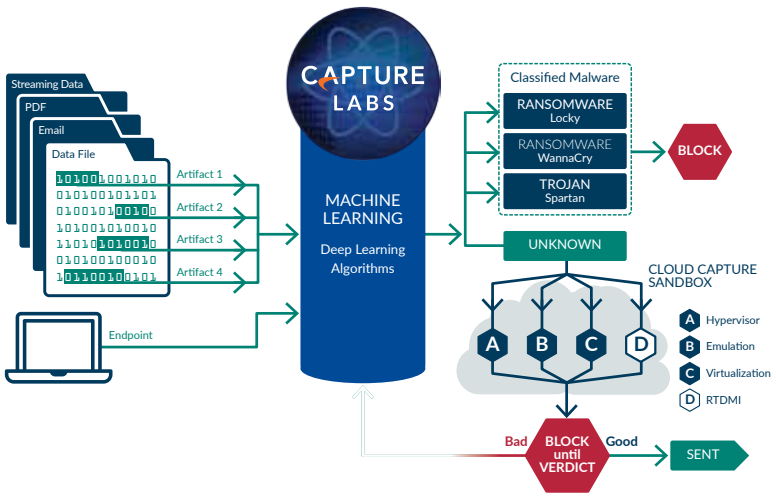
SonicWall NSv(Network Security virtual) 시리즈

공용, 사설, 하이브리드 클라우드 환경을 위한 차세대 보안 솔루션

가상화, 클라우드와 같은 최신 네트워크 아키텍처의 설계, 구현, 배포는 많은 조직에게 계속해서 판도를 바꾸는 전략이 되고 있습니다. 데이터 센터의 가상화나 클라우드로의 마이그레이션, 또는 이 둘의 조합은 운영과 경제적인 부분에서 중요한 장점이 있습니다. 하지만 가상 환경의 취약점은 잘 드러나 있습니다. 심각한 보안 문제와 과제를 야기하는 새로운 점들이 계속 발견됩니다. 애플리케이션 서비스가 안전하고 효율적이며 확장 가능한 방식으로 제공되려면, VM(가상 머신), 애플리케이션 워크로드, 데이터가 포함된 가상 프레임워크의 모든 부분에 유해한 위협 요소에 맞서 싸우는 것이 최우선 순위가 되어야 합니다.

SonicWall NSv(Network Security virtual) 방화벽은 보안 팀이 비즈니스 크리티컬 서비스와 운영에 심각한 장애를 일으킬 수 있는 이러한 종류의 보안 위험과 취약점을 줄일 수 있도록 합니다. NSv는 RFDPI(Reassembly-Free Deep Packet Inspection), 보안 제어, SonicWall 물리적 방화벽과 동일한 기능을 가진 네트워킹 서비스를 포함한 모든 기능을 갖춘 보안 도구와 서비스를 통해 사설 클라우드나 공용 클라우드 환경의 모든 중요한 구성 요소를 효과적으로 보호합니다.

NSv는 다중 테넌트 가상 환경, 일반적으로 VN(가상 네트워크) 사이에 쉽게 배포하고 프로비저닝할 수 있습니다. 이를 통해 자동화된 위반 방지 기능으로 가상 머신 간의 통신과 데이터 교환을 캡처하고, 데이터 기밀성 및 VM 안전과 무결성을 위한 엄격한 액세스 제어 방법을 만들 수 있습니다. SonicWall의 포괄적인 보안 검사 서비스[1]로 보안 위협(가상 머신 사이나 사이드 채널 공격, 일반적인 네트워크 기반 침입, 애플리케이션과 프로토콜 취약성)이 성공적으로 진압됩니다. 모든 VM 트래픽은 침입 방지, 게이트웨이 안티 바이러스와 안티 스파이웨어, 클라우드 안티 바이러스, 봇넷 필터링, 애플리케이션 제어와 Capture ATP(Capture Advanced Threat Protection) 다중 엔진 샌드박싱을 포함한 여러 위협 분석 엔진을 거치게 됩니다.



