



갈수록 정교해지고 늘어나는 네트워크 공격들로 인해, 기업의 네트워크 보안이 그 어느 때보다 중요시되고 있습니다. 새로운 공격들이 만들어지는 속도는 더욱 빨라지고, 애플리케이션들의 숫자와 OS 취약성은 날로 증가하기 때문에 문제는 한층 복잡해졌습니다. Juniper Networks IDP (Intrusion Detection and Prevention) 제품은 다양한 공격들로부터 네트워크를 보호하는 최신 인라인 네트워크 IPS (network Intrusion Prevention System) 기능들을 제공합니다. 또한 주니퍼 IDP 제품들은 Juniper Networks Security Team의 지원을 통해 새로 발견되는 취약점들에 대해 업계에서 가장 신속한 대응을 제공합니다.

Juniper Networks IDP 75/250/800/8200

제품 설명

Juniper Networks IDP (Intrusion Detection and Prevention) 제품은 종합적이면서도 사용이 간편한 인라인 (In-Line) 보안을 제공함으로써 네트워크와 애플리케이션 레벨에서 신속하게 공격을 차단하고 보안 네트워크 유지와 관련된 시간과 비용을 최소화합니다. 업계가 인정하는 스테이트풀 탐지와 검증된 기술들을 사용하는 주니퍼 네트워크의 IDP는 웹, 트로이 목마, 스파이웨어, 키로거 및 기타 악성 코드들이 네트워크에 침투하거나 이미 감염된 사용자들로부터 확산되는 것을 막는 제로-데이 방어를 제공합니다.

Juniper Networks IDP는 각종 공격들로부터 네트워크를 보호할 뿐만 아니라, 악성 서버들에 대한 정보도 제공합니다. 또한 네트워크에 추가된 알려지지 않은 애플리케이션과 운영시스템의 종류 및 버전에 대해서도 정보를 제공합니다. Juniper Networks IDP 상에서 제공되는 애플리케이션 시그니처들은 P2P나 메신저와 같은 특정 애플리케이션들을 정확하게 탐지할 수 있도록 해줍니다. 네트워크 상에서 사용 중인 애플리케이션들에 대한 구체적인 정보를 확보함으로써 관리자는 보다 손쉽게 보안 정책들을 적용하고 회사의 애플리케이션 사용 정책을 준수할 수 있습니다. Juniper Networks IDP는 또한 DiffServ 마킹을 제공하여 덜 중요한 애플리케이션들에 대해서는 모든 라우터가 대역폭을 제한할 수 있게끔 해줍니다. 관리자들은 특정 애플리케이션들에 대한 액세스를 제어할 수 있을 뿐만 아니라, 비즈니스 크리티컬 애플리케이션들이 예측가능한 QoS를 제공받도록 보장할 수 있습니다.

Juniper Networks IDP 제품들은 Juniper Networks NSM (NetScreen-Security Manager)로 관리됩니다. NSM은 중앙에서 시스템에 대한 정교한 제어 기능을 제공하는 규칙기반 관리 솔루션입니다. NSM은 또한 Extensive Logging, 맞춤형 리포팅, 그리고 하나의 사용자 인터페이스를 통해 모든 주니퍼 방화벽/VPN/IDP 시스템을 관리할 수 있는 기능을 제공합니다. 광범위한 보안, 정교한 네트워크 제어, 가시성, 중앙 관리 기능을 제공하는 Juniper Networks IDP는 기업의 중요한 정보 자산을 안전하게 지켜주는 최고의 솔루션입니다.

Juniper Networks IDP 75는 중소형 기업과 리모트 오피스를 위한 완벽한 IPS 솔루션을 제공합니다. 내장된 ByPass 기능은 비용대비 효과적으로 지속적인 네트워크 가용성을 보장합니다. IPS의 모든 기능과 고도의 복원기능을 제공함으로써 기업이 비용대비 효과적인 IPS 제품을 구축하면서도 최고 수준의 보안을 실현할 수 있도록 해줍니다.

