Juniper Networks **ISG Series with IDP**

ISG 1000

ISG 2000

The Juniper Networks Integrated Security Gateway (ISG) Series delivers unmatched firewall, VPN, and IDP performance through a combination of a fourth generation security ASIC, the GigaScreen^3, high speed microprocessors and pluggable security modules each with their own processing and memory. The Juniper Networks ISG 1000 and ISG 2000 – with integrated, best-in-class Intrusion Detection and Prevention (IDP) running on the security modules – stops worms, Trojans, Spyware, malware and other emerging attacks from penetrating and proliferating across the network.

With unmatched processing power, the ISG series is ideally suited for securing enterprise, carrier and data center environments where advanced applications such as VoIP and streaming media dictate network and application level protection with consistent, scalable performance. A stateful inspection firewall, along with an IPSec VPN and robust networking capabilities, complements the integrated IDP functionality to deliver secure, reliable connectivity for critical, high-traffic network segments.

ISG 1000:

The ISG 1000 is a fully integrated FW/VPN/IDP 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. The ISG 1000 also supports two security modules for IDP integration.

ISG 2000:

The ISG 2000 is a fully integrated FW/VPN/IDP 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 and three security modules for full IDP integration. The ISG 2000 is fully managed by NetScreen-Security Manager for centralized and unified policy management, network settings, and device configuration across all the security components.

The Juniper Networks Integrated Security Gateway with IDP features include:

Application level protection:

Unmatched security processing power and network segmentation features allow the ISG Series to protect critical high speed networks against the penetration and proliferation of existing and emerging application level threats such as worms, Trojans, Spyware and malware. With multiple attack detection mechanisms including stateful signatures and protocol anomaly, IDP performs in-depth analysis of application protocol, context and state to deliver Zero Day coverage against existing and emerging threats.

Network friendly:

To simplify network deployments, the IDP functionality is seamlessly integrated with ScreenOS and takes full advantage of proven networking features such as dynamic routing, including OSPF, BGP, and RIP V2; multiple routing domains via virtual routers; and NAT/Route/Transparent deployment options. Seamless ScreenOS integration also means that IDP attack protection can be deployed across Virtual Systems and Security Zones to stop attacks from penetrating or proliferating throughout the network.

Policy-based management:

Using granular, rule-by-rule flexibility provided by NetScreen-Security Manager, administrators can deploy IDP inline or inline-tap mode on a per rule, per protocol basis. Role based administration allows a security team to delegate management authority to appropriate personnel, allowing one team to manage only the IDP component while others can manage firewall, VPN or other tasks. Attack and incident investigation as well as auditing and reporting for compliance purposes are managed easily and quickly with the NetScreen-Security Manager's intuitive graphical user interface.

	ISG 1000[1]	ISG 2000[1]
Maximum Performance and Capacity[1]		
ScreenOS version support	ScreenOS 5.0	ScreenOS 5.0
Firewall performance	1 Gbps	4 Gbps
64 byte packet performance	1 Gbps	2 Gbps
3DES/AES performance	1 Gbps	2 Gbps
Integrated IDP performance	Up to 1 Gbps with 2 security modules	Up to 2 Gbps with 3 security modules
Concurrent sessions	500,000	1,000,000
New sessions/second	20,000	27,000
Policies	10,000	30,000
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)[2]	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[3]	4,096	8,192
MIP/VIP Grouping	Yes	Yes
Virtual IP[4]	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
Deep Inspection (DI) firewall[5]	Yes	Yes
URL filtering (external)	Yes (Websense)	Yes (Websense)
IDP Specifications		
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

	ISG 1000[1]	ISG 2000[1]
IDP Specifications		
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[3]	10,000[3]
Tunnel interfaces	Up to 512[3]	Up to 1,024[3]
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[3]	15,000[3]
3rd Party user authentication	RADIUS, RSA SecurID, and LDAP	
XAUTH VPN authentication	Yes	Yes
Web-based authentication	Yes	Yes
System Management	Yes	Yes
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[6]	0 default, upgradeable to 50[6]
Maximum number of Security zones	20 default, upgradeable to 40[6]	26 default, upgradeable to 126[6]
Maximum number of Virtual routers	3 default, upgradeable to 13[6]	3 default, upgradeable to 53[6]
Number of VLANs supported	250	500

	ISG 1000[1]	ISG 2000[1]
Routing		
OSPF/BGP dynamic routing	up to 8 instances each[3]	up to 8 instances each[3]
BGP dynamic routing	8 instances, 32 peers	8 instances, 32 peers
RIPv1, RIPv2 dynamic routing	up to 12 instances supported[3]	Up to 50 instances supported[3]
Static routes	10,000	20,000
Source Based Routing, Source Interface Based Routing	Yes	Yes
ECMP flow based routing	No	No
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
NAT for H.323/SIP	No	No
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	
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
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] 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.

[3] Shared among all Virtual Systems.

[4] Not available with Virtual Systems.

[5] Deep Inspection is automatically disabled when integrated IDP is installed.

[6] Additional license required.

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
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
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

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, Asia Pacific Finance 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
Juniper House
Guildford Road
Leatherhead
Surrey, KT22 9JH, U. K.
Phone: 44(0)-1372-385500
Fax: 44(0)-1372-385501