장점:

공용 클라우드와 사설 클라우드 보안

- 성능에 영향을 미치지 않고 클라우드의 민첩성, 확장성, 보안을 활용하는 차세대 방화벽 기능 구현
- 자동화된 실시간 위협 방지를 위해 가상 인프라를 완벽하게 파악하고 제어
- 가상 환경 전체의 각 영역에 적용할 보안 정책을 적절하게 배치
- VM 위치에 관계없이 애플리케이션, 사용자, 장치별로 안전한 애플리케이션 실행 규칙 제공
- 적절한 보안 영역 분할, 격리와 함께 다중 테넌시와 마이크로 세분화 활용
- 사설 클라우드 플랫폼(ESXi)과 공용 클라우드 플랫폼(AWS[2], Azure)을 모두 지원

가상 머신 보호

- Capture ATP(Advanced Threat Protection)를 사용하여 제로 데이 취약점을 방어
- 가상 시스템의 무단 점유 방지
- 보호되는 데이터 자산에 대한 무단 액세스 중지
- 맬웨어 전파, 운영 체제 명령 실행, 파일 시스템 탐색, C&C 통신과 같은 악성 행위와 침입 행위 차단
- 가상 에코시스템의 일부나 전체의 서비스 중단 방지

분할 보안

APT(지능형 지속 위협)에 대응하여 최적의 효과를 내기 위해서는 네트워크 보안 세그먼트에 지능형 위협에 대처할 수 있는 동적인, 강제 적용이 가능한 장벽을 사용해야 합니다. 세그먼트 기반의 보안 기능을 통해 NSv는 각 인터페이스에 동일한 정책을 쓰는 것이 아니라 비슷한 인터페이스를 그룹으로 묶어 정책을 적용 할 수 있습니다. VN 내부에 보안 정책을 적용함으로써, 네트워크 리소스를 여러 세그먼트로 나누고 각 세그먼트 사이의 트래픽을 허용하거나 제한하도록 분할을 구성할 수 있습니다. 이 방식으로 중요한 내부 리소스에 대한 액세스를 엄격하게 제어하게 됩니다.

NSv는 사용자 ID 자격 증명, Geo-IP 위치, 모바일 엔드포인트의 보안 수준과 같은 동적 기준으로 분할 제한을 자동으로 적용할 수 있습니다. 또한 보안 강화를 위해 NSv는 다중 기가비트 네트워크 스위칭을 보안 구역 정책과 시행에 포함시킬 수 있습니다. 네트워크 전체의 스위칭 지점에서 트래픽에 세그먼트 정책을 적용하고, 하나의 창에서 세그먼트 보안 정책 시행을 전체적으로 관리합니다.

세그먼트는 그 사이에 보안 정책을 시행할 수 있어야만 효과적이기 때문에 NSv는 IPS(침입 방지 서비스)로 VLAN 세그먼트의 수신 및 발신 트래픽을 검사하여 내부 네트워크 트래픽에 대한 보안을 강화합니다. 각 세그먼트에 대해서는 적용 가능한 정책을 기반으로 여러 인터페이스에 완전한 보안 서비스를 시행합니다.

유연한 배포 사용 사례

HA(고가용성) 구현을 위한 인프라를 통해 NSv는 SDDC(소프트웨어 정의 데이터 센터)의 확장성과 가용성 요구 사항을 충족시킵니다. 시스템 탄력성, 서비스 안정성, 규정 준수를 보장하며 공개, 사설, 하이브리드 등 다양한 사용 사례에 최적화된 NSv는 서비스 수준 변경에 적응할 수 있고 VM과 애플리케이션 워크로드, 데이터 자산을 이용할 수 있는 상태로, 안전하게 유지할 수 있습니다. 이러한 모든 기능을 여러 Gbps 속도와 낮은 지연 시간으로 발휘합니다.

조직에서는 가상화의 운영 및 경제적 혜택뿐 아니라 물리적 방화벽이 가진 보안상 장점도 모두 누릴 수 있습니다. 여기에는 시스템 확장성, 운영 민첩성, 프로비저닝 속도, 간단한 관리, 비용 절감이 포함됩니다.

NSv 시리즈는 다양한 범위의 가상 및 클라우드 배포 사용 사례를 위해 마련된 여러 가상 버전으로 이용할 수 있습니다. 여러 기가비트 위협 예방과 암호화된 트래픽 검사 기능을 갖춘 NSv 시리즈는 용량 수준의 증가에 적응할 수 있으며, VN 안전과 애플리케이션 워크로드, 데이터 자산을 안전하게 사용할 수 있도록 돕습니다.

