vSRX 서비스 게이트웨이

제품 소개

vSRX 서비스 게이트웨이는 서비스 프로바이더와 엔터프라이즈를 위한 고급 보안, 강력한 네트워킹, 자동화된 VM(virtual machine) 라이프사이클 관리 기능이 포함된 종합적인 가상 방화벽 솔루션을 제공합니다. vSRX는 보안담당자가 다이나믹한 환경 내에서 방화벽 보안을 구축하고 확장할 수 있도록 해줍니다.

IPS, AppSecure, UTM과 같은 고급 보안 서비스가 포함된 vSRX의 체험버전은 www.juniper.net/ us/en/dm/free-vsrx-trial/에서 다운로드할 수 있습니다.

제품 설명

서버 가상화를 통해 신속하고 효율적으로 서비스를 제공하고자 하는 데이터센터들이 늘어나고 있습니다. 그러나 가상화된 데이터센터는 물리적 자산을 보호할 때보다 보안에 대해 고려해야 할 사항이 더 많습니다.

가상화된 데이터 센터에서는 VM(virtual machine)들의 추가, 이동, 변경이 빈번하게 발생합니다. 따라서 보안 정책과 VM 인스턴스화를 연결하고 VM 이동 시 보안 정책을 추적하여 지속적인 규제 준수를 보장하는 것이 복잡해질 수 있습니다. 간단히 말해, 물리적 환경에서 당연하게 여겨지는 가시성과 제어가 가상화 환경에서는 가상화 자체의 다이나믹하고 유연한 특성으로 인해 쉽게 손실될 수 있는 것입니다.

네트워크 및 보안 담당자는 조직의 보안을 약화시키지 않으면서 가상화와 클라우드 기술의 이점을 활용할 수 있는 적절한 균형점을 찾아야 합니다. 이러한 과제는 안정성, 가시성, 제어 능력을 저하시키지 않으면서 가상화 및 클라우드 환경의 민첩성과 확장성을 통해 최신 위협에 대응할 수 있는 새로운 보안 솔루션을 통해서만 해결할 수 있습니다.

주니퍼는 다양한 수상 경력을 통해 업계에서 인정받은 주니퍼 네트웍스 SRX 시리즈 서비스 게이트웨이의 기능을 vSRX 서비스 게이트웨이를 통해 가상 환경으로 확장함으로써 이러한 과제를 해결합니다. 주니퍼 네트웍스 Junos® OS 기반의 vSRX는 서비스 프로바이더와 엔터프라이즈를 위한 L4-L7 고급 보안 서비스, 강력한 네트워킹, 자동화된 라이프사이클 관리 기능이 통합된 종합적인 가상 보안 솔루션을 제공합니다.

vSRX의 자동 프로비저닝 기능은 네트워크 및 보안 관리자가 방화벽 보안을 신속하고 효율적으로 프로비저닝하고 확장함으로써 가상화 및 클라우드 환경의 다이나믹한 요구를 충족시킬 수 있게 해줍니다. 관리자는 vSRX를 Junos Space Security Director와 결합시킴으로써 공통 중앙 플랫폼에서 물리적 환경과 가상 환경 전반의 정책 구성, 관리, 가시성을 획기적으로 향상시킬 수 있습니다.

소프트웨어를 통해 서비스 중심 애플리케이션을 구축하는 서비스 프로바이더와 조직을 위해 vSRX의 가상화된 네트워크 및 보안 서비스 포트폴리오는 다양한 NFV(Network Functions Virtualization) 유스케이스를 지원합니다. vSRX는 주니퍼 네트웍스 Contrail, OpenContrail 및 기타 타사 솔루션도 지원하며, OpenStack 같은 다른 차세대 클라우드 오케스트레이션 툴과 직접 또는 풍부한 API를 통해 통합될 수 있습니다.

아키텍처 및 주요 구성요소

고급 보안 서비스

전통적인 방화벽, 개별적인 전용 장비와 소프트웨어로 이루어진 분절적인 레거시 시스템으로는 오늘날의 복잡한 공격을 방어할 수 없습니다. 주니퍼의 최신 보안 스위트는 최신 기술을 통해 현대적인 조직의 새로운 요구 사항을 만족시키고, 끊임없이 변화하는 위협 환경에 대처할 수 있도록 해줍니다. 실시간 업데이트는 기술, 정책, 기타 보안 조치가 항상 최신 상태로 유지되도록 보장합니다.

vSRX는 UTM(Unified Threat Management), IDP(Intrusion Detection and Prevention), AppSecure를 통한 애플리케이션 제어 및 가시성 서비스를 포함한 다양하고 강력한 가상화 전문 고급 보안 서비스 세트를 제공합니다.

