



SSG140

보안 서비스 게이트웨이

제품 개요

주니퍼 네트워크 SSG140 보안 서비스 게이트웨이 (Secure Services Gateway)는 중간 규모의 지사와 기업 구축을 위해 탁월한 성능, 보안, 라우팅 및 LAN/WAN 연결 기능을 완벽하게 결합한 맞춤형 보안 장비입니다. Stateful 방화벽, IPSec VPN (IP Security Virtual Private Network), IPS (Intrusion Prevention System), 바이러스 차단 (스파이웨어/애드웨어/피싱 차단 포함), 스팸 차단 및 웹 필터링을 포함한 포괄적인 UTM (Unified Threat Management) 보안 기능들을 통해 지사 또는 기업에서 수행되는 트랜잭션을 웹, 스파이웨어, 트로이 목마 및 악성 코드로부터 보호합니다.

제품 설명

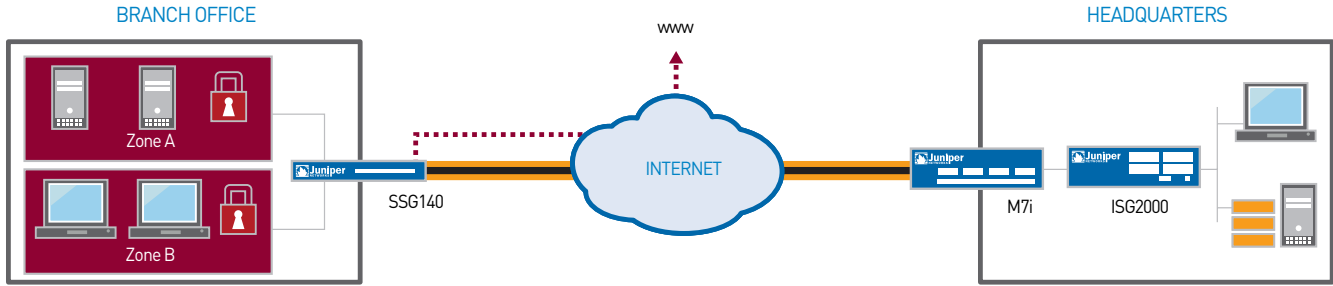
SSG140은 내부와 외부 공격을 막고 불법적인 액세스를 차단하며 규제를 준수할 수 있도록 돕는 지사와 중소기업 단독 기업을 위한 고성능 보안 플랫폼입니다. SSG140은 350 Mbps 이상의 stateful 방화벽 트래픽과 100 Mbps의 IPSec VPN을 제공하는 모듈형 플랫폼입니다.

보안: 동급 최강의 파트너가 뒷받침하는 입증된 UTM (Unified Threat Management) 보안 기능을 통해 바이러스, 스팸 및 신종 악성 코드의 공격을 차단합니다. SSG 140은 관리자들이 내부의 보안 요구를 해결하고 규제를 준수하기 위해 네트워크를 각각 고유한 보안 정책을 가진 별개의 보안 영역으로 나눌 수 있도록 하는 보안 존 (Security Zone), 가상 라우터 및 VLAN 등을 비롯한 일련의 고급 네트워크 보호 기능을 제공합니다. 각각의 보안 존을 보호하는 정책에는 지원되는 모든 UTM 보안 기능을 통한 검사와 접근제어 규칙이 포함될 수 있습니다.

연결 및 라우팅: SSG140은 10개 온보드 (8 10/100 + 2개의 10/100/1000) 인터페이스와 추가로 WAN 인터페이스 (T1, E1, ISDN BRI S/T 및 Serial)를 장착할 수 있는 4개의 I/O 확장 슬롯을 제공한다는 점에서 동급 최강의 확장 가능한 보안 플랫폼으로 평가 받고 있습니다. 라우팅 엔진에 광범위한 I/O 옵션과 함께 WAN 프로토콜 캡슐화 기술을 채용했기 때문에 SSG 140은 기존의 지사 라우터나 통합 보안/라우팅 장비와 마찬가지로 손쉽게 구축할 수 있으며, 따라서 투자 및 운영비용을 줄일 수 있습니다.

