



ISG Series 통합 보안 게이트웨이

제품 소개

주니퍼 네트워크 ISG Series 통합 보안 게이트웨이는 VoIP, 스트리밍 미디어와 같은 첨단 애플리케이션들이 지속적이고 확장 가능한 성능을 요구하는 데이터센터, 통신사업자, 엔터프라이즈 환경의 보안에 이상적입니다. 주니퍼 네트워크 ISG1000 및 ISG2000 통합 보안 게이트웨이는 고속 마이크로프로세서와 4세대 보안 ASIC을 활용해 탁월한 방화벽 및 VPN 성능을 제공하는 전문 보안 솔루션입니다. 동급 최강의 방화벽, VPN과 옵션으로 제공되는 IDP가 통합된 ISG1000 및 ISG2000은 대량의 트래픽이 발생하는 네트워크의 주요 영역에 대한 네트워크 및 애플리케이션 레벨의 보안과 더불어 안전하고 안정적인 연결을 지원합니다.

제품 설명

주니퍼 네트워크 ISG1000 및 ISG2000 통합 보안 게이트웨이는 완벽하게 통합된 방화벽/VPN 시스템으로서 멀티기가비트 성능, 모듈형 아키텍처 및 다양한 가상화 기능들을 제공합니다. ISG1000과 ISG2000은 대기업, 데이터센터, 통신사업자 네트워크에 이상적인 보안 솔루션입니다.

주니퍼 네트워크 ISG Series 통합 보안 게이트웨이는 방화벽/VPN 기반 시스템으로서 IPS (침입방지시스템), 안티스팸, 웹 필터링, ICAP (Internet Content Adaptation Protocol) 안티바이러스 리다이렉션 지원 등과 같은 보안 기능들을 제공합니다. 이 최첨단 시스템은 옵션으로 통합 제공되는 IDP (Intrusion Detection and Prevention) 또는 모바일 네트워크 서비스 사업자 환경을 위한 GPRS (General Packet Radio Service) 방화벽/VPN 등으로 확대가 가능합니다.

ISG Series 모듈형 아키텍처는 다양한 코퍼 및 하이버 인터페이스 옵션으로 구축이 가능합니다. 베투얼 시스템, 베투얼 LAN, 보안 존 등과 같은 최신 기능들을 사용하여 각기 다른 보안 레벨들에 속한 트래픽을 매우 유연하게 분할 및 격리할 수 있습니다. ISG Series는 다수의 독립된 방화벽 인스펙션 또는 라우팅 정책들을 지원하여 네트워크 설계를 단순화합니다. 그럼으로써 매우 복잡한 환경에서도 네트워크 자체에 영향을 미치지 않고 보안 정책들을 트래픽 시스템에 적용할 수 있습니다.

ISG Series 아키텍처의 유연성과 효율성은 방화벽/VPN 또는 옵션 IDP 모듈들을 갖춘 통합 방화벽/VPN/IDP 솔루션으로서 최고 수준의 성능과 기능성을 제공합니다. ISG1000은 최대 2개의 IDP 모듈을 지원하며, ISG2000은 최대 3개의 IDP 모듈을 지원합니다. IDP 모듈들은 전용 프로세싱 및 메모리를 갖추며, IDP 패킷 프로세싱 가속화를 위한 기술을 탑재하고 있습니다. 이를 통해 독립된 보안 장비들과 관리 애플리케이션들의 수를 줄일 수 있습니다. 그리고 구축 작업과 네트워크의 복잡성을 간소화할 수 있습니다. 결과적으로 대폭적인 비용 절감이 가능합니다.

ISG Series with IDP는 주니퍼 네트워크 IDSP Series 침입 탐지 및 방지 어플라이언스들과 동일한 최고수준의 소프트웨어를 사용합니다. IDP 보안 모듈은 스테이트풀 시그니처, 이상 프로토콜 탐지 등 8개의 각기 다른 탐지 메커니즘들이 결합된 다중 탐지 기능을 지원합니다. ISG Series with IDP는 웹, 트로이 목마, 악성코드, 스파이웨어, 해커 등과 같은 보안 위협들로부터 조직을 보호할 뿐만 아니라, 의도하지 않게 네트워크에 추가된 애플리케이션들과 운영체제들의 종류 및 버전, 그리고 악성 서버들과 관련된 정보들을 제공합니다. 애플리케이션 시그니처들은 애플리케이션 트래픽의 정확한 탐지를 통해 관리자들이 각종 규제사항과 기업 비즈니스 정책들을 준수할 수 있도록 해줍니다.