Juniper Networks IDP 250 및 IDP 800은 중대형 기업과 통신사업자를 위한 업계 최고 수준의 IPS 기능들을 제공합니다. 다양한 HA (High Availability) 옵션들을 지원하는 Juniper IDP 250과 IDP 800은 엔터프라이즈 및 통신사업자 네트워크를 위한 연속적인 보안을 보장합니다.

Juniper Networks Integrated Security Gateway (ISG)는 대기업 및 통신사업자의 통합 보안 제품들 구축을 위한 유연한 솔루션을 제공합니다. IDP 보안 모듈 추가 기능이 있는 ISG 제품 라인은 하나의 새 시로 업계 최고 수준의 통합 방화벽, IPSec VPN, IPS 기능을 모두 제공합니다.

Juniper Networks IDP 8200은 실제 처리량 10 Gbps의 업계 최고 성능을 제공하며, 대기업 및 통신사업자에게 적합한 제품입니다. 많은 처리량으로 네트워크 코어와 DMZ에 구축할 수 있으며, 기업 네트워크 내부의 보안과 QoS를 보장합니다. 컨트롤 플레인과 데이터 플레인이 분리되어 있으며 ByPass 기능이 탑재된 IDP 8200은 높은 수준의 처리량과 안정성을 요구하는 네트워크를 위한 이상적인 솔루션입니다.

기능 및 이점

트래픽 탐지 기법

Juniper Networks IDP 제품들은 네트워크를 통과하는 트래픽을 정확하게 탐색하기 위해 8가지 탐지 기법을 동시에 사용합니다. 또한 높은 유연성을 제공함으로써 다양한 탐지 기법들이 오탐지 (False Positives)를 최소화 합니다.

기능	특징 설명	이점
스테이트풀 시그니처 탐지	적합한 프로토콜 컨텍스트에 의해 판별된 네트워크 트래픽의 해당 부분에만 시그니처가 적용됨	오탐지 (False Positives) 최소화
프로토콜 이상 탐지	정식 RFC 이외의 프로토콜 사용에 대한 네트워크 공격성 여부 검사	밝혀지지 않은 취약성들로부터 사전에 네트워크를 보호
백도어 탐지	휴리스틱 (Heuristic) 기반의 변칙 트래픽 패턴 및 패킷 분석을 통해 트로이목마와 루트킷 (Rootkits) 탐지	다른 보안 장치들이 제 기능을 다하지 못할 경우 악성코드의 확산을 방지
트래픽 이상 탐지	휴리스틱 규칙을 통해 탐색이나 공격 등 예상치 못한 트래픽 패턴 탐지	탐색활동이나 DDoS 공격을 사전에 차단
IP 스누핑 탐지	네트워크 내/외부의 어드레스 허용 여부 확인	위장된 소스를 차단하고 허용된 트래픽만 승인
DoS (Denial of Service) 탐지	SYN 플러드 공격으로부터 SYN 쿠키 기반 보호	SYN 플러드 공격으로부터 주요 네트워크 자산 보호
레이어 2 탐지	ARP 테이블 제한, 프래그먼트 핸들링, 연결 시간제한 및 패킷의 바이트 /길이 총량 등에 대한 규칙 사용으로 레이어 2 공격들을 탐지	손상된 호스트가 ARP 캐시 포이즈닝 (Cache Poisoning)과 같은 방법을 사용해 내부 네트워크를 오염시키지 않도록 차단
네트워크 허니팟 (Honeyopt) ¹	개방형 포트가 가짜 리소스 행세를 하면서 침투 활동을 추적	실제 네트워크 위협에 대한 통찰력을 확보하고 중요 자산이 공격 받기 전에 네트워크를 사전 방어

IDP 기능

Juniper Networks IDP 제품들은 최고 수준의 네트워크 보안을 보장하기 위해 여러 가지 독특한 기능들을 제공합니다.