접근제어 정책 적용: Infranet Controller를 추가하면 SSG140은 주니퍼 네트워크의 통합 접근제어 구축 환경에서 정책 적용 지점의 역할을 할 수 있습니다. Infranet Controller는 공격 상황 및 사용자 속성 측면에 대한 큰 폭의 변화를 수용할 수 있도록 단일 장치 상태 및 사용자 ID를 포함한 보다 세분화된 기준에 따라 액세스를 허용/거부하는 솔루션을 바탕으로 방화벽 기반 접근제어를 확장/교체하기 위해 SSG5 또는 SSG20과 상호 작용함으로써 중앙 정책 관리 엔진의 역할을 수행합니다.

세계 정상급 지원: 간단한 랩 테스트에서 대규모 네트워크 구현에 이르는 모든 프로젝트에서 주니퍼 네트워크의 전문 서비스는 고객의 IT 팀과의 협력을 통해 목표 규명, 구축 프로세스 정의, 네트워크 설계의 개발/검증 및 구축 시스템 관리를 수행하여 성공적인 결과를 얻게 됩니다.



SSG140은 기업 본사에 대한 안전한 인터넷 접속 및 사이트 간 VPN을 위해 지사에 구축되었습니다. 내부 지사 자원은 각 보안 존 (Security Zone)을 위한 고유의 보안 정책을 통해 보호됩니다.