중앙 관리

NSv 배포 환경은 중앙에서 관리됩니다. 내부에서 SonicWall GMS[3]와 SonicWall Capture Security Center[3] 모두를 사용해서 관리되는데, 이는 공개형이고 확장 가능한 클라우드 보안 관리, 모니터링, 보고, 분석 소프트웨어이며 경제적인 서비스형 솔루션으로 제공됩니다.

Capture Security Center는 모든 SonicWall 가상 방화벽과 물리적 방화벽 에코시스템을 하나의 창에서 명확하고 정확하며 빠르게 관리할 수 있도록 최고의 가시성, 민첩성, 수용력을 갖추고 있습니다.

기능

SonicOS 플랫폼

SonicOS 아키텍처는 NSv와 NS*a* 시리즈, SuperMassive ™ 시리즈와 TZ 시리즈를 포함하여 모든 SonicWall 물리적 방화벽과 가상 방화벽의 핵심입니다. SonicWALL SonicOS 플랫폼 데이터 시트에서 기능의 전체 목록을 참조하세요.

자동화된 위반 방지[1]

여기에는 고성능 침입과 맬웨어 방지, 클라우드 기반 샌드박싱을 비롯한 완전한 고급 위협 방지 기능이 포함됩니다.

24시간 보안[1]

새로운 위협 업데이트는 능동적인 보안 서비스로 현장의 방화벽에 자동으로 전송되어 재부팅이나 실행 중단없이 즉시 적용됩니다.

파트너 지원 서비스

SonicWall 솔루션의 계획이나 배포, 최적화에 도움이 필요하세요? SonicWall Advanced Services Partner는 세계적 수준의 전문 서비스를 제공할 수 있도록 교육을 받았습니다. www.sonicwall.com/PES 에서 자세히 알아보세요.

제로 데이 보호[1]

NSv는 수천 가지 개별 악용 사례를 활용하는 교묘한 최신 악용 방법과 기법에 대응하여 지속적으로 업데이트된 기술을 사용하여 제로 데이 공격으로부터 보호합니다.

위협 API

NSv는 제로 데이, 악의적인 내부자, 위조된 자격 증명, 랜섬웨어, 지능형 지속 위협과 같은 지능형 위협에 대처하기 위해 원래 장비의 독점 제조업체와 타사 인텔리전스 피드를 받아 활용합니다.

영역 보호

NSv는 네트워크를 여러 보안 영역으로 나누어 침입 방지 서비스로 위협이 영역 경계를 넘어 전파되는 것을 방지함으로써 내부 보안을 강화합니다. 다양한 인터페이스를 통과하는 트래픽을 위해 액세스 규칙과 NAT 정책을 만들고 적용함으로써, 다양한 기준에 따라 내부나 외부 네트워크 액세스를 허용하거나 거부할 수 있습니다.

애플리케이션 인텔리전스와 제어[1]

NSv는 애플리케이션별 정책을 사용하여 사용자, 이메일 주소, 일정, IP 서브넷 기준으로 네트워크 트래픽을 세부적으로 제어합니다. 맞춤형 애플리케이션은 각각의 고유한 매개 변수나 패턴을 기반으로 서명을 만들어 제어합니다. 내부나 외부 네트워크 액세스는 다양한 기준에 따라 허용하거나 거부할 수 있습니다.

중앙 관리

- 네트워크 보안 방어 프로그램을 통합할 수 있는 포괄적인 보안 관리, 분석 보고, 규정 준수를 손쉽게 할 수 있음
- 워크플로를 자동화하고 상호 연관시켜 완전하게 조정된 보안 관리, 규정 준수, 위험 관리 전략 수립

규정 준수

- PCI, HIPAA, SOX 보안 보고를 자동화하여 규제 기관과 감사원의 요구 사항 충족
- 특정 감사 규정을 지킬 수 있도록 보안 감사를 할 수 있는 데이터를 어떤 방식으로든 조합하여 맞춤화 가능

위험 관리

- 공유된 보안 체계 전반에 걸쳐 빠르게 대응하고 공동 작업, 소통, 지식을 이끌어냄
- 높은 수준의 보안 효율을 위해 시간에 민감한 통합된 위협 정보를 기반으로 정보 보안 정책 결정

GMS는 보안 관리, 규정 준수, 위험 관리를 위한 전체적인 접근 방식을 제공합니다.