ISG1000과 ISG2000은 다양한 컨피규레이션으로 구축되어 네트워크 경계 및 내부 네트워크 리소스 모듈을 보호할 수 있습니다. 이동통신사업자 네트워크에 구축되는 ISG1000 및 ISG2000 GPRS 솔루션들은 GPRS Tunneling Protocol (GTP)을 인식하고, 버추얼 시스템 내부의 GTP 기능을 완벽하게 지원합니다. ISG Series는 2개의 PLMN (Public Land Mobile Networks) 간의 Gp 인터페이스 연결, SGSN과 GGSN 지원 노드들 간의 Gn 인터페이스 연결, 그리고 GGSN과 인터넷 간의 Gi 인터페이스 연결에 구축될 수 있습니다.

ISG Series GPRS 방화벽/VPN은 정교한 위협, DoS 공격, 악의적인 사용자들에 대처할 뿐만 아니라, 업링크/다운링크 트래픽을 소비하며 대역폭을 잡아먹는 애플리케이션들과 메시지들을 제한합니다. 그리고 3GPP R6 IE 제거를 실행함으로써 2G와 3G 네트워크 간의 로밍에서 상호운용성 유지를 지원합니다.

기능 및 이점

기능	기능 설명	이점
전문 플랫폼	보안 전용 프로세싱 하드웨어 및 소프트웨어 플랫폼	고속 LAN 환경을 보호하는 데 필요한 성능 제공
예측 가능한 성능	ASIC 기반 아키텍처가 멀티기가비트 속도로 모든 패킷 크기에 대한 일정한 성능 제공	VoIP, 스트리밍 미디어와 같이 시간에 민감한 애플리케이션들에 대해 낮은 지연속도 보장
시스템 및 네트워크 장애 내구성	하드웨어 구성 요소 이중화, 다수의 고가용성 옵션 및 경로 기반 (Route-Based) VPN	고속 네트워크 구축에 필요한 안정성 제공
동급 최강의 네트워크 보안 기능	웹 필터링, 스팸 차단, IPS, ICAP 안티 바이러스 리다이렉션 및 통합 IDP 옵션 내장	Symantec 및 SurfControl과 같은 동급 최강의 보안 파트너들이 추가 보안 기능 지원
인터페이스 유연성	모듈형 아키텍처이기 때문에 다양한 코퍼 및 화이버 인터페이스 옵션을 이용하여 구축할 수 있음	네트워크 통합을 간소화하고 향후 네트워크 업그레이드 비용을 절감할 수 있도록 지원
네트워크 세그먼트 분할	관리자들이 보안 존, 버추얼 LAN 및 버추얼 라우터를 통해 게스트, 무선 네트워크 및 지역 서버/데이터베이스를 분리하여 보안 정책을 구축할 수 있도록 지원	네트워크 상의 다양한 내부, 외부 및 DMZ 서브그룹들에 대한 보안 구축 지원함으로써 무단 액세스 차단
중앙 관리	NSM을 통해 주니퍼 네트워크스 방화벽 및 IDP 제품들에 대한 중앙 관리 실현	여러 플랫폼들의 긴밀한 통합으로 단순하고 한눈에 알아보기 쉬운 네트워크 전반의 보안 관리
강력한 라우팅 엔진	입증된 라우팅 엔진으로 OSPF, BGP 및 RIP v1/2와 함께 Frame Relay, Multilink Frame Relay, PPP, Multilink PPP 및 HDLC 등 지원	보안 및 라우팅 통합 장비의 구축으로 운영 및 투자 비용 절감
종합적인 위협 방어	전용 프로세싱 모듈을 탑재한 단일 솔루션으로 동급 최고의 멀티기가비트급 방화벽/VPN/IDP 성능 제공	탁월한 성능을 통해 고속 네트워크 내에서 모든 방식으로 시도되는 공격으로부터 네트워크가 보호되도록 보장
세계 정상의 전문 서비스	한 랩 테스트에서 대규모 네트워크 구축에 이르는 모든 프로젝트에서 주니퍼 네트워크스의 전문 서비스는 고객의 IT 팀과의 협력을 통해 목표 규명, 구축 프로세스 정리, 네트워크 설계의 개발/검증 및 구축 시스템 관리 활동을 수행	네트워크 인프라스트럭처 혁신을 통해 탁월한 보안성, 유연성, 확장성 및 안정성 보장