기능	특징 설명	이점
프로토콜 디코드 (Protocol Decodes)	500개 이상의 컨텍스트와 함께 60개 이상의 프로토콜 디코딩이 지원 되기 때문에 적절한 프로토콜 활용 보장	정확한 프로토콜 컨텍스트를 통해 시그니처의 정확도 향상
시그니처 ²	트래픽 이상, 공격, 스파이웨어 및 애플리케이션을 식별할 수 있도록 5500개 이상의 시그니처 제공	공격을 정확하게 식별하고 알려진 취약점을 악용하려는 시도 탐지
트래픽 해석	리어셈블리 (Reassembly), 표준화 및 프로토콜 디코딩 제공	난독화 (Obfuscation) 방법을 사용해 다른 IDP 탐지를 우회하려는 시도 차단
애플리케이션 인식/확인	컨텍스트, 프로토콜 정보 및 시그니처를 사용해 모든 포트 상의 애플리케이션 확인	포트가 아닌 애플리케이션 기반의 규칙 및 정책을 지원함으로써 비표준 포트 상의 표준 애플리케이션 보호 또는 폴리싱 (Policing)
제로-데이 보호	새롭게 발견된 취약점에 대해 프로토콜 이상 탐지 및 당일 지원을 제공	모든 신종 익스플로이트 출현 시 즉각적으로 네트워크 보호 체제 완비
권장 정책	일반 엔터프라이즈가 네트워크를 보호하는 데 중요한 역할을 담당하는 주니퍼 네트워크스의 보안 팀에 의해 공격 시그니처 그룹 파악	설치 및 유지 보수를 단순화하는 동시에 최고 수준의 네트워크 보안 보장

¹ 네트워크 허니팟 기능은 IDP 8200상에서 지원되지 않습니다.

² 2008년 1월 현재 5,560개 시그니처를 제공하고 있으며 매주 약 10개씩 추가됩니다.

정교한 트래픽 제어

다양한 비즈니스 요구사항을 지원하기 위해 Juniper Networks IDP 제품들은 네트워크 상의 트래픽 플로우에 대한 정교한 제어 기능을 제공합니다.

기능	특징 설명	이점
액티브 트래픽 대응	패킷 드롭, 연결 드롭, 클라이언트 종료, 서버 종료, 클라이언트/서버 종료 등과 같은 다양한 대응 방법 지원	공격에 대해 적절한 대응 제공
QoS/DiffServ 마킹	DSCP를 이용한 패킷 마킹	네트워크를 최적화하고 비즈니스 크리티컬 애플리케이션에 필요한 대역폭 보장
패시브 트래픽 대응	로그 및 TCP 리셋과 같은 몇 가지 수동적 대응 방법 지원	현재의 네트워크 위협에 대한 가시성과 가능한 공격을 사전에 방어할 수 있는 능력 제공
VLAN 인식 규칙	VLAN 별로 서로 다른 정책 적용	부서, 고객 및 규제 준수 요구사항에 따라 고유의 정책 적용
권장 조치	주니퍼 네트워크의 보안 팀이 각 공격 객체에 적합한 조치를 권장함	유지 보수가 용이 - 관리자들은 더 이상 매일 같이 발생하는 모든 위협에 대한 적절한 대책을 찾을 필요가 없음
IPAction	지정된 기간 동안 특정 호스트에서 특정 트래픽 흐름에 이르기까지 세분화된 수준으로 액세스를 금지시킬 수 있음	트래픽 이상, DoS 탐지 또는 네트워크 허니팟을 통해 탐지된 DDoS 공격을 개시하려는 시도 차단

중앙 관리

Juniper Networks IDP 및 방화벽 제품들의 중앙 관리는 NetScreen-Security Manager를 통해 이루어집니다. 다수의 플랫폼들을 긴밀하게 통합하는 NSM을 통해 네트워크 전반의 보안 관리를 간편하고 한 눈에 알아보기 쉽게 실행할 수 있습니다.

