specific processing hardware and software platform.	Delivers the required performance to protect high-speed LAN environments.
Predictable performance	ASIC-based architecture provides linear performance for all packet sizes at multi-gigabit speeds.	Ensures low latency in sensitive applications such as VoIP and streaming media.
System and network resiliency	Hardware component redundancy, multiple high availability options, and route-based VPNs.	Provides the reliability required for high-speed network deployments.
Best-in-class network security features	Embedded Web filtering, anti-spam, IPS, ICAP antivirus redirect, and optionally integrated IDP.	Additional security features backed by best-in-class security partners such as Symantec and SurfControl.
Interface flexibility	Modular architecture enables deployment with a wide variety of copper and fiber interface options.	Simplifies network integration and helps to reduce the cost of future network upgrades.
Network segmentation	Security zones, virtual LANs, and virtual routers allow administrators to deploy security policies to isolate guests and regional servers or databases.	Powerful capabilities facilitate deploying security for various internal, external, and DMZ subgroups on the network to prevent unauthorized access.
Centralized management	Centralized management of Juniper Networks firewall and IDP products enabled through NSM.	Tight integration across multiple platforms enables simple and intuitive network-wide security management.
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.
Comprehensive threat protection	Dedicated processing modules provide best-in-class multigigabit firewall/VPN/IDP capability in a single solution.	Unmatched performance ensures that the network is protected against all manner of attacks in high-speed networks.
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
Integrated anti-spam	Blocks unwanted email from known spammers and phishers, using an annually licensed anti-spam offering based on Symantec technology.	ISG 1000 & ISG 2000
Integrated IPS (Deep Inspection)	Prevents application level attacks from flooding the network using a combination of stateful signatures and protocol anomaly detection mechanisms. IPS is annually licensed.	ISG 1000 & ISG 2000
Integrated Web filtering	Blocks access to malicious Web sites using the annually licensed Web filtering solution based on SurfControl's market-leading technology.	ISG 1000 & ISG 2000
ICAP antivirus redirect	ICAP antivirus content redirection allows the implementation of a third-party/large-enterprise antivirus solution at the perimeter.	ISG 1000 & ISG 2000
Optionally integrated IDP	Dedicated IDP security modules enable high-speed packet inspection. Requires no network changes to add full IDP functionality, helping to protect against layer 4-7 attacks including zero-day, worms, trojans, and spyware, etc. Additional hardware and system upgrade required.	ISG 1000 & ISG 2000
Application Awareness/Identification	Includes use of contexts, protocol information and signatures to accurately identify applications on any port. Optional IDP security module required.	ISG 1000 & ISG 2000
GPRS firewall/VPN for mobile networks	Support for GPRS networks to provide stateful firewalling and filtering capabilities that mitigate a wide variety of attacks on the Gp, Gn, and Gi interfaces to protect key nodes within the mobile operators' network. Additional license required.	ISG 1000 & ISG 2000

Specifications

	Juniper Networks ISG 1000	Juniper Networks ISG 2000
Maximum Performance and Capacity[1]		
ScreenOS version tested	ScreenOS 6.2	ScreenOS 6.2
Firewall performance (large packets)	2 Gbps	4 Gbps
Firewall performance (small packets)	1 Gbps	2 Gbps
Firewall packets per second (64 byte)	1.5 M PPS	3 M PPS
AES256+SHA-1 VPN performance	1 Gbps	2 Gbps
3DES+SHA-1 VPN performance	1 Gbps	2 Gbps
Maximum concurrent sessions[3]	500,000	1,000,000
New sessions/second	20,000	23,000
Maximum security policies	10,000	30,000
Maximum users supported	Unrestricted	Unrestricted
Network Connectivity		
Fixed I/O	4 10/100/1000 ports	0
Interface expansion slots	2	4
LAN interface options	Up to 8 mini-GBIC (SX, LX, or TX), up to 8 10/100/1000, up to 20 10/100, up to 2 10GE	Up to 16 mini-GBIC (SX, LX, or TX), up to 8 10/100/1000, up to 28 10/100, up to 4 10GE
Firewall		
Network attack detection	Yes	Yes
Denial of service (DoS) and Distributed denial of service (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
Integrated IPS (Optional Integrated IDP)[2][10]		
Stateful protocol signatures	Yes	Yes
Attack detection mechanisms	Stateful signatures, traffic anomaly detection, protocol anomaly detection (zero-day coverage), backdoor detection	Stateful signatures, traffic anomaly detection, protocol anomaly detection (zero-day coverage), backdoor detection
Attack response mechanisms	Drop connection, close connection, session packet log, session summary, email, custom	Drop connection, close connection, session packet log, session summary, email, custom
Attack notification mechanisms	Session packet log, session summary, email, SNMP, system log, WebTrends	Session packet log, session summary, email, SNMP, system log, WebTrends
Worm protection	Yes	Yes
Simplified installation through recommended policies	Yes	Yes
Trojan protection	Yes	Yes
Spyware/adware/keylogger protection	Yes	Yes
Other malware protection	Yes	Yes
Protection against attack proliferation from infected systems	Yes	Yes
Reconnaissance protection	Yes	Yes
Request and response side attack protection	Yes	Yes
Compound attacks – combines stateful signatures and protocol anomalies	Yes	Yes
Create custom attack signatures	Yes	Yes
Access contexts for customization	500+	500+
Attack editing (port range, etc.)	Yes	Yes
Stream signatures	Yes	Yes
Protocol thresholds	Yes	Yes
Stateful protocol signatures	Yes	Yes
Approximate number of attacks covered	5,500+*	5,500+*
Detailed threat descriptions and remediation/patch info	Yes	Yes
Enterprise security profiler	Yes	Yes
Create and enforce appropriate application-usage policies	Yes	Yes
Attacker and target audit trail and reporting	Yes	Yes
Deployment modes	In-line or in-line TAP	In-line or in-line TAP
Frequency of updates	Daily and emergency	Daily and emergency