UTM (Unified Threat Management)

vSRX는 동급 최고의 안티바이러스, 안티스팸, 웹 필터링, 콘텐츠 필터링 기능을 통해 멀웨어, 바이러스, 피싱 공격, 침입, 스팸 및 기타 위협에 대한 종합적인 콘텐츠 보안을 제공합니다.

표 1: vSRX UTM 기능 및 이점

기능	기능 설명	이점
안티바이러스	• 안티바이러스에는 레퓨테이션(reputation), 클라우드 기반 안티바이러스 기능이 포함되어 스파이웨어, 애드웨어, 바이러스, 키로거, 기타 POP3 HTTP, SMTP, FTP 프로토콜을 통해 들어오는 멀웨어를 탐지하고 차단. • 이 서비스는 안티-멀웨어 기술 전문기업인 Sophos Labs과의 제휴을 통해 제공됨.	• 안티바이러스 전문기업을 통해 데이터 유출 및 생산성 손실을 초래할 수 있는 멀웨어 공격에 대한 정교한 보호 제공.
웹 필터링	• 웹 보안 전문기업인 Websense와의 제휴를 통해 더욱 정교한 카테고리 분류(90+ 카테고리)를 통한 강력한 웹 필터링 및 실시간 위협 파악(scorecard) 제공.	• 악성 URL로 인한 생산성 손실을 방지하고, 주요 비즈니스 트래픽을 위한 네트워크 대역폭 유지를 지원.
콘텐츠 필터링	• MIME 타입, 파일 확장자, 프로토콜 명령어를 기반으로 한 효과적인 인바운드 및 아웃바운드 콘텐츠 필터링.	• 네트워크 상의 악성 콘텐츠 및 부주의한 파일 전송을 차단하여 보안 침해 또는 데이터 유출의 리스크를 최소화.
안티스팸	• 보안전문기업인 Sophos Labs과의 제휴을 통해 다단계 스팸 방어, 최신 피싱 URL 탐지, 표준기반 S/MIME, Open PGP 및 TLS 암호화, MIME 타입 및 Extension Blocker 제공.	• 정교한 이메일 필터링 및 Content Blocker를 통해 소셜 네트워킹 공격을 통한 APT(advanced persistent threats) 및 최신 피싱 공격들에 대한 방어 제공.

IPS (Intrusion Prevention System)

vSRX용 IPS는 데이터 검사를 통해 진행 중인 공격을 선제적으로 차단하는 대응 조치를 실행하거나, 방화벽 내에 일련의 규칙을 생성함으로써 IT 네트워크에 대한 액세스를 제어하고 시스템을 공격으로부터 보호합니다. IPS는 주니퍼의 애플리케이션 보안 기능을 네트워크 인프라에 통합하여 위협을 무력화시키고 다양한 공격과 취약점들로부터 보호합니다.

