

Juniper Networks SSG 140

Juniper Networks Secure Services Gateway 140 (SSG 140)은 중견 기업의 지사와 기업 구축을 위한 솔루션으로 탁월한 성능, 보안, 라우팅 및 LAN/WAN 연결 기능을 완벽하게 결합한 맞춤형 보안 장비입니다. 방화벽, IPSec VPN, IPS, 바이러스 차단 (스파이웨어/애드웨어/피싱 차단 포함), 스팸 차단 및 웹 필터링을 포함한 포괄적인 UTM (Unified Threat Management) 보안 기능 세트를 통해 지사에서 수행되는 트랜잭션을 웹, 스파이웨어, 트로이 목마 및 악성 코드로부터 보호합니다.

이와 같이 포괄적인 UTM 보안 기능을 활용해 SSG 140을 독립형 네트워크 보호 장비로 구축할 수 있습니다. 또한, 강력한 라우팅 엔진을 장착하고 있기 때문에 기존의 지사 라우터나 보안/라우팅 통합 장비로 구축해 IT 투자 비용 및 운영 경비를 줄일 수 있습니다. SSG 140은 고객에게 다음과 같은 기능 및 이점을 제공합니다.

- 탁월한 보안 기능을 토대로 LAN 및 WAN 접속 옵션을 제공함으로써, 비용 절감 및 한층 강력한 투자 보호의 이점을 제공하는 확장형 I/O 아키텍처
- 동급 최강의 전문 보안 솔루션을 탑재하여 모든 형태의 공격으로부터 네트워크를 보호하는 UTM 보안 기능. 시만텍 안티스팸, 케이스퍼스키 안티바이러스, 서프컨트롤의 웹 필터링 탑재.
- 관리자가 게스트, 무선 네트워크 및 지역 서버/데이터베이스를 구분해 보안 정책을 구축함으로써 인증 받지 않은 액세스를 차단하고 발생 가능한 모든 공격을 억제할 수 있도록 보장하는 네트워크 세그먼트 분할 등을 비롯한 고급 보안 기능
- 고속 LAN을 비롯해 저속 WAN 접속을 보호하기 위해 필요한 성능을 제공하는 보안 전용 프로세싱 하드웨어 및 소프트웨어 플랫폼

대기업, 서비스 사업자, 독립 사업부 등에서 사용되는 SSG 140은 WAN 및 고속 LAN을 통해 전달되는 비즈니스 코리티컬 트래픽을 보호할 수 있는 고급 보안 및 라우팅 기능을 필요로 하는 중견 기업에 가장 이상적입니다. 구축 사례에는 중소 규모의 독립 사업부와 지사 환경 등이 포함되어 있습니다.



앞 면



뒷 면

SSG 140은 350Mbps 이상의 S방화벽 트래픽과 100Mbps의 IPSec VPN을 제공하는 모듈식 플랫폼으로서, 8개 온보드 10/100 2개의 10/100/1000 인터페이스를 비롯해 T1, E1, ISDN BRI S/T, Serial 연결 등을 위한 4개 I/O 확장 슬롯을 지원합니다.

보안

성능이 입증된 방화벽 및 IPSec VPN이 IPS, 바이러스 차단 (스파이웨어/애드웨어/피싱 차단 포함), 스팸 차단 및 웹 필터링 등을 포함한 동급 최강의 UTM 보안 기능에 통합되어 있기 때문에 웹, 스파이웨어, 트로이 목마, 악성 코드 및 기타 신종 공격으로부터 LAN 및 WAN 트래픽을 보호할 수 있습니다.

LAN/WAN 접속

LAN/WAN 접속 옵션과 지원 프로토콜을 모두 갖추고 있기 때문에 고객은 SSG 140을 기존 LAN 기반 방화벽이나 라우팅/보안 통합 장비로서 구축할 수 있으며, 이를 통해 TCO도 절감할 수 있습니다.

네트워크 세그먼트 분할

SSG 140은 관리자들이 네트워크를 각각 고유한 보안 정책을 가진 별개의 보안 영역으로 나누어 사용자 그룹에 따라 다른 보안 수준을 구현할 수 있는 보안 존 (Security Zone), 가상 라우터 및 VLAN 등을 비롯한 일련의 고급 네트워크 세그먼트 분할 기능을 제공합니다.