기능	특징 설명	이점
역할 기반 관리	여러 다른 관리자들의 각기 다른 고유 권한에 따라 100가지 이상의 다양한 활동 배정	다양한 관리자의 역할을 논리적으로 구분 및 적용함으로써 업무 운영 간소화
예약된 보안 업데이트	새로운 공격 객체/시그니처에 따라 IDP 장비를 자동 업데이트	수동 개입 없이 업데이트된 보안 솔루션 제공
도메인	장비, 정책, 보고서 및 기타 관리 활동을 논리적으로 구분	업무 방식에 따라 장비를 그룹화함으로써 비즈니스 운영 준수
객체 잠금 (Object Locking)	관리 설정값을 안전하게 동시 수정할 수 있도록 지원	관리 설정값의 덮어쓰기로 인한 구성 오류 발생 방지
예약된 데이터베이스 백업	NSM 데이터베이스에 대한 자동 백업이 제공됨	구성 이중화 제공
Job Manager	진행 중인 작업과 완료된 작업 확인	다양한 작업 및 IDP 장비의 업데이트 간소화

로그, 리포팅, 알림 기능

Juniper Networks IDP 제품들과 NSM의 통합 운영을 통해 강력한 로그, 리포팅, 알림 기능을 구현할 수 있습니다.

기능	특징 설명	이점
IDP Reporter	각 IDP 어플라이언스에 사전 구성된 실시간 리포팅 기능이 지원됨	중앙 IT 부서의 업무 부담 없이 네트워크 내에 설치된 각 IDP 어플라이언스에서 실시간 상세 보고서 제공
프로파일러 ³	특정 시간대 동안 트래픽 패턴에 대한 정확하면서도 세부적인 정보 수집	네트워크를 비롯해 다양한 애플리케이션 트래픽 혼합으로 인해 발생한 위협에 대한 상세 정보 제공
Security Explorer	양방향 동적 터치그래프 (Touchgraph)로 포괄적인 네트워크 및 애플리케이션 계층 뷰 제공	네트워크 트래픽은 물론, 공격의 세부 사항을 손쉽게 이해할 수 있도록 지원

³ 프로파일러 기능은 IDP 8200에서 지원되지 않습니다.