표 2: vSRX IPS 기능 및 이점

기능	기능 설명	이점
Stateful 시그니처 검사	해당되는 프로토콜 컨텍스트에 따라 결정된 네트워크 트래픽의 관련 부분에만 시그니처가 적용됨	오탐 최소화 및 유연한 시그니처 개발 지원
프로토콜 디코딩	65가지 이상의 프로토콜 디코딩 및 500 가지 이상의 컨텍스트를 지원함으로써 프로토콜의 적절한 사용을 보장.	정확한 프로토콜 컨텍스트를 통해 시그니처의 정확도 향상
시그니처	트래픽 이상, 공격, 스파이웨어 및 애플리케이션을 식별할 수 있도록 8,500개 이상의 시그너처 제공	공격을 정확하게 식별하고 알려진 취약점을 악용하려는 시도 탐지
트래픽 표준화	리어셈블리(reassembly), 표준화(normalization) 및 프로토콜 디코딩 제공	난독화(obfuscation) 기법을 사용해 다른 IPS 탐지를 우회하려는 시도 차단
제로 데이(Zero-day) 보호	새롭게 발견된 취약점에 대해 프로토콜 이상 탐지 및 당일 지원을 제공	모든 신종 익스플로이트 출현 시 즉각적으로 네트워크 보호 체제 완비
권장 정책	주니퍼 네트웍스 보안 팀이 일반적인 엔터프라이즈의 네트워크 보호에 필수적인 공격 시그너처 파악.	설치 및 유지 보수를 단순화하는 동시에 최고 수준의 네트워크 보안 보장
액티브/ 액티브 트래픽 모니터링	액티브/액티브 vSRX 섀시 클러스터를 포함한 IPS 모니터링	액티브/액티브 IPS 모니터링 지원
패킷 캡처 (Packet capture)	IPS 정책이 규칙 별로 패킷 캡처 로깅(packet capture logging)을 지원.	주변 트래픽에 대한 심층 분석을 실행하고 타겟 보호를 위한 추가적인 대응책을 결정.

AppSecure를 통한 애플리케이션 가시성 및 제어

AppSecure는 vSRX 및 SRX 시리즈 서비스 게이트웨이를 위한 차세대 애플리케이션 보안 스위트로서 위협 사항들에 대한 가시성, 보호, 정책 적용, 제어를 제공합니다.

Facebook과 같은 클라우드 기반 애플리케이션에 매일 얼마나 많은 사용자들이 액세스하고 있는지를 파악해야 할 때나, 어떤 애플리케이션이 가장 많은 대역폭을 사용하고 있는지를 파악해야 할 때 모두 AppSecure가 강력한 가시성과 지속적인 애플리케이션 추적을 제공합니다. 오픈 시그니처를 통해 조직의 비즈니스 우선 순위에 따른 애플리케이션 세트를 모니터링하고, 측정하고, 제어할 수 있습니다.

표 3: AppSecure for vSRX 기능 및 이점

기능	기능 설명	이점
AppTrack	애플리케이션 데이터를 분석하고 리스크 레벨, 존(zone), 소스, 대상 주소를 기준으로 분류.	애플리케이션 사용 추적 기능을 제공함으로써 고위험 애플리케이션 식별 및 트래픽 패턴 분석을 지원하고 네트워크 관리 및 제어 강화.
AppFW	다이나믹 애플리케이션 네임 또는 그룹 네임을 기반으로 트래픽 허용/차단을 실행하는 애플리케이션 제어 정책 생성.	전통적인 포트 및 프로토콜 분석이 아닌, 애플리케이션 및 사용자 역할을 기반으로 한 보안 정책 설정 및 실행 강화.
AppQoS	관리자가 설정한 애플리케이션 보안 정책을 기준으로 트래픽 측정 및 표시.	애플리케이션 정보 및 컨텍스트를 기반으로 트래픽을 우선순위화하고 대역폭을 제한, 쉐이핑하는 기능을 제공함으로써 애플리케이션 및 전체 네트워크 성능을 향상시킴.

Juniper Sky Advanced Threat Prevention

주니퍼 Sky™ Advanced Threat Prevention은 vSRX와 통합되어 알려진 멀웨어와 최신 제로데이 위협에 대한 동적인 자동 방어와 즉각적인 대응을 제공합니다.