데이터 유출 방지

NSv는 데이터 스트림에서 특정 키워드를 검사할 수 있습니다. 이렇게 하면 특정 파일 이름, 파일 형식, 이메일 첨부 파일, 첨부 파일 형식, 제목을 가진 이메일과 특정 키워드나 바이트 패턴이 있는 이메일이나 첨부 파일의 전송이 제한됩니다.

애플리케이션 계층 대역폭 관리

NSv는 패킷 모니터를 사용하여 다양한 대역폭 관리 설정 중에서 선택할 수 있으므로 애플리케이션의 네트워크 대역폭 사용이 줄어듭니다. 이는 네트워크 제어에도 도움이 됩니다.

안전한 통신

NSv는 가상 머신 그룹 사이의 데이터 교환이 안전하게 이루어지도록 합니다. 격리, 기밀성, 무결성도 보장하며 분할을 통해 이러한 네트워크 내의 정보 흐름을 제어합니다.

액세스 제어

NSv는 지정된 조건 세트를 충족시키는 VM만 VLAN을 사용하여 다른 VM의 데이터에 액세스할 수 있는지 검증합니다.

사용자 인증

NSv는 인증되지 않은 사용자가 VM과 워크로드에 액세스하는 것을 제어하거나 제한하는 정책을 만듭니다.

데이터 기밀성

NSv는 정보 도난과 보호된 데이터 및 서비스에 대한 불법적인 액세스를 차단합니다.

가상 네트워크 복원력과 가용성

NSv는 애플리케이션 서비스와 통신을 방해하거나 저해하는 활동을 차단합니다.

시스템 안전과 무결성

NSv는 VM 시스템과 서비스의 무단 점유를 중단시킵니다.

트래픽 검증, 검사, 모니터링 메커니즘

NSv는 변칙적이고 악의적인 활동을 감지하여 VM 워크로드를 대상으로 공격하지 못하도록 막습니다.

[1] SonicWall AGSS(Advanced Gateway Security Services) 구독이 필요합니다.
[2] AWS 마켓플레이스 출시는 보류 중입니다.
[3] SonicWall Global Management System과 Capture Security Center에는 별도의 라이센스나 구독이 필요합니다.

NSv 시리즈 시스템 사양

방화벽 일반	NSv 10	NSv 25	NSv 50	NSv 100
운영 체제	SonicOS			
지원되는 하이퍼바이저	VMware ESXi v5.5 / v6.0 / v6.5			
최대 지원 vCPU	2	2	2	2
인터페이스 수(ESXi)	8	8	8	8
최대 관리/데이터 플레인 코어	1/1	1/1	1/1	1/1
최소 메모리[1]	4GB	4GB	4GB	4GB
최대 메모리[2]	6GB	6GB	6GB	6GB
지원되는 IP/노드	10	25	50	100
최소 스토리지	60GB			
SSO 사용자	25	50	100	100
로깅	분석기, 로컬 로드, Syslog			
고가용성	액티브/패시브			
방화벽/VPN 성능[1]	**NSv 10**	**NSv 25**	**NSv 50**	**NSv 100**
방화벽 검사 처리량	2Gbps	2.5Gbps	3Gbps	3.5Gbps
전체 DPI 처리량(GAV/GAS/IPS)	450Mbps	550Mbps	650Mbps	750Mbps
애플리케이션 검사 처리량	1Gbps	1.25Gbps	1.5Gbps	1.75Gbps
IPS 처리량	1Gbps	1.25Gbps	1.5Gbps	1.75Gbps
안티 맬웨어 검사 처리량	450Mbps	550Mbps	650Mbps	750Mbps
IMIX 처리량	750Mbps	850Mbps	950Mbps	1100Mbps
TLS/SSL DPI 처리량	650Mbps	750Mbps	850Mbps	950Mbps
VPN 처리량	500Mbps	550Mbps	600Mbps	650Mbps
초당 연결	1,800	5,000	8,000	10,000
최대 연결(SPI)	2,500	6,250	12,500	25,000
최대 연결(DPI)	2,500	6,250	12,500	25,000
TLS/SSL DPI 연결	500	1,000	2,000	4,000
VPN	**NSv 10**	**NSv 25**	**NSv 50**	**NSv 100**
사이트 간 VPN 터널	10	10	25	50
IPSec VPN 클라이언트	10	10	25	25
SSL VPN NetExtender 클라이언트(최대)	2(10)	2(25)	2(25)	2(25)
암호화/인증	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B, CAC(일반 액세스 카드)			
키 교환	Diffie Hellman Groups 1, 2, 5, 14v			
경로 기반 VPN	RIP, OSPF, BGP			
네트워킹	**NSv 10**	**NSv 25**	**NSv 50**	**NSv 100**
IP 주소 할당	고정, DHCP, 내부 DHCP 서버, DHCP 릴레이			
NAT 모드	일대일, 다대일, 일대다, 유연한 NAT(중첩 IP), PAT			
VLAN 인터페이스	25	25	50	50
라우팅 프로토콜	BGP, OSPF, RIPv1/v2, 고정 라우팅, 정책 기반 라우팅			
QoS	대역폭 우선, 최대 대역폭, 대역폭 보장, DSCP 마킹, 802.1p			
인증	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, 내부 사용자 데이터베이스, 터미널 서비스, Citrix			
VoIP	전체 H323-v1-5, SIP			
표준	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, L2TP, PPTP, RADIUS			

