Juniper Networks ISG Series

ISG 1000

ISG 2000

The Juniper Networks Integrated Security Gateways (ISG) are ideally suited for securing enterprise, carrier and data center environments where advanced applications such as VoIP and streaming media dictate consistent, scalable performance. The Juniper Networks ISG 1000 and ISG 2000 are purpose-built security solutions that leverage a fourth generation security ASIC, the GigaScreen[3], along with high speed microprocessors to deliver unmatched firewall and VPN performance. Integrating best-in-class firewall, VPN and DoS solutions, the ISG 1000 and ISG 2000 enable secure, reliable connectivity along with network and application-level protection for critical, high traffic network segments.

ISG 1000:

The ISG 1000 is a fully integrated FW/VPN system with gigabit performance, a modular architecture and rich virtualization capabilities. The base FW/VPN system comes with four fixed 10/100/1000 interfaces and two additional I/O modules for interface expansion.

ISG 2000:

The ISG 2000 is a fully integrated FW/VPN system with multi-gigabit performance, a modular architecture and rich virtualization capabilities. The base FW/VPN system allows for up to four I/O modules for interface expansion.

Optional Integrated IDP

The ISG Series can be easily upgraded to support integrated Intrusion Detection and Prevention (IDP), providing robust network and application layer protection against current and emerging threats. Leveraging the same award-winning software found on Juniper Networks' IDP platforms -but integrated into ScreenOS - the ISG Series provides a combination of best in class firewall, VPN, and IDP with dedicated processing modules that ensure multi-gigabit capability in a single solution. With unmatched security and network segmentation features, the ISG Series can be deployed to protect both perimeter deployments as well as internal networks.

The ISG 1000 supports up to two security modules, while the ISG 2000 supports up to three security modules for IDP integration.

Optional GPRS Firewall/VPN

Both the ISG 1000 and ISG 2000 can be upgraded to support GPRS (General Packet Radio Service) to provide stateful-firewalling and filtering capabilities, eliminating many of the security risks that are inherant within the GPRS protocol (GTP). Mitigating a wide variety of attacks on the Gp, Gn, and Gi interfaces, the Juniper Networks GPRS Firewall/VPN solutions protect key nodes within the mobile operators' network.

The Juniper Networks Integrated Security Gateway features include:

Security

Stateful and IPS (Deep Inspection) firewall, DoS protection and optional integrated IDP prevent network and application level attacks to defend against the propagation of malicious code, such as worms, Trojans, malware, spyware, and hackers.

Network Friendly

Support for key routing protocols, such as OSPF, RIPv2, and BGP, along with transparent Layer 2 operation, NAT and Route mode help facilitate network integration. To satisfy complex internal network segmentation demands dictated by various government regulations such as Sarbanes-Oxley and GLBA, the ISG Series delivers the most advanced set of network segmentation features including Virtual Systems, Security Zones, Virtual Routers and VLANs.

Resiliency

Hardware component redundancy, multiple high availability options and route-based VPNs provide the reliability required for high speed network security deployments.

Interface Flexibility

The ISG Series FW/VPN modular architechture enables deployment with a wide variety of copper and fiber interface options, simplifying network integration and helping to reducing the cost of future network upgrades.