기능 및 이점

기능	기능 설명	이점
고성능	맞춤형 하드웨어, 강력한 프로세싱 및 보안 전용 운영 체제를 통합한 맞춤형 플랫폼	현재 및 미래에 내부/외부 공격을 차단하는 데 필요한 성능 헤더룸 제공
등급 최강의 UTM 보안 기능	UTM 보안 기능 (바이러스/스팸 차단, 웹 필터링, IPS)으로 네트워크에 손상을 입기 전에 모든 형태의 바이러스 및 악성 코드 차단	모든 형태의 공격으로부터 네트워크 보호
통합 바이러스 차단	Kaspersky Lab 엔진 기반의 연간 등록제 바이러스 백신 엔진 제공	바이러스, 스파이웨어, 애드웨어 및 기타 악성 코드 차단
통합 스팸 차단	Symantec 기술 기반의 연간 등록제 스팸 차단 제공	알려진 스팸/피싱 공격자로부터 오는 원치 않는 e-메일 차단
통합 웹 필터링	SurfControl 기술 기반의 연간 등록제 웹 필터링 솔루션 제공	악의적 웹 사이트에 대한 접근제어/차단
통합 IPS (Deep Inspection)	연간 등록제 IPS 엔진	네트워크에 플래그되는 애플리케이션 레벨 공격 차단
고정 인터페이스	8개의 고정 10/100 인터페이스와 2개의 10/100/1000 인터페이스, 1개의 USB 포트, 1개의 콘솔 포트 및 1개의 Auxiliary 포트	고속 LAN 연결, 향후 연결 옵션 및 유연한 관리 기능 제공
네트워크 세그먼트 분할	관리자는 브리지 그룹 (Bridge Group), 보안 존, 가상 LAN 및 가상 라우터를 통해 게스트, 무선 네트워크 및 지역 서버/데이터 베이스를 분리하도록 보안 정책을 구축할 수 있음*	강력한 기능을 활용하여 인증 받지 않은 액세스를 차단하도록 네트워크상의 다양한 내부, 외부 및 DMZ 서브그룹에 대한 정책 구축 지원
강력한 라우팅 엔진	임집된 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 자본 비용 절감
높은 인터페이스 밀도	8개의 10/100 인터페이스와 2개의 10/100/1000 인터페이스, 1개의 콘솔과 관리용 보조 인터페이스	경쟁 제품에 비해 뛰어난 인터페이스 밀도를 제공
인터페이스 모듈성	4개의 SSG 140 인터페이스 확장 슬롯으로 T1, E1, ISDN BRI S/T, ADSL2+, G.SHDSL 및 시리얼 PIM (Physical Interface Modules), 10/100/1000 및 SFP uPIM (universal PIM) 옵션 지원**	비용 절감 및 투자 보호 강화를 위해 탁월한 보안을 바탕으로 LAN 및 WAN 연결 제공
관리의 유연성	CLI (Command Line Interface), WebUI 또는 주니퍼 네트워크 Network and Security Manager 메커니즘을 이용한 보안 정책의 구축, 모니터링 및 관리	모든 위치에서 관리자가 액세스할 수 있도록 하여 현장 방문의 필요성을 없앴. 이를 통해 응답 시간 단축 및 운영 비용 절감 실현
주니퍼 네트워크 UAC (Unified Access Control) Enforcement Point	중앙 정책 관리 엔진 (IC Series)과 연동되어 사용자 계정, 장비 보안 상태, 네트워크 위치 등과 같은 정보를 통해 세션별 접근제어 실행	고객의 기존 네트워크 인프라스트럭처 구성요소들과 최상급 기술을 활용하여 비용대비 효과적으로 보안 수준 강화
세계 정상의 전문 서비스	간단한 랩 테스트에서 대규모 네트워크 구현에 이르는 모든 프로젝트에서 주니퍼 네트워크의 전문 서비스는 고객의 IT 팀과의 협력을 통해 목표 규명, 구축 프로세스 정의, 네트워크 설계의 개발/검증 및 구축 시스템 관리를 수행함	네트워크 인프라스트럭처 혁신을 통해 탁월한 보안성, 유연성, 확장성 및 안정성 보장
Auto-Connect VPN	허브 앤 스포크 (Hub-and-Spoke) 토폴로지에서 스포크 사이트 간 VPN 터널의 자동 설정/해제	VoIP 및 화상 회의와 같이 지연 시간에 민감한 애플리케이션을 지원하는 메시 (Mesh) 아키텍처를 위한 확장형 VPN 솔루션 제공

* 브리지 그룹은 ScreenOS 6.0 이상의 uPIM 상에서만 지원

** uPIM은 ScreenOS 6.0 이상에서만 지원

제품 옵션

옵션	옵션 설명	해당 제품
DRAM	SSG140은 256MB 또는 512MB DRAM 지원	SSG140
UTM (Unified Threat Management)/컨텐츠 보안 (대용량 메모리 옵션 필요)	SSG140은 바이러스 차단 (스파이웨어/피싱 차단 포함), IPS (Deep Inspection 방화벽), 웹 필터링 및 스팸 차단 등을 비롯한 동급 최강 UTM 및 콘텐츠 보호 기능의 모든 조합으로 구성 가능	SSG140 대용량 메모리 모델에서만 지원
I/O 옵션	4개의 SSG140 인터페이스 확장 슬롯으로 T1, E1, ISDN BRI S/T, ADSL2+, G.SHDSL 및 시리얼 PIM (Physical Interface Modules), 10/100/1000 및 SFP uPIM (universal PIM) 옵션 지원	SSG140



SSG140

사양

Maximum Performance and Capacity⁽¹⁾

ScreenOS [®] version tested	ScreenOS 6.2
Firewall throughput (large packets)	350+ Mbps
Firewall throughput (IMIX) ⁽²⁾	300 Mbps
Firewall packets per second (64 byte)	100,000 PPS
Advanced Encryption Standard (AES) 256+SHA-1 VPN throughput	100 Mbps
3DES encryption +SHA-1 VPN throughput	100 Mbps
Maximum concurrent sessions	48,000
New sessions/second	8,000
Maximum security policies	1,000
Maximum users supported	Unrestricted