*As of November 2008, there are 5,560 signatures with approximately 10 new signatures added every week.

	Juniper Networks ISG 1000	Juniper Networks ISG 2000
Unified Threat Management/Content Security[5]		
Deep Inspection signature packs[4]	Yes	Yes
IPS (Deep Inspection firewall)[4]	Yes	Yes
Protocol anomaly detection	Yes	Yes
Stateful protocol signatures	Yes	Yes
IPS/Deep Inspection attack pattern obfuscation	Yes	Yes
ICAP antivirus redirection	Yes	Yes
Anti-spam	Yes	Yes
Integrated URL filtering	Yes	Yes
External URL filtering[6]	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
GPRS Security[10]		
GTP tunnels[7]	200,000	400,000
GTP packet inspection (IPS or IDP)	Yes	Yes
IPsec VPN		
Concurrent VPN tunnels[8]	2,000	10,000
Tunnel interfaces[8]	Up to 512	Up to 1,024
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), IKEv2 with EAP	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
User Authentication and Access Control		
Built-in (internal) database - user limit[8]	50,000	50,000
Third-party user authentication	Remote Authentication Dial In User Service (RADIUS), RSA SecurID, and 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

	Juniper Networks ISG 1000	Juniper Networks ISG 2000
Virtualization[10]		
Maximum number of virtual systems	0 default, upgradeable to 50	0 default, upgradeable to 250
Maximum number of security zones	20 default, upgradeable to 120	26 default, upgradeable to 526
Maximum number of virtual routers	3 default, upgradeable to 53	3 default, upgradeable to 253
Maximum number of VLANs	4,094	4,094
Routing		
BGP instances	8	64
BGP peers	128	128
BGP routes	10,000	20,000
OSPF instances	8	8
OSPF routes	4,096	6,000
RIP v1/v2 instances	Up to 12 instances supported	Up to 50 instances supported
RIP v2 tablesize	10,000	20,000
Dynamic routing	Yes	Yes
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
IPv6		
Dual stack IPv4/IPv6 firewall and VPN	Yes	Yes
Syn-cookie and Syn-proxy DoS attack detection	Yes	Yes
SIP, RTSP, Sun-RPC, and MS-RPC ALG's	Yes	Yes
IPv4 to/from IPv6 translations and encapsulations	Yes	Yes
Virtualization (VSYS, security zones, VR, VLAN)	Yes	Yes
RIPng	Yes	Yes
BGP version 4	Yes	Yes
DHCPv6 Relay	Yes	Yes
NSRP (Active/Passive and Active/Active)	Yes	Yes
Transport Mode for IPv6	Yes	Yes
Mode of Operation		
Layer 2 (transparent) mode[7]	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	4,096	8,192
Virtual IP (VIP)[9]	8	8
MIP/VIP grouping	Yes	Yes
IP Address Assignment		
Static	Yes	Yes
DHCP, PPPoE client	Yes, No	No, No
Internal DHCP server	Yes	No
DHCP relay	Yes	Yes