원활한 네트워크 전환 수행

로컬 사이트에 단 몇 대의 SSG를 구축하건, 아니면 세계 전역에 수천 대를 구축하든 관계 없이 Juniper Networks Professional Services를 유용하게 활용할 수 있습니다. 간단한 랩 테스트에서 대규모 네트워크 구현에 이르기까지 주니어의 전문가들이 목표 규명, 구축 프로세스의 정의, 네트워크 설계의 개발/검증, 구축 시스템 관리 등 모든 단계에서 귀사를 지원할 것입니다. 또한, 귀사 팀과의 협력을 통해 뛰어난 유연성, 확장성, 안정성 및 보안성을 갖춘 네트워크 인프라로 탈바꿈시킬 것입니다.

SSG 140

Maximum Performance and Capacity⁽¹⁾

ScreenOS version support	ScreenOS 5.4
Firewall performance (Large packets)	350+ Mbps
Firewall performance (IMIX) ⁽²⁾	300 Mbps
Firewall packets per second (64 byte)	100,000 PPS
3DES + SHA-1 VPN performance	100 Mbps
Concurrent sessions	32,000
New sessions/second	8,000
Policies	500
Users supported	Unrestricted

Network Connectivity

Fixed I/O	8 10/1000, 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 ⁽³⁾	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⁽⁴⁾

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 ⁽⁵⁾	Yes

VPN

Concurrent VPN tunnels	125
Tunnel interfaces	50
DES (56-bit), 3DES (168-bit) and AES encryption	Yes
MD-5 and SHA-1 authentication	Yes
Manual key, IKE, PKI (X.509)	Yes
Perfect forward secrecy (DH Groups)	1, 2, 5
Prevent replay attack	Yes
Remote access VPN	Yes
L2TP within IPSec	Yes
IPSec NAT traversal	Yes
Redundant VPN gateways	Yes

SSG 140

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

SSG 140

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

SSG 140

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	L, 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

- 위의 성능, 용량 및 기능은 Screen OS 5.4를 실행하는 시스템을 기준으로 한 것으로, 별도의 언급이 없으면 이상적인 테스트 조건에서 측정된 최대값을 뜻합니다. 실제 결과는 ScreenOS 버전 및 구축 시스템에 따라 다를 수 있습니다.
- IMIX란 Internet Mix의 약자로서 보다 일반적인 고객 네트워크의 트래픽 혼합 구성을 나타내기 때문에 단일 패킷 크기 보다 성능 요구 수준이 훨씬 높습니다. 사용되는 IMIX 트래픽은 64바이트 패킷 (58.33%) + 570바이트 패킷 (33.33%) + 1518바이트 패킷 (8.33%)의 UDP 트래픽으로 이루어집니다.
- NAT, PAT, 정책 기반 NAT, 가상 IP, 매핑된 IP, 가상 시스템, 가상 라우터, VLAN, OSPF, BGP, RIPv2, Active/Active HA 및 IP 주소 할당은 Layer 2 투명 모드에서는 지원되지 않습니다.
- UTM 보안 기능 (침입탐지, 안티바이러스, 안티스팸, 웹필터링)은 Juniper Networks에서 매 해 기능별로 라이선스를 구매, 등록 갱신을 하고 있습니다. UTM 보안기능을 위해서는 256M이상의 메모리 용량이 필요합니다.
- 웹 필터링을 외부 서버와 연동할 경우 Websense나 SurfControl에서 직접 라이선스를 구매하여 써야 합니다.

IPS (Deep Inspection FW) Signature Pack

Signature Pack은 특정 시스템이나 공격 유형에 따라 공격 보호 기능을 구성하는 기능을 제공합니다. 다음은 SSG 140에서 지원되는 Signature Pack입니다.