Network Connectivity

Fixed I/O	8x10/100, 2x10/100/1000
Physical Interface Module (PIM) slots	4
Modular WAN/LAN interface options (PIMs/uPIMs)	2xT1, 2xE1, 2xSerial, 1xISDN BRI S/T SFP, 10/100/1000

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⁽³⁾

IPS (Deep Inspection firewall)	Yes
Protocol anomaly detection	Yes
Stateful protocol signatures	Yes
IPS/DI attack pattern obfuscation	Yes
Antivirus	Yes
Signature database	200,000+
Protocols scanned	POP3, HTTP, SMTP, IMAP, FTP, IM
Anti-spyware	Yes
Anti-adware	Yes
Anti-keylogger	Yes
Instant message AV	Yes
Anti-spam	Yes
Integrated URL filtering	Yes
External URL filtering ⁽⁴⁾	Yes

VoIP Security

H.323. Application-level gateway (ALG)	Yes
SIP ALG	Yes
MGCP ALG	Yes
SCCP ALG	Yes
Network Address Translation (NAT) for VoIP protocols	Yes

IPsec VPN

Concurrent VPN tunnels	500
Tunnel interfaces	50
DES encryption (56-bit), 3DES encryption (168-bit) and AES (256-bit)	Yes
MD-5 and SHA-1 authentication	Yes
Manual key, Internet Key Exchange (IKE), IKEv2 with EAP public key infrastructure (PKI) (X.509)	Yes
Perfect forward secrecy (DH Groups)	1,2,5
Prevent replay attack	Yes
Remote access VPN	Yes
Layer 2 Tunneling Protocol (L2TP) within IPsec	Yes
IPsec Network Address Translation (NAT) traversal	Yes
Auto-Connect VPN	Yes
Redundant VPN gateways	Yes

사양 (계속)

User Authentication and Access Control

Built-in (internal) database user limit	250
Third-party user authentication	RADIUS, RSA SecureID, LDAP
RADIUS Accounting	Yes - start/stop
XAUTH VPN authentication	Yes
Web-based authentication	Yes
802.1X authentication	Yes
Unified Access Control (UAC) enforcement point	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
Self signed certificates	Yes

Virtualization

Maximum number of security zones	40
Maximum number of virtual routers	6
Bridge groups*	Yes
Maximum number of VLANs	100

Routing

BGP instances	6
BGP peers	24
BGP routes	2,048
OSPF instances	3
OSPF routes	2,048
RIPv1/v2 instances	64
RIP v2 routes	2,048
Static routes	2,048
Source-based routing	Yes
Policy-based routing	Yes
Equal-cost multipath (ECMP)	Yes
Multicast	Yes
Reverse Forwarding Path (RFP)	Yes
Internet Group Management Protocol (IGMP) (v1, v2)	Yes
IGMP Proxy	Yes
Protocol Independent Multicast (PIM) single mode	Yes
PIM source-specific multicast	Yes
Multicast inside IPsec tunnel	Yes

Encapsulations

Point-to-Point Protocol (PPP)	Yes
Multilink Point-to-Point Protocol (MLPPP)	Yes
MLPPP max physical interfaces	4
Frame relay	Yes

* 브리지 그룹은 ScreenOS 6.0 이상의 uPIM 상에서만 지원

Encapsulations (계속)

Multilink Frame Relay (MLFR) (FRF 15, FRF 16)	Yes
MLFR max physical interfaces	4
HDLC	Yes

IPv6

Dual stack IPv4/IPv6 firewall and VPN	Yes
IPv4 to/from IPv6 translations and encapsulations	Yes
Syn-Cookie and Syn-Proxy DoS Attack Detection	Yes
SIP, RTSP, Sun-RPC, and MS-RPC ALG's	Yes
RIPng	Yes
BGP	Yes
Transparent mode	Yes
NSRP	Yes
DHCPv6 Relay	Yes