	Juniper Networks ISG 1000	Juniper Networks ISG 2000
Traffic Management Quality of Service (QoS)		
Maximum bandwidth	Yes - per physical interface only	Yes - per physical interface only
Jumbo frames	Yes[11]	Yes[11]
DiffServ marking	Yes - per policy	Yes - per policy
High Availability (HA)		
Active/active - transparent & L3 mode	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	Yes
NetScreen-Security Manager	Yes	Yes
All management via VPN tunnel on any interface	Yes	Yes
Rapid deployment	Yes	Yes
Administration		
Local administrator database size	256	256
External administrator database support	RADIUS, LDAP	RADIUS, LDAP
Restricted administrative networks	Yes	Yes
Root Admin, Admin, and Read Only user levels	Yes	Yes
Software upgrades	Yes	Yes
Configuration rollback	Yes	Yes
Logging/Monitoring		
Syslog (multiple servers)	Yes	Yes
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	Supports 1 GB or 2 GB industrial-grade SanDisk	Supports 1 GB or 2 GB industrial-grade SanDisk
Event logs and alarms	Yes	Yes
System configuration script	Yes	Yes
ScreenOS Software	Yes	Yes
Dimensions and Power		
Dimensions (W x H x D)	17.5 x 5.25 x 17.3 in (44.5 x 13.3 x 43.9 cm)	17.5 x 5.25 x 23 in (44.5 x 13.3 x 58.4 cm)
Weight	30 lb/14 kg	50 lb/23 kg
Rack-mountable	Yes, 3 U's	Yes, 3 U's
Power supply (AC)	Single, field upgradeable	Dual, redundant
Power supply (DC)	Single, field upgradeable	Dual, redundant
Maximum thermal output	444 BTU/hour (W)	537 BTU/hour (W)

	Juniper Networks ISG 1000	Juniper Networks ISG 2000
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	Yes	Yes
MTBF (Bellcore model)	7.6 years	7.6 years
Security Certifications		
Common Criteria: EAL4 and EAL4+	Yes	Yes
FIPS 140-2: Level 2	Yes	Yes
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% noncondensing	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 by deployment. For a complete list of supported ScreenOS versions for ISG 1000 and ISG 2000 platforms, please visit the Juniper Customer Support Center (http://www.juniper.net/customers/support/).

(2) Additional IDP license and hardware upgrade required.

(3) Concurrent sessions listed are based upon maximums with current shipping ISG hardware. Older ISG units may need the optional memory upgrade to achieve maximum concurrent session capacity. Firewall/VPN concurrent sessions maximum for older ISG units without the optional memory upgrade are 250,000 for the ISG 1000 and 500,000 for the ISG 2000. Older ISG units with the optional IDP upgrades installed already have the maximum concurrent session capacity and do not require a memory upgrade.

(4) IPS (Deep Inspection firewall) is automatically disabled when optionally integrated IDP is installed.

(5) Security features (IPS/Deep Inspection, anti-spam and Web filtering) are delivered by annual subscriptions purchased separately from Juniper Networks. Annual subscriptions provide signature updates and associated support.

(6) Redirect Web filtering sends traffic to a secondary server and therefore entails purchasing a separate Web filtering license from either Websense or SurfControl.

(7) 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.

(8) Shared among all virtual systems.

(9) Not available with virtual systems.

(10) Additional license required.

(11) Requires 4-port mini GBIC modules - NS-ISG-SX4, NS-ISG-LX4 or NS-ISG-TX4.

Licensing Options

The ISG 1000 and ISG 2000 are available with two licensing options to provide two different levels of functionality and capacity:

- **Advanced Models**: the Advanced software license provides all of the features and capacities listed within this spec sheet.
- **Baseline Models**: the Baseline software license provides an entry-level solution for customer environments where features such as Deep Inspection, OSPF and BGP dynamic routing, advanced High Availability, and full capacity are not critical requirements.

The following table shows the features and capacities that differ between the Baseline and Advanced models:

	Baseline		Advanced	
	ISG 1000	**ISG 2000**	**ISG 1000**	**ISG 2000**
Sessions	125,000	256,000	500,000	1,000,000
Concurrent VPN tunnels	1,000	1,000	2,000	10,000
Deep inspection Firewall	No	No	Yes	Yes
VLANs	50	100	4,094	4,094
OSPF/BGP	No	No	Yes	Yes
High availability (HA)	A/P	A/P	A/A	A/A
Integrated IDP	No	No	Optional upgrade	Optional upgrade
GTP inspection	No	No	Optional upgrade	Optional upgrade

Performance-Enabling 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, faster rollouts of new business models and ventures, and greater market reach, while generating higher levels of customer satisfaction. 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/products_and_services.