제품 옵션

옵션	옵션 설명	적용 제품
통합 스팸 차단	Symantec 기술을 바탕으로 제공되는 연간 등록제 스팸 차단 기능을 이용하여 알려진 스팸 발송자와 피셔 (Phisher)가 보낸 원치 않는 이메일 차단	ISG1000 & ISG2000
통합 IPS (Deep Inspection)	Stateful 시그니처 및 이상 프로토콜 탐지 메커니즘을 사용하여 애플리케이션 레벨의 네트워크 플러딩 공격 차단. IPS는 연간 등록제로 제공됨	ISG1000 & ISG2000
통합 웹 필터링	업계 최고 SurfControl의 기술을 기반으로 하는 연간 등록제 웹 필터링 솔루션을 이용하여 악의적인 웹 사이트에 대한 액세스 차단	ISG1000 & ISG2000
ICAP 안티바이러스 리다이렉션	ICAP 안티바이러스 콘텐츠 리다이렉션으로 써드파티/대기업의 바이러스 차단 솔루션을 네트워크 경계에 구축할 수 있도록 지원	ISG1000 & ISG2000
통합 IDP 옵션	전용 IDP 보안 모듈로 고속 패킷 검사 실행. 전체 IDP 기능을 추가하는 데 그 어떤 네트워크 변경도 요구하지 않기 때문에 제로 데이 (Zero-Day), 웜, 트로이 목마 및 스파이웨어 등과 같은 Layer 4-7 공격을 차단할 수 있음. 하드웨어 및 시스템 추가 업그레이드가 필요함	ISG1000 & ISG2000
애플리케이션 인식/탐지	컨텍스트, 프로토콜 정보, 시그니처를 사용하여 모든 포트에서 애플리케이션들을 정확하게 탐지함. IDP 보안 모듈 옵션 필요	ISG1000 & ISG2000
이동통신사업자를 위한 GPRS 방화벽 /VPN	GPRS 네트워크에 대한 지원을 통해 Gp, Gn, 및 Gi 인터페이스상의 다양한 공격을 무력화시킴으로써 이동통신사업자 네트워크 내 핵심 노드를 보호하는 Stateful 방화벽 및 필터링 기능 제공. 추가 라이선스 필요함	ISG1000 & ISG2000



사양

	ISG1000	ISG2000
Maximum Performance and Capacity¹		
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

사양 (계속)

	ISG1000	ISG2000
Integrated IPS (Optional Integrated IDP)¹⁰ (continued)		
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
Unified Threat Management/Content Security⁵		
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
Unified Threat Management/Content Security⁵		
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
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 Security⁰		
GTP tunnels ⁷	200,000	400,000
GTP packet inspection (IPS or IDP)	Yes	Yes

* 2008년 11월 기준으로 5,560개의 시그니처가 있으며, 매주 약 10개의 새로운 시그니처가 추가됨.

사양 (계속)

	ISG1000	ISG2000
IPsec VPN		
Concurrent VPN tunnels ²	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 ⁶	50,000	50,000
Third-party user authentication	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
Virtualization⁹		
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

사양 (계속)

	ISG1000	ISG2000
Routing (continued)		
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) ⁸	8	8
MIP/VIP grouping	Yes	Yes
Address Translation		
Static	Yes	Yes
DHCP, PPPoE client	Yes, No	No, No
Internal DHCP server	Yes	No
DHCP relay	Yes	Yes

사양 (계속)

	ISG1000	ISG2000
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
Network and 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

사양 (계속)

	ISG1000	ISG2000
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)
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°C to 158°F (-20° to 70°C)
Humidity	10% to 90% noncondensing	10% to 90% noncondensing

(1) 표시된 성능, 용량, 사양은 ScreenOS 6.2가 탑재된 시스템 기준이며, 이상적인 테스트 환경에서 나오는 최대치로 측정하였습니다. 실제 결과는 탑재된 ScreenOS 릴리즈에 따라 다를 수 있습니다. ISG1000 및 ISG2000 플랫폼을 지원하는 ScreenOS 버전 전체 목록은 Juniper Customer Support Center (<http://www.juniper.net/customers/support/>)에서 확인 가능합니다.

(2) 추가 IDP 라이선스 및 하드웨어 업그레이드 필요.

(3) 동시 세션은 현재 출하되는 ISG 하드웨어의 최대치 기준입니다. 구형 ISG 유닛으로 최대 동시 세션 용량을 얻으려면 옵션 제공되는 메모리 업그레이드가 필요합니다. 메모리 업그레이드를 하지 않은 구형 ISG 유닛의 FW/VPN 최대 동시 세션은 ISG1000이 250,000이며, ISG2000이 500,000입니다. IDP 업그레이드 옵션이 적용된 구형 ISG 유닛은 최대 동시 세션 용량을 지원하며, 추가적인 메모리 업그레이드가 필요 없습니다.