[1]점보 프레임을 비활성화한 상태의 메모리입니다.
[2]점보 프레임을 활성화한 상태의 메모리입니다. 점보 프레임을 사용하려면 더 많은 메모리가 필요합니다.

NSv 시리즈 시스템 사양 계속됨

방화벽 일반	NSv 200	NSv 300	NSv 400	NSv 800	NSv 1600
운영 체제	SonicOS				
지원되는 하이퍼바이저	VMware ESXi v5.5 / v6.0 / v6.5				
지원되는 공용 클라우드 플랫폼(인스턴스 유형)	AWS(c5.large), Azure(Std D2 v2)	해당 없음	AWS(c5.xlarge), Azure(Std D3 v2)	AWS(c5.2xlarge), Azure(Std D4 v2)	AWS(c5.4xlarge), Azure(Std D5 v2)
최대 지원 vCPU	2	3	4	8	16
인터페이스 수(ESXi/AWS/Azure)	8/3/2	8/-/-	8/4/4	8/4/8	8/8/8
최대 관리/데이터 플레인 코어	1/1	1/2	1/3	1/7	1/15
최소 메모리[1]	4GB	6GB	8GB	10GB	12GB
최대 메모리[2]	6GB	8GB	10GB	14GB	18GB
지원되는 IP/노드	무제한	무제한	무제한	무제한	무제한
최소 스토리지	60GB				
SSO 사용자	500	5,000	10,000	15,000	20,000
로깅	분석기, 로컬 로드, Syslog				
고가용성	액티브/패시브[3]				
방화벽/VPN 성능[4]	**NSv 200**	**NSv 300**	**NSv 400**	**NSv 800**	**NSv 1600**
방화벽 검사 처리량	4.1Gbps	5.9Gbps	7.8Gbps	13.9Gbps	17.2Gbps
전체 DPI 처리량(GAV/GAS/IPS)	900Mbps	1.6Gbps	2.2Gbps	4.0Gbps	6.4Gbps
애플리케이션 검사 처리량	2.3Gbps	3.4Gbps	4.1Gbps	5.5Gbps	6.4Gbps
IPS 처리량	2.3Gbps	3.4Gbps	4.1Gbps	5.5Gbps	6.7Gbps
안티 맬웨어 검사 처리량	900Mbps	1.6Gbps	2.2Gbps	4.0Gbps	6.6Gbps
IMIX 처리량	1.5Gbps	2.3Gbps	2.8Gbps	4.2Gbps	5.3Gbps
TLS/SSL DPI 처리량	1.1Gbps	1.2Gbps	1.8Gbps	3.4Gbps	5.1Gbps
VPN 처리량	750Mbps	1.4Gbps	1.9Gbps	4.2Gbps	8.4Gbps
초당 연결	13,760	24,360	37,270	75,640	125,000
최대 연결(SPI)	225,000	1M	1.5M	3M	4M
최대 연결(DPI)	125,000	500,000	1.5M	2M	2.5M
TLS/SSL DPI 연결	8,000	12,000	20,000	30,000	50,000
VPN	**NSv 200**	**NSv 300**	**NSv 400**	**NSv 800**	**NSv 1600**
사이트 간 VPN 터널	75	100	6000	10,000	25,000
IPSec VPN 클라이언트(최대)	50(1000)	50(1000)	2000(4000)	2000(6000)	2000(10,000)
SSL VPN NetExtender 클라이언트(최대)	2(100)	2(100)	2(100)	2(100)	2(100)
암호화/인증	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B, CAC(일반 액세스 카드)				
키 교환	Diffie Hellman Groups 1, 2, 5, 14v				
경로 기반 VPN	RIP, OSPF, BGP				
네트워킹	**NSv 200**	**NSv 300**	**NSv 400**	**NSv 800**	**NSv 1600**
IP 주소 할당	고정, DHCP, 내부 DHCP 서버, DHCP 릴레이				
NAT 모드	일대일, 다대일, 일대다, 유연한 NAT(중첩 IP), PAT				
VLAN 인터페이스	50	256	500	512	512
라우팅 프로토콜	BGP, OSPF, RIPv1/v2, 고정 라우팅, 정책 기반 라우팅				
QoS	대역폭 우선, 최대 대역폭, 대역폭 보장, DSCP 마킹, 802.1p				
인증	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, 내부 사용자 데이터베이스, 터미널 서비스, Citrix				
VoIP	전체 H323-v1-5, SIP				
표준	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, L2TP, PPTP, RADIUS				