표 4: AppSecure for vSRX 기능 및 이점

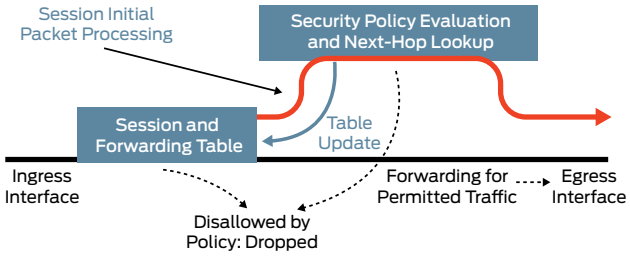
기능	이점
딥 인스펙션 및 분석	알려진 위협을 신속하게 파악하고 심층 파일 분석을 통해 우회성 멀웨어를 탐지하기 위해 감염된 파일을 추출하여 클라우드로 전송합니다.
즉각적인 식별을 통한 공격 차단	멀웨어를 즉각적으로 식별하고 SRX 시리즈 방화벽에 탐지된 멀웨어 정보를 전송하여 공격을 차단합니다.
다양한 리포팅 및 분석 툴을 갖춘 웹 포털	구성, 제품 업데이트 등의 관리 작업수행을 위한 웹 기반 인터페이스를 제공합니다. 또한 위협과 감염된 호스트에 대한 가시성을 제공하는 다양한 리포팅 및 분석 툴을 지원합니다.
시스템 및 호스트 격리	분석 기능을 통해 관리자와 보안 담당자가 데이터 분석 및 상관관계 분석(correlation)을 실행할 수 있도록 해줍니다. 아울러 감염된 시스템을 파악하고 관련 정보를 SRX 시리즈 방화벽으로 전송하여 해당 시스템들을 격리시킵니다.
Spotlight Secure 통합	Spotlight Secure Threat Intelligence 서비스와 통합되어 SRX 시리즈 방화벽에 위협 정보를 전송함으로써 즉각적인 대응을 지원합니다.
C&C(Command and control) 데이터	SRX 시리즈 방화벽에 C&C 데이터를 제공하여 감염된 내부 시스템들이 해당 기기들과 통신하지 못하도록 합니다.
이메일 분석 및 치료	악성 멀웨어를 격리하고, 이메일이 공격 벡터로 사용되는 것을 방지합니다. 머신러닝 알고리즘으로 이메일 트래픽을 분석하여 악성 첨부파일을 탐지하고 방화벽에서 해당 파일을 차단합니다.
위협 인텔리전스	강력한 오픈 API를 사용하여 써드파티 벤더와 매끄러운 통합이 가능합니다. 이를 통해 다수의 위협 인텔리전스 피드를 제공하고 공격 노출을 줄입니다.

간단한 구성

vSRX는 존(zone)과 정책의 두 가지 기본 기능을 사용합니다. 기본 구성에는 "트러스트(trust)" 존과 "언트러스트(untrust)" 존이 포함됩니다. 트러스트 존은 내부 네트워크를 vSRX에 연결하고 구성하는 데 사용됩니다. 언트러스트 존은 일반적으로 신뢰할 수 없는 네트워크에 사용됩니다. 설치를 간소화하고 구성을 단순화하기 위해, 트러스트 존으로부터 온 트래픽은 언트러스트 존으로 흐를 수 있지만, 언트러스트 존에서 온 트래픽은 트러스트 존으로 들어갈 수 없도록 차단하는 기본 정책이 설정되어 있습니다. 기존의 라우터는 방화벽(세션 인식) 또는 정책(세션의 발생지 및 목적지)과 관계없이 모든 트래픽을 포워딩합니다. 또한 vSRX의 가상화 특성 덕분에 고객은 스냅샷, 클로닝(cloning) 및 관련 기술을 활용하여 유지 관리와 운영 작업을 간소화할 수 있습니다.

통합된 라우터와 방화벽의 처리량 및 지연을 최적화하기 위해 Junos OS는 기존 방화벽의 세션 상태 정보와 클래식 라우터의 넥스트 홉 포워딩을 단일 운영으로 결합하는 혁신적 기술인 세션 기반 포워딩을 구현합니다. Junos OS를 통해, 포워딩 정책에 따라 허용된 세션이 넥스트 홉 경로로 연결되는 포인터(pointer)와 함께 포워딩 테이블에 추가됩니다.

이 효율적인 알고리즘은 다수의 테이블 룩업(table lookup)을 실행하여 세션 정보를 검증한 후 넥스트 홉 경로를 검색하는 클래식 라우터에 비해 세션 트래픽에 대한 처리량을 높이고 대기 시간을 단축할 수 있습니다. 설정된 세션에 대한 후속 패킷은 세션 및 포워딩 테이블 내 단일 테이블 룩업을 필요로 하며, Egress 인터페이스로 포워딩됩니다. 보안 정책은 한 영역에서 발생한 세션이 다른 영역으로 포워딩될 수 있는지를 결정합니다. vSRX는 패킷을 수신하고 모든 세션과 애플리케이션, 사용자를 추적합니다. VM이 가상화된 환경이나 클라우드 환경 내에서 이동하는 동안에도 처리할 패킷을 vSRX에 계속 보냄으로써 안전 모드에서 계속 통신할 수 있습니다.