사양

	IDP 75	IDP 250	IDP 800	IDP 8200
Dimensions and Power				
Dimensions (W x H x D)	17 x 1.69 x 15 in (43.2 x 4.3 x 38.1 cm)	17 x 1.69 x 15 in (43.2 x 4.3 x 38.1 cm)	17 x 3.4 x 19 in (43.2 x 8.6 x 48.3 cm)	17 x 3.4 x 19 in (43.2 x 8.6 x 48.3 cm)
Weight	15 lb	16.5 lb	27 lb	41 lb
A/C Power Supply	100 - 240 VAC 50 - 60 Hz 4.0 - 2.0 A Max 200 W	100 - 240 VAC 50 - 60 Hz 5.0 - 1.5 A Cold Swappable, Max 300 W	100 - 240 VAC 50 - 60 Hz 6.0 - 2.0 A Hot Swappable, Dual Redundant, Max 400 W	100 - 240 VAC 50 - 60 Hz 10.0 - 4.0 A Hot Swappable, Dual Redundant, Max 700 W
D/C Power Supply	N/A	N/A	(Optional) 36 V - 75 VDC, 24 - 11 A Hot Swappable, Dual Redundant, 710 W Max	(Optional) 36 V - 75 VDC, 24 - 11 A Hot Swappable, Dual Redundant, 710 W Max
Mean Time Between Failures (MTBF)	75,000 hrs	73,000 hrs	108,000 hrs	73,000 hrs
Memory	1 GB	2 GB	4 GB	16 GB
Hard Drive	80 GB	80 GB	2 x 74 GB Redundant RAID 1 Array	2 x 74 GB Redundant RAID 1 Array
Ports				
Fixed I/O	Two RJ-45 Ethernet 10/100/1000 with ByPass	Eight RJ-45 Ethernet 10/100/1000 with ByPass	Ten RJ-45 Ethernet 10/100/1000 with ByPass	N/A
Modular I/O Slots	0	0	0	4
Modular I/O Cards	N/A	N/A	N/A	4-Port GE Copper with ByPass 4-Port GE Fiber SFP 4-Port GE SX-ByPass 2-Port 10 GE SR-ByPass
Management	One RJ-45 Ethernet 10/100/1000	One RJ-45 Ethernet 10/100/1000	One RJ-45 Ethernet 10/100/1000	One RJ-45 Ethernet 10/100/1000
High Availability (HA)	N/A	One RJ-45 Ethernet 10/100/1000	One RJ-45 Ethernet 10/100/1000	One RJ-45 Ethernet 10/100/1000
Performance ⁴				
Max Session	10,000	70,000	500,000	5 Million
Throughput	150 Mbps	300 Mbps	1 Gbps	10 Gbps
Redundancy				
Redundant Power	No	No	Yes	Yes
DC	No	No	Yes	Yes
RAID	No	No	Yes	Yes
Built-In Bypass	Yes	Yes	Yes	Yes
Environment				
Operating Temp	41° to 104° F (5° to 40° C)	41° to 104° F (5° to 40° C)	41° to 104° F (5° to 40° C)	41° to 104° F (5° to 40° C)
Storage Temp	-40° to 158° F (-40° to 70° C)	-40° to 158° F (-40° to 70° C)	-40° to 158° F (-40° to 70° C)	-40° to 158° F (-40° to 70° C)
Relative Humidity (Operating)	8% to 90% Noncondensing	8% to 90% Noncondensing	8% to 90% Noncondensing	8% to 90% Noncondensing
Relative Humidity (Storage)	5% to 95% Noncondensing	5% to 95% Noncondensing	5% to 95% Noncondensing	5% to 95% Noncondensing
Altitude (Operating)	10,000 ft (3,048 m)	10,000 ft (3,048 m)	10,000 ft (3,048 m)	10,000 ft (3,048 m)
Altitude (Storage)	40,000 ft (12,192 m)	40,000 ft (12,192 m)	40,000 ft (12,192 m)	40,000 ft (12,192 m)

⁴ 목록에 나와있는 성능, 용량, 기능은 IDP 소프트웨어 버전 4.2r1이 탑재된 IDP 8200 및 4.1r2a이 탑재된 IDP 75, IDP 250, IDP 800 시스템을 기준으로 합니다. 다른 언급이 없는 경우, 표준 테스트 환경에서 권장 정책 실행 하에 최대치를 특정한 값입니다. 실제 결과는 IDP 소프트웨어 버전과 구축에 따라 달라질 수 있습니다. IDP 75, IDP 250, IDP 800, IDP 8200을 지원하는 소프트웨어 버전 전체에 대한 정보는 주니어 Customer Support Center <http://www.juniper.net/customers/support/>에서 확인할 수 있습니다.

주문 정보

Model Number	Description
Juniper Networks IDP Appliances	
IDP75	IDP 75 Intrusion Detection and Prevention Appliance
IDP250	IDP 250 Intrusion Detection and Prevention Appliance
IDP800-BNDL	IDP 800 Intrusion Detection and Prevention Appliance
IDP8200	IDP 8200 Intrusion Detection and Prevention Appliance