[1]점보 프레임을 비활성화한 상태의 메모리입니다.
[2]점보 프레임을 활성화한 상태의 메모리입니다. 점보 프레임을 사용하려면 더 많은 메모리가 필요합니다.
[3]VMware ESXi 플랫폼에서 고가용성을 발휘할 수 있습니다.
[4]게시된 성능 수치는 최고 사양이며 실제 성능은 기반 하드웨어, 네트워크 상태, 방화벽 상태와 활성화된 서비스에 따라 달라질 수 있습니다. 성능과 기능은 기반의 가상화 인프라에 따라서도 달라질 수 있으며, 실제 사용 환경에서 추가로 테스트하여 성능과 용량 요구 사항에 맞는지 확인할 것을 권합니다. 성능 측정에 사용된 환경에는 Intel Xeon W 프로세서(W-2195 2.3GHz, 4.3GHz Turbo, 24.75M 캐시)와 SonicOSv 6.5.0.2, VMware vSphere 6.5입니다.
테스팅 방법론:
최대 성능은 RFC 2544(방화벽용)를 기반으로 합니다.
전체 DPI/게이트웨이 AV/안티 스파이웨어/IPS 처리량은 업계 표준 Spirent WebAvalanche HTTP 성능 테스트와 Ixia 테스트 도구를 사용하여 측정되었습니다.
테스팅은 여러 포트 짝을 통한 여러 흐름으로 수행되었습니다.
VPN 처리량은 RFC 2544에 따라 1418바이트의 패킷 크기로 UDP 트래픽을 측정하였습니다. 모든 사양과 기능은 변경될 수 있습니다.