Left column table

	ISG 1000[1]	ISG 2000[1]
Maximum Performance and Capacity[1]		
ScreenOS version support	ScreenOS 5.4	ScreenOS 5.4
Firewall performance (large packet)	1 Gbps	4 Gbps
Firewall performance (64 byte)	1 Gbps	2 Gbps
Firewall packets per second (64 byte)	1.5 M	3 M
3DES + SHA-1/AES performance	1 Gbps	2 Gbps
Integrated IDP performance[2]	1 Gbps	2 Gbps
Concurrent sessions[3]	500,000	1,000,000
New sessions/second	20,000	25,000
Policies	10,000	30,000
GTP Tunnels[4]	150,000	300,000
Interfaces	4 fixed 10/100/1000 ports, up to 4 mini GBIC (SX or LX), up to 8 10/100/1000, up to 20, 10/100	Up to 8 Mini GBIC (SX or LX), up to 8 10/100/1000, up to 28 10/100
Mode of Operation		
Layer 2 mode (transparent mode)[4]	Yes	Yes
Layer 3 mode (route and/or NAT mode)	Yes	Yes
NAT (Network Address Translation)	Yes	Yes
PAT (Port Address Translation)	Yes	Yes
Policy-based NAT	Yes	Yes
Mapped IP[5]	4,096	8,192
MIP/VIP Grouping	Yes	Yes
Virtual IP[6]	8	8
Users supported	Unrestricted	Unrestricted
Firewall		
Number of network attacks detected	31	31
Network attack detection	Yes	Yes
DoS and DDoS protections	Yes	Yes
TCP reassembly for fragmented packet protection	Yes	Yes
Malformed packet protections	Yes	Yes
Brute force attack mitigation	Yes	Yes
CPU protection	Yes	Yes
Syn cookie protection	Yes	Yes
Zone-based IP spoofing	Yes	Yes
URL filtering (external)	Yes (Websense, SurfControl)	
IPS (Deep Inspection FW)[7]		
Stateful protocol signatures	Yes	Yes
Protocol Anomaly	Yes	Yes
IPS (Optional, Integrated IDP) Specifications[2][8]		
Stateful protocol signatures	Yes	Yes
Deep Inspection (DI) signature packs	Yes	Yes
Attack detection mechanisms	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, E-mail, Custom, Log	
Attack notification mechanisms	Session Packet Log, Session Summary, E-mail, SNMP, Syslog, Webtrends	
Worm Protection	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

Right column table

	ISG 1000[1]	ISG 2000[1]
IPS (Optional, Integrated IDP) Specifications cont'd[2][8]		
Approximate number of attacks covered	3,600 +	3,600 +
Detailed Threat Descriptions and Remediation/Patch Info	Yes	Yes
Enterprise Security Profiler (ESP)	No	No
Create and enforce appropriate application usage policies	Yes	Yes
Attacker and Target Audit Trail and Reporting	Yes	Yes
Deployment Modes	Inline or Inline TAP	Inline or Inline TAP
Frequency of updates	Daily and Emergency	Daily and Emergency
VPN		
Concurrent VPN tunnels	2,000[5]	10,000[5]
Tunnel interfaces	Up to 512[5]	Up to 1,024[5]
DES (56-bit), 3DES (168-bit) and AES encryption	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
Dead Peer Detection	Yes	Yes
IPSec NAT traversal	Yes	Yes
Redundant VPN gateways	Yes	Yes
Firewall and VPN User Authentication		
Built-in (internal) database - user limit	5,000[5]	15,000[5]
3rd Party user authentication	RADIUS, RSA SecurID, and LDAP	
XAUTH VPN authentication	Yes	Yes
Web-based authentication	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, v1.5 and v2.0 compatible	
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	
System Management		
NetScreen-Security Manager	Yes	Yes
All management via VPN tunnel on any interface	Yes	Yes
SNMP full custom MIB	Yes	Yes
Rapid deployment	No	No
Logging/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
Virtualization		
Maximum number of Virtual Systems	0 default, upgradeable to 10[8]	0 default, upgradeable to 50[8]
Maximum number of Security zones	20 default, upgradeable to 40[8]	26 default, upgradeable to 126[8]
Maximum number of Virtual routers	3 default, upgradeable to 13[8]	3 default, upgradeable to 53[8]
Number of VLANs supported	1,000	2,000

	ISG 1000[1]	ISG 2000[1]
Routing		
OSPF/BGP dynamic routing	up to 8/64 instances each[5]	up to 8/64 instances each[5]
RIPv1, RIPv2 dynamic routing	up to 12 instances supported[5]	Up to 50 instances supported[5]
BGP dynamic routing	64 instances, 128 peers	64 instances, 128 peers
Static routes	10,000	20,000
Source Based Routing, Source Interface Based Routing	Yes	Yes
ECMP flow based routing	Yes	Yes
High Availability (HA)		
Active/Active	Yes	Yes
Active/Passive	Yes	Yes
Redundant interfaces	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
VoIP		
H.323 ALG	Yes	Yes
SIP ALG	Yes	Yes
MGCP ALG	Yes	Yes
SCCP ALG	Yes	Yes
NAT for H.323/SIP/SCCP	Yes	Yes
IP Address Assignment		
Static	Yes	Yes
DHCP, PPPoE client	Yes, No	No, No
Internal DHCP server	Yes	No
DHCP relay	Yes	Yes
Administration		
Local administrators database	20	20
External administrator database	RADIUS/LDAP/SecurID	
Restricted administrative networks	6	6
Root Admin, Admin, and Read Only user levels	Yes	Yes
Software upgrades	TFTP/WebUI/NSM	
Configuration Roll-back	Yes	Yes

