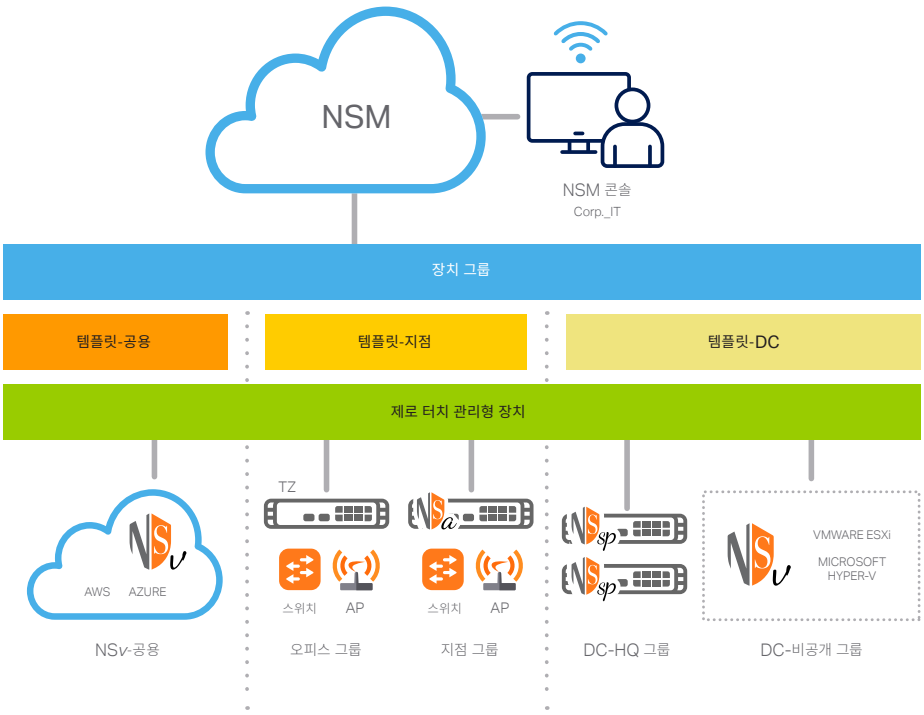
SONICWALL

네트워크 시큐리티 매니저

모든 환경에 확장 가능한 통합 방화벽 관리 시스템

소규모 기업, 분산 엔터프라이즈 또는 여러 기업을 보호하려할 때, 네트워크 보안은 운영 혼란, 숨겨진 위험 및 규제 요건으로 인해 매우 까다로울 수 있습니다. 역사적으로 우수한 방화벽 관리 방식에서는 대부분 견고하고 내구성이 있는 시스템과 운영 통제 조치가 활용되어 왔습니다. 그러나 일반적인 오류, 잘못된 구성 및 이러한 통제 위반은 올바르게 운영되는 보안 운영 센터(SOC)에 지속적인 과제가 되고 있습니다.

멀티 테넌트 중앙집중식 방화벽 관리자인 SonicWall Network Security Manager(NSM)를 활용하여 감사가 가능한 워크플로를 유지하여, 오류 없이 모든 방화벽 운영을 중앙에서 관리할 수 있습니다. 그리고 기본 분석 엔진은 단일 창 가시성을 제공하며 모든 방화벽 전반에서 통합 및 상관 관계 로그를 통해 위협을 모니터링하고 발견하는 기능을 제공합니다. NSM은 또한 모든 구성 변경의 완벽한 감사 추적 및 세밀한 보고 기능으로 규정 준수를 지원합니다. NSM은 여러 위치에 배치된 수천 개의 방화벽 장치까지 규모와 상관없이 모든 조직 관리 네트워크로 신속하고 편리하게 확장할 수 있습니다.