(4) 통합 IDP 옵션이 탑재되면 DI (Deep Inspection Firewall) 기능은 자동적으로 불능화됩니다.

(5) 보안 사양 (IPS/Deep Inspection, 안티스팸 및 웹 필터링)은 주니퍼 네트워크로부터 연간 약정으로 구매 가능합니다. 연간 약정 구매 시 시그니처 업데이트와 관련 지원이 함께 제공됩니다.

(6) Redirect Web Filtering이 트래픽을 보조 서버로 보내므로 Websense 또는 SurfControl 각각으로부터 별도의 웹 필터링 라이선스를 구매해야 합니다.

(7) NAT, PAT, 정책 기반 NAT, 비주요 IP, mapped IP, 비주요 시스템, 비주요 라우터, VLANs, OSPF, BGP, RIPv2, active/active HA, IP 주소 할당은 레이어 2 트랜스퍼렌트 모드에서 사용이 불가능합니다.

(8) 모든 비주요 시스템들 사이에서 공유됨.

(9) 비주요 시스템에서 사용 불가.

(10) 추가 라이선스가 필요함.

(11) 4-포트 미니 GBIC 모듈 필요 - NS-ISG-SX4, NS-ISG-LX4 또는 NS-ISG-TX4.

라이선스 옵션

ISG1000 및 ISG2000은 서로 다른 수준의 기능 및 용량을 지원하는 2개의 라이선스 옵션과 함께 제공됩니다.

- **Advanced 모델:** Advanced Software License는 본 스펙 시트에 제시된 모든 기능 및 용량을 제공합니다.
- **Baseline 모델:** Baseline Software License는 Deep Inspection™, OSPF 및 BGP 다이나믹 라우팅, 고급 High Availability 및 최대 용량 등이 필수적으로 요구되지 않는 고객 환경을 위한 엔트리 레벨 솔루션을 제공합니다.

아래 표에서는 Baseline 모델과 Advanced 모델 간의 기능 및 용량 차이를 설명하고 있습니다.

	BASELINE		ADVANCED	
	ISG1000	ISG2000	ISG1000	ISG2000
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 서비스 및 지원

주니퍼는 하이 퍼포먼스 네트워킹의 가치를 가속, 확장, 최적화시키는 Performance-Enabling 서비스 및 지원을 제공합니다. 이러한 서비스를 통해 매출과 직결되는 역량들을 신속하게 제공함으로써 생산성을 향상시키고, 새로운 비즈니스 모델을 지원하며, 시장 확대와 고객 만족 증대를 실현시킵니다. 동시에 주니퍼는 뛰어난 운영 효율성을 통해 성능, 안정성, 가용성, 확장성 요구를 만족 시키고 운영비용을 절감시키며 IT 위험 요소들을 제거합니다.

주문정보

Model Number	Description
ISG1000 Systems	
NS-ISG-1000	NS-ISG-1000 system (includes AC power supply, no I/O cards)
NS-ISG-1000-DC	NS-ISG-1000 system (includes DC power supply, no I/O cards)
NS-ISG-1000B	NS-ISG-1000 baseline system (includes AC power supply, no I/O cards)
NS-ISG-1000B-DC	NS-ISG-1000 baseline system (includes DC power supply, no I/O cards)
ISG2000 Systems	
NS-ISG-2000	NS-ISG-2000 system (includes AC power supplies, no I/O cards)
NS-ISG-2000-DC	NS-ISG-2000 system (includes DC power supplies, no I/O cards)
NS-ISG-2000B	NS-ISG-2000 baseline system (includes AC power supplies, no I/O cards)
NS-ISG-2000B-DC	NS-ISG-2000 baseline system (includes DC power supplies, no I/O cards)
Integrated IDP Upgrades	
NS-ISG-SEC	Security module for IDP on ISG1000 and ISG2000 systems
NS-ISG-1000-IKT	IDP upgrade kit for ISG1000 system, including IDP license key, additional memory, and 5-device NSM
NS-ISG-2000-IKT	IDP upgrade kit for ISG2000 system, including IDP license key, additional memory, and 5-device NSM
ISG1000 and ISG2000 I/O Modules	
NS-ISG-1XG	I/O Module – 1-port 10-Gigabit Ethernet – does NOT include transceiver
NS-SYS-GBIC-MXSR	Transceiver – XFP 10 GigE Short Range (SR) (300 m)
NS-SYS-GBIC-MXLR	Transceiver – XFP 10 GigE Long Range (LR) (10 km)
NS-ISG-SX2	I/O Module – 2-port mini GBIC-SX
NS-ISG-LX2	I/O Module – 2-port mini GBIC-LX
NS-ISG-SX4	I/O Module – 4-port mini GBIC-SX
NS-ISG-LX4	I/O Module – 4-port mini GBIC-LX
NS-ISG-TX4	I/O Module – 4-port mini GBIC-TX
NS-ISG-FE4	I/O Module – 4-port 10/100 Fast Ethernet
NS-ISG-FE8	I/O Module – 8-port 10/100 Fast Ethernet
NS-ISG-TX2	I/O Module – 2-port 10/100/1000 Gigabit Ethernet