HA (High Availability)

vSRX는 Active/Active 및 Active/Passive 모드에 대한 섀시 클러스터링을 지원하여 업무에 필수적인 안정성을 제공합니다. HA 기능은 처리 중인 모든 연결은 물론 하이퍼바이저 상의 클러스터 멤버들에 대해서도 완벽한 스테이트풀 페일오버(stateful failover)를 제공합니다. 클러스터에서 vSRX VM이 구성될 때, VM은 연결/세션 상태 및 플로우 정보, IPsec 보안 연결, NAT(Network Address Translation) 트래픽, 주소록 정보, 구성 변경 등과 같은 정보를 동기화합니다. 그 결과, 페일오버 도중 보존된 세션뿐만 아니라 보안도 그대로 유지됩니다. 불안정한 네트워크에서는 vSRX가 링크 플래핑(link flapping)을 완화합니다.

성능

예전에는 고객이 확장성과 성능 사이에서 양자택일의 고민을 해야 했습니다. vSRX 솔루션은 여러 개의 가상 CPU를 활용하여 가상 환경에서 패킷 처리 및 전체 처리량을 극대화하도록 최적화되었습니다. 또한 각 vSRX VM에 여러 개의 vNIC (virtual network interface cards)가 있는데, 이를 다양한 가상 네트워크에 연결하여 여러 네트워크 세그먼트를 동시에 보호할 수 있습니다. 가상 패브릭 내에서 작동하는 vSRX는 가상화된 환경이나 클라우드 기반 환경을 지원하는 데 필요한 뛰어난 성능과 강력한 보안의 두 가지 이점을 모두 제공합니다.

표 5 : vSRX 서비스 게이트웨이 주요 성능 지표

Performance and Capacity[1]	VMware VMXNET3		KVM Virtio with OVS-DPDK	
vCPUs	2	5	2	5
Memory	4 GB	8 GB	4 GB	8 GB
Firewall throughput, large packet (1514B)	8 Gbps	20 Gbps	17 Gbps	20 Gbps
Firewall throughput, IMIX	2 Gbps	5.4 Gbps	4 Gbps	5.4 Gbps
AES+GCM IPSec VPN throughput (1420B)	2.7 Gbps	7 Gbps	2.7 Gbps	7 Gbps
Application visibility and control[2]	2.9 Gbps	8.3 Gbps	2.9 Gbps	8.3 Gbps
IPS recommended signatures	1.8 Gbps	5.2 Gbps	1.8 Gbps	5.2 Gbps
TCP connections per second	50,000	60,000	50,000	60,000
Maximum concurrent sessions	512,000	1,000,000	512,000	1,000,000

[1] 성능 레퍼런스 플랫폼: HP DL580 Gen 9 E7-8890 v3, 72 CPU * 2.493 Ghz; HT: Disabled with Intel 82599 NIC ixgbe version: 4.21; firmware version: 0x80000208; VMware version: 6.0; build: 3620759; KVM: Ubuntu 16.04 OpenVSwitch (OVS): 2.7.0. 기반입니다. 모든 성능 수치는 "최대치"이며 기본 하드웨어 구성에 따라 다릅니다(일부 서버 구성에서 성능이 더 높을 수 있음). 목록의 성능, 용량, 기능은 Junos OS 15.1X49-D70 릴리즈를 사용하는 vSRX를 기준으로 하며, 이상적인 테스트 조건에서 측정된 수치입니다. 실제 결과는 Junos OS 릴리즈 및 구축 환경에 따라 다를 수 있습니다.

[2] 처리량은 44KB 크기 트랜잭션, HTTP 트래픽 기준입니다.

*Number of cores should be power of 2 + 1 (i.e. $2^n + 1$)

vSRX는 스케일업(scale-up) 모델을 활용하여 고객이 가상 보안 용량을 유연하게 업그레이드할 수 있도록 해줍니다. 새로운 인스턴스 이미지를 인증할 필요없이 동일한 인스턴스에 vCPU 최소 2개 이상의 코어*를 추가하는 것만으로 용량 업그레이드가 가능합니다. vSRX는 싱글 소켓에서 vCPU 17개를 사용하여 최고 100 Gbps 성능을 실현할 수 있습니다.