Ordering Information

ISG 1000 Systems	Part Number
NS-ISG-1000 system (inc. AC power supply, no I/O cards)	NS-ISG-1000
NS-ISG-1000 system (inc. DC power supply, no I/O cards)	NS-ISG-1000-DC
NS-ISG-1000 baseline system (inc. AC power supply, no I/O cards)	NS-ISG-1000B
NS-ISG-1000 baseline system (inc. DC power supply, no I/O cards)	NS-ISG-1000B-DC

ISG 2000 Systems	Part Number
NS-ISG-2000 system (inc. AC power supplies, no I/O cards)	NS-ISG-2000
NS-ISG-2000 system (inc. DC power supplies, no I/O cards)	NS-ISG-2000-DC
NS-ISG-2000 baseline system (inc. AC power supplies, no I/O cards)	NS-ISG-2000B
NS-ISG-2000 baseline system (inc. DC power supplies, no I/O cards)	NS-ISG-2000B-DC

Integrated IDP Upgrades	Part Number
Security module for IDP on ISG 1000 and ISG 2000 systems	NS-ISG-SEC
IDP upgrade kit for ISG 1000 system, including IDP license key, additional memory, and 5-device NSM	NS-ISG-1000-IKT
IDP upgrade kit for ISG 2000 system, including IDP license key, additional memory, and 5-device NSM	NS-ISG-2000-IKT

ISG 1000 and ISG 2000 I/O Modules	Part Number
I/O Module - 1-port 10 Gigabit Ethernet - does NOT include transceiver	NS-ISG-1XG
Transceiver - XFP 10GigE Short Range (SR) (300 m)	NS-SYS-GBIC-MXSR
Transceiver - XFP 10GigE Long Range (LR) (10 km)	NS-SYS-GBIC-MXLR
I/O Module - 2-port mini GBIC-SX	NS-ISG-SX2
I/O Module - 2-port mini GBIC-LX	NS-ISG-LX2
I/O Module - 4-port mini GBIC-SX	NS-ISG-SX4
I/O Module - 4-port mini GBIC-LX	NS-ISG-LX4
I/O Module - 4-port mini GBIC-TX	NS-ISG-TX4
I/O Module - 4-port 10/100 Fast Ethernet	NS-ISG-FE4
I/O Module - 8-port 10/100 Fast Ethernet	NS-ISG-FE8
I/O Module - 2-port 10/100/1000 Gigabit Ethernet	NS-ISG-TX2

ISG 1000 Software Options	Part Number
VSYS upgrade 0 to 5	NS-ISG-1000-VSYS-5
VSYS upgrade 5 to 10	NS-ISG-1000-VSYS-10
VSYS upgrade 10 to 25	NS-ISG-1000-VSYS-25
VSYS upgrade 25 to 50	NS-ISG-1000-VSYS-50
GPRS firewall/VPN license	NS-ISG-1000-GKT

ISG 2000 Software Options	Part Number
VSYS upgrade 0 to 5	NS-ISG-2000-VSYS-5
VSYS upgrade 5 to 25	NS-ISG-2000-VSYS-25
VSYS upgrade 25 to 50	NS-ISG-2000-VSYS-50
VSYS upgrade 50 to 100	NS-ISG-2000-VSYS-100
VSYS upgrade 100 to 250	NS-ISG-2000-VSYS-250
GPRS firewall/VPN license	NS-ISG-2000-GKT

ISG 1000 and ISG 2000 Spares	Part Number
SX transceiver (mini-GBIC)	NS-SYS-GBIC-MSX
LX transceiver (mini-GBIC)	NS-SYS-GBIC-MLX
ISG 1000 AC power supply	NS-ISG-1000-PWR-AC
ISG 1000 DC power supply	NS-ISG-1000-PWR-DC
ISG 2000 AC power supply	NS-ISG-2000-PWR-AC2
ISG 2000 DC power supply	NS-ISG-2000-PWR-DC2
Japan power cord option	NS-ISG-2000-Japan
Fan module	NS-ISG-FAN
Rack-mount kit (19 in, all mounting hardware)	NS-ISG-2000-RCK-01
Rack-mount kit (23 in, all mounting hardware)	NS-ISG-2000-RCK-02
Blank interface panel	NS-ISG-IPAN2
ISG 2000 blank power-supply cover	NS-ISG-2000-PPAN2

Note: The appropriate power cord is included based upon the sales order "Ship To" destination.
Note: Every virtual system includes 1 additional virtual router and 2 additional security zones, usable in the virtual or root system.

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.

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