Model Number	Description
ISG1000 Software Options	
NS-ISG-1000-VSYS-5	VSYS upgrade 0 to 5
NS-ISG-1000-VSYS-10	VSYS upgrade 5 to 10
NS-ISG-1000-VSYS-25	VSYS upgrade 10 to 25
NS-ISG-1000-VSYS-50	VSYS upgrade 25 to 50
NS-ISG-1000-GKT	GPRS firewall/VPN license
ISG2000 Software Options	
NS-ISG-2000-VSYS-5	VSYS upgrade 0 to 5
NS-ISG-2000-VSYS-25	VSYS upgrade 5 to 25
NS-ISG-2000-VSYS-50	VSYS upgrade 25 to 50
NS-ISG-2000-VSYS-100	VSYS upgrade 50 to 100
NS-ISG-2000-VSYS-250	VSYS upgrade 100 to 250
NS-ISG-2000-GKT	GPRS firewall/VPN license
ISG1000 and ISG2000 Spares	
NS-SYS-GBIC-MSX	SX transceiver (mini-GBIC)
NS-SYS-GBIC-MLX	LX transceiver (mini-GBIC)
NS-ISG-1000-PWR-AC	ISG1000 AC power supply
NS-ISG-1000-PWR-DC	ISG1000 DC power supply
NS-ISG-2000-PWR-AC2	ISG2000 AC power supply
NS-ISG-2000-PWR-DC2	ISG2000 DC power supply
NS-ISG-2000-Japan	Japan power cord option
NS-ISG-FAN	Fan module
NS-ISG-2000-RCK-01	Rack-mount kit (19 in, all mounting hardware)
NS-ISG-2000-RCK-02	Rack-mount kit (23 in, all mounting hardware)
NS-ISG-IPAN2	Blank interface panel
NS-ISG-2000-PPAN2	ISG2000 blank power-supply cover

알람: 주문 내역에 표시된 배송지 정보에 따라 알맞은 파워 코드가 제공됩니다.

알람: 모든 비추열 시스템에는 하나의 비추열 라우터와 비추열 또는 루트 시스템에서 사용할 수 있는 2개의 추가 보안 존이 포함됩니다.

주니퍼 네트워크에 대하여

주니퍼 네트워크는 하이 퍼포먼스 네트워킹을 지향하는 네트워크 업계 선도적인 업체입니다. 주니퍼는 단일 네트워크 상에서 서비스와 애플리케이션 운용을 가속화시킬 수 있는 신뢰성 있는 네트워크 환경 구축을 위해 하이 퍼포먼스 네트워크 인프라를 제공하는데 주력하고 있습니다. 이러한 하이 퍼포먼스 네트워크는 곧 고객에게 하이 퍼포먼스 비즈니스가 가능하게 하는 원동력이 되고 있습니다.

추가 정보는 www.juniper.net/kr/kr 에서 확인할 수 있습니다.



한국주니퍼네트웍스(주) 서울시 강남구 역삼 1동 736-1 캐피탈 타워 19층 TEL : 02)3483-3400 FAX : 02)3483-3488 www.juniper.net/kr/kr

Corporate And Sales Headquarters

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

ACAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600 Fax: 35.31.8903.601

©2009 주니퍼 네트워크 사. 모든 권리 보유. 주니퍼 네트워크, 주니퍼 네트워크 로고, NetScreen 및 ScreenOS는 미국과 다른 나라에서 주니퍼 네트워크의 등록 상표입니다. JUNOS와 JUNOSe는 주니퍼 네트워크의 상표입니다. 다른 모든 상표, 서비스 마크, 등록 상표 또는 등록 서비스 마크는 해당 소유권자의 자산일 수 있습니다. 주니퍼 네트워크는 본 자료의 오류에 대해 그 어떠한 책임도 지지 않습니다. 주니퍼 네트워크는 사전 통보 없이 본 자료를 변경, 수정, 교체 또는 정정할 수 있는 권한을 보유하고 있습니다.

주니퍼 네트워크 솔루션의 구매를 원하시면 주니퍼 네트워크 영업 담당자 02-3483-3400 또는 공인 리셀러에게 문의해 주십시오.