장점:

비즈니스

- 보안 관리 오버헤드 감소
- 위협 환경 및 보안 상태에 대한 지식
- SaaS를 통한 CAPEX 감소

운영

- HW/SW를 구축할 필요 없음
- 방화벽 관리 사일로 제거
- 대수에 관계 없이 손쉽게 방화벽을 온보드
- 모든 보안 운영에 대한 가시성

보안

- 모든 환경 전반에서 일관적인 보안 정책 감사, 할당 및 적용
- 문제 및 위험을 추적하고 이에 대응
- 정보에 기반한 보안 의사결정

통제 유지: 한 곳에서 방화벽 운영 조정

NSM은 통합 방화벽 관리 시스템에서 필요한 모든 기능을 제공하며, 테넌트 수준의 가시성, 그룹 기반 장치 제어 및 무제한 확장 기능으로 SonicWall 네트워크 보안 운영을 중앙에서 관리 및 제공할 수 있도록 해줍니다. 여기에는 모든 방화벽 장치, 장치 그룹 및 테넌트를 구축하고 관리하는 기능, 유연한 로컬 제어를 활용하여 환경 전반에서 일관적인 보안 정책을 동기화하고 적용하는 기능, 세부 보고서 및 분석이 제공되는 단일의 동적 대시보드에서 모든 사항을 모니터링하는 기능이 포함됩니다. 그리고 브라우저 지원 장치를 사용하여 어디서나 액세스할 수 있는 사용자 친화적인 단일 네이티브 콘솔에서 이러한 모든 작업을 수행할 수 있습니다.

멀티 테넌트 관리

각 네트워크 세그먼트별로 다양한 보안 요건이 있는 복잡한 멀티 클라우드 및 다중 위치 테넌트로 방화벽 환경이 성장함에 따라 그러한 환경에 따라 확장이 가능한 방화벽 관리 시스템이 필요합니다. NSM은 모든 관리형 테넌트 전반에서 완벽한 멀티 테넌트 관리 및 독립 정책 제어 분리를 제공합니다. 이러한 분리는 각 테넌트에 대한 방화벽을 운영하는 NSM의 모든 관리 기능에 적용됩니다. 사용자는 할당된 테넌트 계정의 경계 내에서 장치 그룹 관리, 정책 조율 및 기타 모든 관리 작업을 수행하기 위해 모든 테넌트가 고유한 사용자 집합, 그룹 및 역할을 갖도록 구성할 수 있습니다.

장치 그룹 관리

장치 그룹은 방화벽 장치를 그룹 또는 계층 구조 그룹으로 생성하고 관리하며 방화벽 그룹에 구성 템플릿을 할당하고 구축하기 위한 효과적인 방법을 제공합니다. 이를 통해 사용자는 일관적이고 신뢰할 수 있는 방식으로 선택한 방화벽 그룹 전반에서 공통 정책, 객체 및 설정 요구 사항을 동기화하고 이를 적용할 수 있습니다. 템플릿의 승인된 모든 정책 변경 사항은 해당 템플릿에 연결된 모든 장치 그룹에 자동으로 적용됩니다. 장치 그룹은 편리한 관리, 식별 및 연결을 위해 네트워크 유형, 위치, 사업부, 조직 구조 또는 관련 속성의 조합 등과 같은 특성에 따라 세밀하게 정의할 수 있습니다.

템플릿 관리, 할당 및 구축

NSM의 간소화된 워크플로를 통해 사용자는 쉽고 빠르게 구성 템플릿을 설계, 검증, 감사 및 할당하여 하나 또는 수천 개의 방화벽 장치를 여러 지리적 위치 전반에서 관리할 수 있습니다. 다양한 방화벽 정책, 설정 및 관련 객체가 적용된 템플릿은 장치와 독립적으로 정의되며 NSM에서 사용되어 유사한 구성이 필요한 장치 또는 장치 그룹으로 중앙에서 자동으로 푸시됩니다.