Signature Pack	목표 대상	방어 유형	공격 객체의 유형
목표 대상	지사, 중소 기업	클라이언트/서버 및 웹 차단 기능	서명 및 프로토콜 이상의 범위
클라이언트	원격 사무실 및 지사	경계선 방어, 호스트 (데스크탑 등)에서의 규제 준수	서버-클라이언트 방향의 공격
서버	중소 기업	경계선 방어, 서버 인프라에서의 규제 준수	클라이언트-서버 방향의 공격
웹 공격 완화	대기업의 원격 사무실 및 지사	웹 공격을 막는 가장 포괄적인 방어책	웹, 트로이 목마, 백도어 공격

주문 정보

Product	Part Number
SSG 140	
SSG 140 System, 256 MB memory, 0 PIM cards, AC power	SSG-140-SB
SSG 140 System, 512 MB memory, 0 PIM cards, AC power	SSG-140-SH

SSG 140 I/O Options

1 Port ISDN BRI S/T Interface	JX-1BRI-ST-S
2 Port E1 PIM with integrated CSU/DSU	JX-2E1-RJ48-S
2 Port T1 PIM with integrated CSU/DSU	JX-2T1-RJ48-S
2 Port Serial PIM	JX-2Serial-S

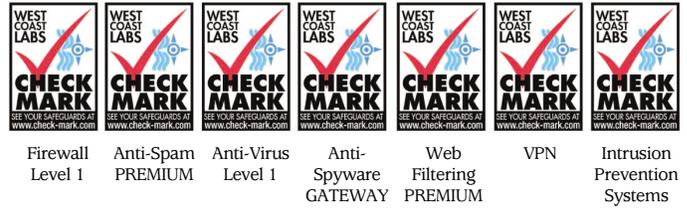
Unified Threat Management/Content Security (High Memory Option Required)

Antivirus (Anti-Spyware, Anti-Phishing)	NS-K-AVS-SSG140
IPS (Deep Inspection)	NS-DI-SSG140
Anti-Spam	NS-SPAM-SSG140
Web Filtering	NS-WF-SSG140
Remote Office Bundle (AV, IPS, WF)	NS-RBO-CS-SSG140
Main Office Bundle (AV, IPS, WF, AS)	NS-SMB-CS-SSG140

SSG 140 Memory Upgrades, Spares and Communications Cables

512 MB memory upgrade for the SSG 140	SSG-100-MEM-512
Power Cable, Australia	CBL-JX-PWR-AU
Power Cable, China	CBL-JX-PWR-CH
Power Cable, Europe	CBL-JX-PWR-EU
Power Cable, Italy	CBL-JX-PWR-IT
Power Cable, Japan	CBL-JX-PWR-JP
Power Cable, UK	CBL-JX-PWR-UK
Power Cable, US	CBL-JX-PWR-US
Blank I/O plate	JX-Blank-PP-S
EIA530 cable (DCE)	JX-CBL-EIA530-DCE
EIA530 cable (DTE)	JX-CBL-EIA530-DTE
RS232 cable (DCE)	JX-CBL-RS232-DCE
RS232 cable (DTE)	JX-CBL-RS232-DTE
RS449 cable (DCE)	JX-CBL-RS449-DCE
RS449 cable (DTE)	JX-CBL-RS449-DTE
V.35 cable (DCE)	JX-CBL-V35-DCE
V.35 cable (DTE)	JX-CBL-V35-DTE
X.21 cable (DCE)	JX-CBL-X21-DCE
X.21 cable (DTE)	JX-CBL-X21-DTE

* 참고 : 판매 주문서에 있는 "배송" 목적지에 따라 정격 전원 코드가 포함됩니다.



한국주니퍼네트웍스(주) 서울시 서초구 서초동 1303-22 교보타워 A동 4층 TEL : 02)3483-3400 FAX : 02)3483-3488 www.kr.juniper.net

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 Tower
 3 Garden Road, 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

저작권 © 2006, 주니퍼 네트웍스 사. 모든 권리 보유. 주니퍼 네트웍스 및 주니퍼 네트웍스 로고는 미국과 기타 국가에서 주니퍼 네트웍스 사의 등록 상표입니다. 본 문서의 다른 모든 상표, 서비스 마크, 등록 상표 또는 등록 서비스 마크는 주니퍼 네트웍스 사나 각 소유권자의 자산일 수 있습니다. 모든 스펙은 사전 통보 없이 변경될 수 있습니다. 주니퍼 네트웍스는 본 문서의 오류에 대해 어떠한 책임도 지지 않으며 본 문서를 업데이트해야 할 의무도 없습니다. 주니퍼 네트웍스는 사전 통보없이 본 자료를 변경, 수정, 교체 또는 정정할 수 있는 권한을 보유하고 있습니다.

파트번호 : 100181-001 Nov 2006