Mode of Operation

Layer 2 (transparent) mode ⁽⁵⁾	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 (L2 and L3 mode)	Yes
Mapped IP (MIP) (L3 mode)	1,500
Virtual IP (VIP) (L3 mode)	16
MIP/VIP Grouping (L3 mode)	Yes

IP Address Assignment

Static	Yes
Dynamic Host Configuration Protocol (DHCP), Point-to-Point Protocol over Ethernet (PPPoE) client	Yes
Internal DHCP server	Yes
DHCP relay	Yes

Traffic Management Quality of Service (QoS)

Guaranteed bandwidth	Yes - per policy
Maximum bandwidth	Yes - per policy
Ingress traffic policing	Yes
Priority-bandwidth utilization	Yes
Differentiated Services marking	Yes - per policy

High Availability (HA)

Active/active - L3 mode	Yes
Active/passive - Transparent & L3 mode	Yes
Configuration synchronization	Yes
Session synchronization for firewall and VPN	Yes
Session failover for routing change	Yes
VRRP	Yes
Device failure detection	Yes
Link failure detection	Yes
Authentication for new HA members	Yes
Encryption of HA traffic	Yes

사양 (계속)

System Management

WebUI (HTTP and HTTPS)	Yes
Command line interface (console)	Yes
Command line interface (telnet)	Yes
Command line interface (SSH)	Yes - v1.5 and v2.0 compatible
Network and Security Manager (NSM)	Yes
All management via VPN tunnel on any interface	Yes
Rapid deployment	No

Administration

Local administrator database size	20
External administrator database support	RADIUS, RSA SecureID, LDAP
Restricted administrative networks	6
Root Admin, Admin, and Read Only user levels	Yes
Software upgrades	TFTP, WebUI, NSM, SCP, USB
Configuration roll-back	Yes

Logging/Monitoring

System log (multiple servers)	Yes - up to 4 servers
Email (2 addresses)	Yes
NetIQ WebTrends	Yes
SNMP (v2)	Yes
SNMP full custom MIB	Yes
Traceroute	Yes
VPN tunnel monitor	Yes

External Flash

Additional log storage	USB 1.1
Event logs and alarms	Yes
System configuration script	Yes
ScreenOS Software	Yes

Dimensions and Power

Dimensions (W x H x D)	17.5 x 1.8 x 15 in (44.5 x 4.5 x 38.1 cm)
Weight	10.2 lb (4.63 kg)
Rack mountable	Yes, 1RU
Power supply (AC)	100-240 VAC, AC Input line frequency 50 Hz or 60 Hz AC system current rating 2 A
Maximum thermal output	580 BTU/hour (170 W)
Noise Level	48.8 dB

Certifications

Safety certifications	UL, CUL, CSA, CB
Electromagnetic compatibility (EMC) certifications	FCC class B, CE class B
Network Equipment Building System (NEBS)	No
Mean time between failures (MTBF) (Bellcore model)	16 years

Security Certifications

Common Criteria: EAL4	Future
FIPS 140-2: Level 2	Future
ICSA Firewall and VPN	Yes

Operating Environment

Operating temperature	32° to 122° F (0° to 50° C)
Non-operating temperature	-4° to 158° F (-20° to 70° C)
Humidity	10% to 90% noncondensing