효율성 향상: 보다 효율적으로 신속하게 보안 조치를 취하고 스마트하게 작업 수행

NSM은 스마트하게 작업을 수행하고 보다 효율적으로 신속하게 보안 조치를 취할 수 있도록 해주는 생산성 관리 도구입니다. 그리고 비즈니스 프로세스를 기반으로 설계되며 일상적인 보안 작업 및 관리 작업을 수행하는 데 따른 복잡성, 시간 및 오버헤드를 줄이면서 보안 조정을 향상하기 위해 워크플로를 단순화하고 일부 경우에는 자동화 원칙을 기반으로 합니다.

편리한 제로 터치 구축

NSM으로의 통합은 제로 터치 구축 방식으로 수행되며, 이를 통해 사용자는 SonicWall 방화벽, 스위치 및 액세스 포인트를 원격 및 지점 사무실에서 편리하게 구축 및 운영할 수 있습니다. 전체 프로세스에서는 최소한의 사용자 개입만이 필요하며 완전 자동화됩니다. 제로 터치 지원 장치는 설치 현장으로 직접 배송됩니다. 포장을 풀어 등록한 후 네트워크에 연결하고 전원을 켜면 보안 및 연결이 원활하게 수행되며 연결된 모든 장치가 즉시 작동합니다. NSM과 함께 사전 구축된 장치 템플릿에 통신 링크가 연결되면 사전 공급 장치 템플릿은 모든 제로 터치 지원 장치로 자동으로 푸시됩니다. 이를 통해 기존 현장 투입 프로세스의 시간, 비용 및 복잡성이 제거됩니다.

오류가 없는 변경 관리

NSM은 방화벽 정책 변경 관리 및 SOC의 감사 요구 사항을 준수하는 자동화된 강력한 워크플로에 대한 즉각적인 액세스를 제공합니다. 이를 통해 구축하기 전에 방화벽 정책을 구성, 비교, 검증, 검토, 승인을 하기 위한 일련의 엄격한 절차를 적용하여 오류가 없는 정책 변경이 보장됩니다. 승인 그룹은 유연하여 다양한 유형의 조직에서 요구되는 다양한 인증 및 감사 절차를 준수할 수 있습니다. NSM은 완벽하게 검증 및 감사가 수행된 보안 정책을 프로그래밍 방식으로 구축하여 운영 효율성을 향상하고 위험을 완화하며 잘못된 구성 및 사람에 의한 오류를 제거합니다.

RESTful API를 통한 관리 자동화

NSM RESTful API는 숙련된 보안 운영자가 관리 웹 인터페이스를 사용하지 않고 프로그래밍 방식으로 NSM의 특정 기능을 관리할 수 있는 표준 방식을 제공합니다. 이를 통해 NSM과 타사 관리 콘솔 사이의 호환성이 간소화되어 내부 보안 팀의 효율성이 향상될 수 있습니다. 그리고 API 서비스를 사용하여 관리형 장치에 대한 방화벽 운영을 자동화할 수 있습니다. 여기에는 테넌트, 장치 그룹 및 테넌트 관리, 감사 구성, 시스템 상태 확인 수행 등과 같은 일반적인 일일 작업이 포함됩니다.

인식 능력 향상: 활성 모니터링, 보고 및 분석 기능으로 숨겨진 위험 조사

NSM 대화형 대시보드에는 실시간 모니터링, 보고 및 분석 데이터가 로드되어 문제 해결, 위험 조사 및 강력한 적응형 보안 태세를 위한 스마트 보안 정책 결정과 정책 조치가 지원됩니다.