표 6 : vSRX 시스템 요구사항4

CPU Cores	2	5
Memory	4 GB	8 GB
Disk Space	16 GB	16 GB
Network Drivers - VMware ESXi	VMXNET3, SR-IOV on Intel X710/XL710 or X520/X540	VMXNET3
Network Drivers KVM	Virtio, SR-IOV on Intel X710/XL710 or X520/X540	Virtio, SR-IOV on Intel X710/XL710

Junos Space Security Director

Junos Space Security Director는 직관적인 중앙 웹 기반 인터페이스를 통해 최신 리스크 경로와 기존 리스크 경로 전반에 대한 보안 정책 관리를 제공합니다. Junos Space 플랫폼 상에서 실행되는 애플리케이션인 Security Director 는 광범위한 보안 커버리지, 세분화된 정책 제어, 네트워크 전반에 대한 폭넓은 정책을 제공합니다. 관리자가 스테이트풀 방화벽, UTM, IPS, AppFW, VPN, NAT에 대한 보안 정책 라이프사이클의 모든 단계를 빠르게 관리할 수 있게 도와줍니다.

통합 관리

Junos Space Security Director의 성능을 활용해 관리자는 공통의 중앙 플랫폼에서 물리적 환경과 가상 환경 전반의 정책 구성, 관리, 가시성을 획기적으로 향상시킬 수 있습니다.

주요 기능 및 이점

- 스테이트풀 패킷 처리 및 애플리케이션 레이어 게이트웨이 기능을 갖춘 완전한 방화벽을 VM 형태로 제공함으로써 멀티테넌트 프라이빗 및 퍼블릭 클라우드 환경을 보호
- SRX 시리즈 서비스 게이트웨이와 동일한 일관된 고급 보안 및 네트워킹 기능(IPsec VPN, NAT, QoS 및 모든 라우팅 기능) 활용
- 강력한 UTM, IPS와 애플리케이션 가시성 및 제어 기능을 통합한 종합적인 위협 관리 프레임워크를 제공하여 갈수록 복잡해지는 위협 환경으로부터 안전하게 보호
- 오픈 RESTful API를 통한 관리 유연성 향상으로 타사 관리 및 클라우드 오케스트레이션 툴과의 통합 지원
- Junos Space Security Director를 통해 방화벽 보안 정책 구성과 관리에 대한 가시성 및 제어를 가상 및 비가상 환경 전반으로 확장
- Contrail, OpenContrail 및 기타 타사 솔루션과의 통합을 통해 SDN및 NFV 지원

Amazon Web Services 마켓플레이스에서 구매 가능

vSRX는 AWS (Amazon Web Services) 마켓플레이스에서 구매 가능하며 AWS VPC, 프라이빗 클라우드, 온프레미스 리소스에 대한 고급 네트워크 및 애플리케이션 보안과 안전한 IPsec VPN 연결을 제공합니다. 고객은 Junos Space Security Director를 사용하여 온프레미스 및 AWS VPC 전반의 SRX 시리즈 서비스 게이트웨이들에서 일관된 보안 정책을 관리할 수 있습니다. vSRX on AWS를 사용하는 고객은 자체 vSRX 라이센스를 가져오거나 사용량 기반 과금방식(pay-as-you-go, 시간당 또는 연간)을 통해 지불할 수 있습니다.

Microsoft Azure 마켓플레이스에서 구매 가능

vSRX는 Microsoft Azure 마켓플레이스와 Microsoft Azure Government에서 구매 가능하며 Azure 가상 네트워크에 대한 안전한 IPsec VPN 연결과 고급 차세대 보안을 제공합니다. 고객은 Junos Space Security Director를 사용하여 온프레미스 및 Azure 가상 네트워크 전반의 SRX 시리즈 차세대 방화벽들에서 일관된 보안 정책을 관리할 수 있습니다. vSRX는 자체 Microsoft Azure 마켓플레이스와 Microsoft Azure Government에서 BYOL(Bring-YourOwn-License) 모델로 구매 가능합니다.