- (1) 위의 성능, 용량 및 기능은 ScreenOS 6.2를 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.
- (2) IMIX란 Internet Mix의 약자로서 보다 일반적인 고객 네트워크의 트래픽 혼합 구성을 나타내기 때문에 단일 패킷 크기보다 성능 요구 수준이 훨씬 높습니다. 사용되는 IMIX 트래픽은 64바이트 패킷 (58.33%) + 570바이트 패킷 (33.33%) + 1518바이트 패킷 (8.33%)의 UDP 트래픽으로 이루어집니다.
- (3) UTM 보안 기능 (IPS/Deep Inspection, 바이러스/스팸 차단 및 웹 필터링)은 주니퍼 네트워크에서 별도로 구입한 연간 회원제 서비스를 통해 제공됩니다. 연간 회원제 서비스는 패턴 업데이트 및 관련 지원 서비스를 제공합니다. UTM 보안 기능의 경우, 하이 메모리 (High Memory) 옵션이 필요합니다.
- (4) 리다이렉트 웹 필터링은 방화벽에서 보조 서버로 트래픽을 전송합니다. 리다이렉트 기능은 무료로 제공되지만, Websense 또는 SurfControl로부터 별도의 웹 필터링 라이선스를 구입해야 합니다.
- (5) 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 Transparent 모드에서는 지원되지 않습니다.

IPS (Deep Inspection FW) Signature Pack

Signature Pack은 특정 시스템이나 공격 유형에 따라 공격 보호 기능을 구성하는 기능을 제공합니다. 다음은 SSG140에서 지원되는 Signature Pack입니다 :

Signature Pack	목표 대상	방어 유형	공격 객체의 유형
기본	지사, 중소기업	클라이언트/서버 및 웹 차단 기능	시그니처 및 프로토콜 이상의 범위
클라이언트	원격 사무실/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

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 운영효율성을 통해 성능, 안정성, 가용성, 확장성 요구를 만족 시키고 운영 비용을 절감시키며 IT 위험 요소들을 제거합니다.

주문 정보

Model Number	Description
SSG 140	
SSG-140-SB	SSG140 with 256 MB memory, 0 PIM cards, AC power
SSG-140-SH	SSG140 with 512 MB memory, 0 PIM cards, AC power
SSG140 I/O Options	
JX-1BRI-ST-S	1-port ISDN BRI S/T PIM
JX-2E1-RJ48-S	2-port E1 PIM with integrated CSU/DSU
JX-2T1-RJ48-S	2-port T1 PIM with integrated CSU/DSU
JX-2Serial-S	2-port Serial PIM
JX-1ADSL-A-S	1-port ADSL 2/2+ Annex A PIM
JX-1ADSL-B-S	1-port ADSL 2/2+ Annex B PIM
JX-2SHDSL-S	1-port G.SHDSL PIM
JXU-6GE-SFP-S	6-port SFP Gigabit Ethernet Universal PIM*
JXU-1SFP-S	1-port SFP 100 Mbps or Gigabit Ethernet Universal PIM* (SFP sold separately)
JXU-8GE-TX-S	8-port Gigabit Ethernet 10/100/1000 Copper Universal PIM*
JXU-16GE-TX-S	16-port Gigabit Ethernet 10/100/1000 Copper Universal PIM*

* 브리지 그룹은 ScreenOS 6.0 이상의 uPIM 상에서만 지원

Model Number	Description
Unified Threat Management/Content Security (High Memory Option Required)	
NS-K-AVS-SSG140	Antivirus (anti-spyware, anti-phishing)
NS-DI-SSG140	IPS (Deep Inspection)
NS-SPAM-SSG140	Anti-spam
NS-WF-SSG140	Web filtering
NS-RBO-CS-SSG140	Remote Office Bundle (AV, IPS, WF)
NS-SMB-CS-SSG140	Main Office Bundle (AV, IPS, WF, AS)

* uPIM은 ScreenOS 6.0 이상에서만 지원

SSG140 Memory Upgrades, Spares and Communications Cables

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

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

주니퍼 네트워크에 대하여

주니퍼 네트워크는 하이 퍼포먼스 네트워킹을 지향하는 네트워크 업계 선도적인 업체입니다. 주니퍼는 단일 네트워크 상에서 서비스와 애플리케이션 운영을 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 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

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

APAC 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
Airsides 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.