어디서나 모든 사항 확인

NSM 보고, 분석 및 위험 모니터링 대시보드는 테넌트, 그룹 또는 장치 수준별로 전체 SonicWall 보안 생태계에 대한 최대 7일 동안의 연속적이고 완전한 가시성을 제공합니다. 그리고 방화벽 생태계를 통과하는 모든 네트워크 트래픽 및 데이터 통신에 대한 통계 및 준실시간 분석도 제공됩니다. 모든 로드 데이터는 유의미하고 실행 가능하며 쉽게 사용할 수 있는 방식으로 자동으로 기록, 집계, 문맥화 및 제공되어 사용자는 데이터 중심의 통찰력과 상황 인식에 기반하여 적절한 방어 및 교정 조치를 발견, 해석, 우선 순위 지정 및 이행할 수 있습니다. 예약 보고서를 사용하면 감사가 가능한 데이터 조합으로 보고서를 완전하게 사용자 지정할 수 있습니다. 그리고 기록 분석, 이상 감지, 보안 격차 검색 등을 위해 장치 수준에서 최대 365일 동안의 기록된 로그도 제공됩니다. 이를 통해 효율적인 네트워크 및 보안 운영을 추적, 측정 및 실시할 수 있습니다.

위험 파악

드릴 다운 및 피벗 기능을 사용하면 데이터를 추가적으로 조사 및 연결하여 보다 정확하고 신뢰성 있게 숨겨진 위협 및 문제를 조사하고 발견할 수 있습니다. 이력 보고, 사용자 기반 및 애플리케이션 기반 분석과 엔드포인트 가시성을 혼합하여 사용하면 유입/유출 트래픽, 애플리케이션 사용, 사용자 및 장치 액세스, 위협 동작 등과 관련된 다양한 패턴과 경향을 철저하게 분석할 수 있습니다. 그리고 상황을 파악하고 귀중한 통찰력과 지식을 얻을 수 있어 보안 위험을 발견할 뿐만 아니라 수정 사항을 조정하는 동시에 결과를 모니터링 및 추적하여 환경 전반에서 일관적인 보안 시행을 촉진하고 주도할 수 있습니다.

기능 요약

관리

- 테넌트 및 장치 그룹 수준 관리
- 구성 템플릿
- 장치 그룹화
- 할당 및 구축 마법사
- 구성 감사
- 구성 – 차이비교
- 오프라인 관리 및 일정 수립
- 보안 방화벽 정책 관리
- 보안 VPN 정책 관리
- SD-WAN 관리
- 부가 가치 보안 서비스 관리
- 백업 및 높은 가용성
- 방화벽 어플라이언스를 위한 환경 설정 파일 백업
- RESTful API
- 펌웨어 업그레이드
- 역할 기반 관리
- 액세스 포인트 및 스위치 관리

모니터링

- 장치 상태
- 라이선스 및 지원 상태
- 네트워크/위협 요약
- 경고 및 알림 센터
- 이벤트 로그
- 형상 보기

분석

- 사용자 기반 활동
- 애플리케이션 사용
- Capture Client를 통한 제품 전반에서의 가시성
- 실시간 역동적 가시화
- 드릴 다운 및 피벗 기능

보고

- 예약 PDF 보고서 – 테넌트/그룹/장치 수준
- 사용자 지정 가능 보고서
- 중앙집중식 로깅
- 멀티 테넌트 보고서
- 사용자 중심의 보고서
- 애플리케이션 사용 보고서
- 대역폭 및 서비스 보고서
- 사용자별 대역폭 보고

라이선싱 및 패키징

기능	필수	고급
테넌트당 수백 개의 장치 관리	예	예
멀티 테넌트 관리	예	예
장치 인벤토리	예	예
그룹 수준에서 정책 푸시	예	예
장치 그룹	예	예
템플릿	예	예
할당 및 구축	예	예
구성 감사	예	예
구성 차이	예	예
워크플로 자동화	예	예
API	예	예
제로 터치 구축(Zero-Touch Deployment)	예	예
작업 예약	예	예

기능	필수	고급
백업/복원	예	예
펌웨어 업그레이드	예	예
액세스 포인트 및 스위치 관리	예	예
데이터 보고 기간(일)	7일	365일
그룹/테넌트 수준 대시보드	예	예
ATP 캡처(장치 레벨)	예	예
위협 평가 캡처(장치 레벨)	예	예
그룹 수준 가시성 및 보고	예	예
예약 리포트(장치 그룹 레벨)	예	예
사용자 기반 분석	아니요	예
애플리케이션 분석	아니요	예
위협 분석	아니요	예
드릴 다운 및 피벗	아니요	예