SONICWALL®

NSv 시리즈 주문 정보

제품	AWS SKU[1]	Azure SKU	ESXi SKU
SonicWall NSv 10 Virtual Appliance TotalSecure Advanced Edition(1년)	–	–	01-SSC-5875
SonicWall NSv 25 Virtual Appliance TotalSecure Advanced Edition(1년)	–	–	01-SSC-5923
SonicWall NSv 50 Virtual Appliance TotalSecure Advanced Edition(1년)	–	–	01-SSC-5926
SonicWall NSv 100 Virtual Appliance TotalSecure Advanced Edition(1년)	–	–	01-SSC-5929
SonicWall NSv 200 Virtual Appliance TotalSecure Advanced Edition(1년)	02-SSC-0906	02-SSC-0868	01-SSC-5950
SonicWall NSv 300 Virtual Appliance TotalSecure Advanced Edition(1년)	–	–	01-SSC-5964
SonicWall NSv 400 Virtual Appliance TotalSecure Advanced Edition(1년)	02-SSC-0912	02-SSC-0888	01-SSC-6084
SonicWall NSv 800 Virtual Appliance TotalSecure Advanced Edition(1년)	02-SSC-0914	02-SSC-0889	01-SSC-6101
SonicWall NSv 1600 Virtual Appliance TotalSecure Advanced Edition(1년)	02-SSC-0921	02-SSC-0895	01-SSC-6109
제품	AWS SKU[1]	Azure SKU	ESXi SKU
SonicWall NSv 10 Virtual Appliance TotalSecure Advanced Edition(3년)	–	–	01-SSC-5008
SonicWall NSv 25 Virtual Appliance TotalSecure Advanced Edition(3년)	–	–	01-SSC-4830
SonicWall NSv 50 Virtual Appliance TotalSecure Advanced Edition(3년)	–	–	01-SSC-5165
SonicWall NSv 100 Virtual Appliance TotalSecure Advanced Edition(3년)	–	–	01-SSC-5161
SonicWall NSv 200 Virtual Appliance TotalSecure Advanced Edition(3년)	02-SSC-0903	02-SSC-0866	01-SSC-5194
SonicWall NSv 300 Virtual Appliance TotalSecure Advanced Edition(3년)	–	–	01-SSC-5189
SonicWall NSv 400 Virtual Appliance TotalSecure Advanced Edition(3년)	02-SSC-0911	02-SSC-0887	01-SSC-5219
SonicWall NSv 800 Virtual Appliance TotalSecure Advanced Edition(3년)	02-SSC-0913	02-SSC-0891	01-SSC-5216
SonicWall NSv 1600 Virtual Appliance TotalSecure Advanced Edition(3년)	02-SSC-0920	02-SSC-0897	01-SSC-5306
제품	AWS SKU[1]	Azure SKU	ESXi SKU
SonicWall NSv 10 Virtual Appliance TotalSecure Advanced Edition(5년)	–	–	01-SSC-5584
SonicWall NSv 25 Virtual Appliance TotalSecure Advanced Edition(5년)	–	–	01-SSC-5587
SonicWall NSv 50 Virtual Appliance TotalSecure Advanced Edition(5년)	–	–	01-SSC-5649
SonicWall NSv 100 Virtual Appliance TotalSecure Advanced Edition(5년)	–	–	01-SSC-5671
SonicWall NSv 200 Virtual Appliance TotalSecure Advanced Edition(5년)	02-SSC-0901	02-SSC-0864	01-SSC-5581
SonicWall NSv 300 Virtual Appliance TotalSecure Advanced Edition(5년)	–	–	01-SSC-5681
SonicWall NSv 400 Virtual Appliance TotalSecure Advanced Edition(5년)	02-SSC-0910	02-SSC-0886	01-SSC-5684
SonicWall NSv 800 Virtual Appliance TotalSecure Advanced Edition(5년)	02-SSC-0918	02-SSC-0890	01-SSC-5690
SonicWall NSv 1600 Virtual Appliance TotalSecure Advanced Edition(5년)	02-SSC-0919	02-SSC-0896	01-SSC-5693

[1]AWS 마켓플레이스 출시는 보류 중입니다.

회사 소개

SonicWall은 전 세계 중소기업과 대기업을 보호하면서 27년 넘게 사이버 범죄와 싸우고 있습니다. 우리의 제품과 파트너 제품의 조합으로 215개 이상의 국가와 지역에 있는 50만 개 이상의 기업이 각자의 요구 사항에 맞는 조정된 자동화된 실시간 위반 탐지와 방지 솔루션을 마련하여 안심하고 더 많은 업무를 하고 있습니다. 자세한 내용을 보려면 www.sonicwall.com을 방문하거나 트위터, 링크드인, 페이스북, 인스타그램을 팔로우하세요.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
추가 정보는 웹 사이트를 참조하세요.
www.sonicwall.com

Datasheet-NSvVirtualFirewalls-US-VG-MKTG4149