I/O Modules for IDP 8200

IDP-10GE-2SR-BYP	IDP 2-Port 10GE with ByPass (SR)
IDP-10GE-2XFP	IDP 2-Port 10GE (SR/LR)
IDP-1GE-4COP-BYP	IDP 4-Port Copper with ByPass
IDP-1GE-4SFP	IDP 4-Port SFP (Non-ByPass)
IDP-1GE-4SX-BYP	IDP 4-Port Fiber with ByPass (SX)
UNIV-SFP-COP	IDP Copper SFP
UNIV-SFP-FLX	IDP Fiber SFP LX
UNIV-SFP-FSX	IDP Fiber SFP SX
UNIV-SFP-FSR	XFP Short Range Fiber Transceiver
UNIV-SFP-FLR	XFP Long Range Fiber Transceiver

Management

NS-SM-5	NetScreen-Security Manager, 5-Device License (Included with IDP Appliance)
NS-SM-10	NetScreen-Security Manager, 10-Device License
NS-SM-25	NetScreen-Security Manager, 25-Device License
NS-SM-50	NetScreen-Security Manager, 50-Device License
NS-SM-100	NetScreen-Security Manager, 100-Device License
	Additional NSM License Options Available

Model Number	Description
Accessories	
UNIV-74G-HDD	Replacement HDD for IDP 800 and IDP 8200
UNIV-PS-710W-DC	DC Power Supply for IDP 800 and IDP 8200
UNIV-PS-400W-AC	AC Power Supply for IDP 800
UNIV-PS-700W-AC	AC Power Supply for IDP 8200
UNIV-PS-300W-AC	AC Power Supply for IDP 250
IDP-FLASH	Installation Media for IDP 75, IDP 250, IDP 800
IDP-FLASH-8200	Installation Media for IDP 8200
UNIV-MR2U-FAN	Replacement Fan for IDP 800
UNIV-HE2U-FAN	Replacement Fan for IDP 8200
UNIV-HE2U-RAILKIT	Rack Mounting Kit for IDP 8200 (Includes Rails)
UNIV-MR2U-RAILKIT	Rack Mounting Kit for IDP 800 (Includes Rails)
UNIV-MR1U-RAILKIT	Rack Mounting Kit for IDP 250 and IDP 75 (Includes Rails)

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 만족시키고 운영 비용을 절감시키며 IT 위험 요소들을 제거합니다.

주니퍼 네트워크에 대하여

주니퍼 네트워크는 High-performance networking을 지향하는 네트워크 업계 선도적인 업체입니다. 주니퍼는 단일 네트워크 상에서 서비스와 애플리케이션 운용을 가속화시킬 수 있는 신뢰성 있는 네트워크 환경 구축을 위해 High-performance network 인프라스트럭처를 제공하는데 주력하고 있습니다. 이러한 High-performance network는 곧 고객에게 High-performance 비즈니스가 가능하게 하는 원동력이 되고 있습니다.

추가 정보는 www.kr.juniper.net에서 확인할 수 있습니다.



한국주니퍼네트웍스(주) 서울시 강남구 역삼 1동 736-1 한솔빌딩 19층 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

EUROPE, MIDDLE EAST, AFRICA REGIONAL SALES HEADQUARTERS

Juniper Networks (UK) Limite
Building 1
Aviator Park
Station Road
Aldlestone
Surrey, KT15 2PG, U.K.
Phone : 44.(0).1372.385500
Fax : 44.(0).1372.385501

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

저작권 © 2008, 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. 본 문서의 다른 모든 상표, 서비스 마크, 등록 상표 또는 등록 서비스 마크는 주니퍼 네트워크 사나 각 소유권자의 자산일 수 있습니다. 주니퍼 네트워크는 본 문서의 오류에 대해 그 어떠한 책임도 지지 않습니다. 주니퍼 네트워크는 사전 통보없이 본 자료를 변경, 수정, 교체 또는 정정할 수 있는 권한을 보유하고 있습니다.

주니퍼 네트워크 솔루션의 구매를 원하시면 주니퍼 네트워크 영업 담당자 또는 공인 리셀러에게 문의해 주십시오.