제품	SKU
NSM ESSENTIAL FOR SOHO 250 1년	02-SSC-5219
NSM ADVANCED FOR SOHO 250 1년	02-SSC-5213
NSM ESSENTIAL FOR TZ 350 1년	02-SSC-5239
NSM ADVANCED FOR TZ 350 1년	02-SSC-5231
NSM ESSENTIAL FOR TZ 400 1년	02-SSC-5263
NSM ADVANCED FOR TZ 400 1년	02-SSC-5257
NSM ESSENTIAL FOR TZ 500 1년	02-SSC-5183
NSM ADVANCED FOR TZ 500 1년	02-SSC-5177
NSM ESSENTIAL FOR TZ 570 1년	02-SSC-4975
NSM ADVANCED FOR TZ 570 1년	02-SSC-4963
NSM ESSENTIAL FOR TZ 600 1년	02-SSC-5201
NSM ADVANCED FOR TZ 600 1년	02-SSC-5195
NSM ESSENTIAL FOR TZ 670 1년	02-SSC-5011
NSM ADVANCED FOR TZ 670 1년	02-SSC-4999
NSM ESSENTIAL FOR NS*a* 2600/NS*a* 2650 1년	02-SSC-5281
NSM ADVANCED FOR NS*a* 2600/NS*a* 2650 1년	02-SSC-5275
NSM ESSENTIAL FOR NS*a* 3600/NS*a* 3650 1년	02-SSC-5299
NSM ADVANCED FOR NS*a* 3600/NS*a* 3650 1년	02-SSC-5293
NSM ESSENTIAL FOR NS*a* 4600/NS*a* 4650 1년	02-SSC-5325
NSM ADVANCED FOR NS*a* 4600/NS*a* 4650 1년	02-SSC-5319
NSM ESSENTIAL FOR NS*a* 5600/NS*a* 5650 1년	02-SSC-5347
NSM ADVANCED FOR NS*a* 5600/NS*a* 5650 1년	02-SSC-5341
NSM ESSENTIAL FOR NS*a* 6600/NS*a* 6650 1년	02-SSC-5365
NSM ADVANCED FOR NS*a* 6600/NS*a* 6650 1년	02-SSC-5359

다년간의 SKU 및 지원 계약도 제공됩니다. 전체 목록은 원하는 리셀러 또는 SonicWall 영업부로 문의해 주십시오.

인터넷 브라우저

- Microsoft® Internet Explorer 11.0 이상 및 Microsoft Edge, Mozilla Firefox, Google Chrome 및 Safari 최신 버전.

NSM 관리형 장치[1]

- SonicWall 네트워크 보안 어플라이언스: SuperMassive 9000 Series[2], E-Class NSA, NS*sp* 12000 Series[2], NS*a* Series, TZ Series, SOHO-W, SOHO 250, SOHO 250W
- SonicWall Network Security Virtual Appliances: NS*v* Series
- SonicWall SonicWave, SonicPoint
- SonicWall Switch

[1] SonicOS 버전 6.x 또는 7.x로 구동되는 방화벽 지원.
[2] 365일의 보고 및 30일의 분석은 지원되지 않음.

SonicWall 소개

SonicWall은 초분산 시대를 위해 그리고 모든 사람이 원격, 모바일 및 비보안 상태인 업무 현실을 위해 Boundless Cybersecurity를 제공합니다. SonicWall은 알려지지 않은 정보를 파악하고 실시간 가시성을 제공하며 혁신적인 경제성을 제공함으로써 전 세계 기업, 정부 및 중소기업의 사이버 보안 비즈니스 격차를 해소합니다. 자세한 정보는 www.sonicwall.com에서 확인할 수 있습니다.

SonicWall Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
저희 웹사이트에서 더 많은 정보를 보실 수 있습니다.
www.sonicwall.com

Datasheet-NSM-US-COG-2114