	ISG 1000[1]	ISG 2000[1]
Traffic Management		
Guaranteed bandwidth	No	No
Maximum bandwidth	Yes, per physical interface only	
Ingress Traffic Policing	No	No
Priority-bandwidth utilization	No	No
DiffServ stamp	Yes, per policy	Yes, per policy
External Flash		
CompactFlash™	Supports 128 or 512 MB Industrial-Grade SanDisk	
Event logs and alarms	Yes	Yes
System config script	Yes	Yes
NetScreen ScreenOS Software	Yes	Yes
Dimensions and Power		
Dimensions (H/W/L)	5.25/17.5/17.258 inches	5.25/17.5/23 inches
Weight	30 lbs.	52 lbs.
Rack mountable	19" standard, 23" optional	19" standard, 23" optional
Power Supply (AC)	100 to 240 VAC, 250 watts	100 to 240 VAC, 250 watts
Power Supply (DC)	-36 to -72 VDC, 250 watts	-36 to -60 VDC, 250 watts
Redundant Power Supply	No (single, field replaceable)	Yes (dual, hot swappable)
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
Security Certifications	Common Criteria: EAL4	Common Criteria: EAL4 ICSA Firewall and VPN
Environment		
Operational temperature:	32° to 122° F, 0° to 50° C	32° to 122° F, 0° to 50° C
Non-operational temperature:	-4° to 158° F, -20° to 70° C	-4° to 158° F, -20° to 70° C
Humidity:	10 to 90% non-condensing	10 to 90% non-condensing
MTBF (Bellcore model)	7.6 years	7.6 years
Other	NEBS Level 3	NEBS Level 3
Security	No	Pending

(1) Performance, capacity and features listed are based upon measured maximums under ideal testing conditions. Performance may vary with other ScreenOS releases and by deployment. Actual throughput may vary based upon packet size and enabled features.

(2) Additional IDP license and hardware upgrade required

(3) Concurrent sessions listed are based upon maximums with optional IDP upgrade. FW/VPN concurrent sessions maximum without optional IDP upgrade are 250,000 for the ISG 1000 and 500,000 for the ISG 2000.

(4) NAT, PAT, policy based NAT, virtual IP, mapped IP, virtual systems, virtual routers, VLANs, OSPF, BGP, RIPv , Active/Active HA, and IP address assignment are not available in layer 2 transparent mode.

(5) Shared among all Virtual Systems.

(6) Not available with Virtual Systems.

(7) IPS (Deep Inspection FW) is automatically disabled when optionally integrated IDP is installed.

(8) Additional license required.

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	250,000	512,000
Concurrent VPN tunnels	1,000	1,000	2,000	10,000
Deep Inspection Firewall	No	No	Yes	Yes
VLANs	50	100	1,000	2,000
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
GPRS firewall/VPN	No	No	Optional Upgrade	Optional Upgrade

Ordering Information

Product	Part Number
ISG 1000 Systems	
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	
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	
Security module for IDP on ISG 1000 and ISG 2000 systems	NS-ISG-SEC
IDP Upgrade Kit for ISG 1000 system, including IDP Lic Key, additional memory, and 5-device NSM	NS-ISG-1000-IKT
IDP Upgrade Kit for ISG 2000 system, including IDP Lic Key, additional memory, and 5-device NSM	NS-ISG-2000-IKT
ISG 1000 and ISG 2000 I/O Modules	
I/O Module - Dual Port Mini GBIC-SX	NS-ISG-SX2
I/O Module - Dual Port Mini GBIC-LX	NS-ISG-LX2
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 - Dual Port 10/100/1000 Gig Ethernet	NS-ISG-TX2
ISG 1000 Software Options	
VSYS Upgrade 0 to 5	NS-ISG-1000-VSYS-5
VSYS Upgrade 5 to 10	NS-ISG-1000-VSYS-10
GPRS Firewall/VPN license	NS-ISG-1000-GKT
ISG 2000 Software Options	
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 0 to 25	NS-ISG-2000-VSYS-025
VSYS Upgrade 0 to 50	NS-ISG-2000-VSYS-050
GPRS Firewall/VPN license	NS-ISG-2000-GKT
ISG 1000 and ISG 2000 Spares	
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

Every Virtual System includes 1 additional virtual router and 2 additional security zones, usable in the virtual or root system