주니퍼 네트웍스 서비스 및 지원

주니퍼는 하이 퍼포먼스 네트워킹의 가치를 가속, 확장, 최적화시키는 성능 보장 서비스를 제공합니다. 주니퍼 서비스를 통해 고객은 운영 효율성을 극대화하고, 비용을 절감하며, 리스크를 최소화고, 네트워크 가치를 신속하게 실현할 수 있습니다. 주니퍼 네트웍스는 네트워크를 최적화함으로써 고객이 필요로 하는 성능, 안정성, 가용성을 유지하고 뛰어난 운영 효율성을 실현하도록 보장합니다. 보다 자세한 사항은 http://www.juniper.net/kr/kr/products-services/에서 확인할 수 있습니다.

사양

다음 표에는 주요 사양이 나와 있습니다. 전체 목록을 보려면 제품 설명서를 참조하십시오.

표 7 : vSRX 서비스 게이트웨이 사양

Protocols	IP Address Management	Security	SLA, Measurement, and Monitoring	Hypervisors
• IPv4, IPv6, MPLS, ISO Connectionless Network Service (CLNS) • Static routes • RIPv2 +v1 • OSPF/OSPFv3 • BGP • IS-IS • Multicast (Internet Group Management Protocol, PIM, Session Description Protocol) • MPLS • VPLS	• Static • Dynamic Host Configuration Protocol (DHCP) • Internal DHCP server, DHCP relay • Address Translation • Source NAT with Port Address Translation (PAT) • Static NAT • Destination NAT with PAT • Persistent NAT, NAT64 • Encapsulations • Ethernet • 802.1q VLAN support	• Firewall • Firewall, zones, screens, policies • Stateful firewall, stateless filters • Network attack detection • Screens denial of service (DoS) and distributed DoS (DDoS) protection (anomaly-based) • Replay attack prevention; anti-replay • Unified access control (UAC) • TCP reassembly for fragmented packet protection • Brute force attack mitigation • SYN cookie protection • Zone-based IP spoofing • Malformed packet protection • VPN • Tunnels (generic routing encapsulation, IP-IP) • IPsec, Data Encryption Standard (DES) (56-bit), triple Data Encryption Standard (3DES) (168-bit), Advanced Encryption Standard (AES) (128-bit+) encryption • Message Digest 5 (MD5), SHA-1, SHA-128, SHA-256 authentication • IPv6	• Real-time performance monitoring (RPM) • Sessions, packets, and bandwidth usage • IP monitoring • Logging • System logging • Traceroute • Extensive control and data plane structured and unstructured system log administration • Junos Space Security Director support • Juniper Networks Secure Analytics • Juniper Networks Advanced Insight Solutions support • External administrator database (RADIUS, LDAP, SecureID) • Auto-configuration • Configuration rollback • Rescue configuration with button • Commit confirm for changes • Auto-record for diagnostics • Software upgrades • J-Web • CLI	• VMware ESXi 5.5, 6.0; KVM/QEMU: - CentOS 7.1 - Ubuntu 14.04, 16.04 - RHEL 7.2 • Hyper-V 2012, 2012R2, 2016

주문 정보

주니퍼 네트웍스 vSRX 가상 방화벽에 대한 자세한 정보는 www.juniper.net/us/en/products-services/security/srx-series/vsrx를 참조하거나, 주니퍼 네트웍스 영업 담당자에게 문의해 주십시오. vSRX 무료 체험버전은 www.juniper.net/us/en/dm/free-vsrx-trial/에서 확인할 수 있습니다.

주니퍼 네트웍스에 대하여

주니퍼 네트웍스는 네트워크 업계의 혁신을 선도하는 제품과 솔루션, 서비스를 개발하기 위해 끊임없이 도전하고 있다. 주니퍼 네트웍스는 탁월한 확장성 및 안전성, 자동화를 바탕으로 높은 민첩성과 성능, 가치를 제공하는 네트워크를 구현하기 위해 고객 및 파트너와 함께 혁신을 거듭하고 있다. 자세한 정보는 주니퍼 네트웍스 웹사이트와 블로그, 트위터 및 페이스북을 통해 확인할 수 있다.

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

본사
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

아태지역 및 EMEA 본부
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

주니퍼 네트웍스 솔루션에 대한 구매 문의는 한국주니퍼네트웍스 (전화 02-3483-3400, 이메일 salesinfo-korea@juniper.net)로 연락주십시오.

주니퍼 둘러보기
앱 다운로드

1000489-011-KR Nov 2017