SonicWall TZ series (Gen 7)

중소기업 및 지점 사무소를 위한 차세대 보안 기능과 SD- WAN 플랫폼

최신 SonicWall TZ 시리즈는 10기가 또는 5 기가비트 이더넷 인터페이스를 갖춘 최초의 데스크톱 폼 팩터 차세대 방화벽 (NGFW)입니다.

이 시리즈는 다양한 구성 사례에 적합한 다양한 제품으로 구성되어 있습니다.
SD-Branch에 위치한 중소 규모 기업 및 분산 기업을 위해 설계된 7 세대 (Gen 7) TZ 시리즈는 동급 최고의 가격 대비 성능과 업계에서 검증 된 보안 효율성을 제공합니다.
이러한 NGFW는 자동화 된 실시간 침해 탐지와 방지에 대한 요구를 충족하는 솔루션을 제공함으로써 웹 암호화, 연결된 장치 및 고속 모빌리티의 증가 추세에 대응하도록 합니다.

Gen 7 TZ 시리즈는 최대 10개 포트의 높은 포트 집적도를 통해 뛰어난 확장성을 제공합니다. 또한 최대 256GB까지 확장 가능한 스토리지를 모두 갖추고 있어 로깅, 보고서, 캐싱, 펌웨어 백업 등을 비롯한 다양한 기능을 지원합니다.
선택 사양인 보조 전원 공급 장치는 방화벽에서 문제가 발생할 경우 추가적인 이중화를 제공합니다.

Zero-Touch 배포를 사용하면 최소한의 IT 지원으로 여러 위치에 걸쳐 이러한 장치를 여러 위치에서 동시에 원격 설치 할 수 있어 Gen 7 TZ의 구축은 더욱 간소화됩니다.

차세대 하드웨어를 기반으로 하여 방화벽, 스위칭 및 무선 기능을 통합하고 SonicWall 스위치 및 SonicWave 액세스 포인트에 대한 단일 창 관리를 제공합니다.

또한 완벽한 엔드 포인트 보안을 위해 Capture Client와 긴밀하게 통합됩니다

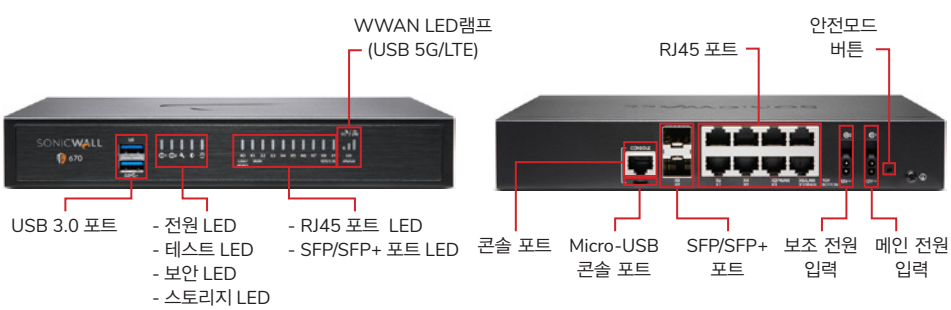
SonicOS 및 보안 서비스

SonicOS 아키텍처는 TZ NGFW의 핵심입니다. Gen 7 TZ는 새롭고 현대적인 UX / UI, 고급 보안, 네트워킹 및 관리 기능을 갖춘 풍부한 기능의 SonicOS 7.0 운영 체제를 기반으로 합니다. Gen 7 TZ는 통합 SD-WAN, TLS 1.3 지원, 실시간 시각화, 고속 VPN (가상 사설망) 및 기타 강력한 보안 기능을 제공합니다.

알 수 없는 위협은 분석을 위해 SonicWall의 클라우드 기반 ATP (Capture Advanced Threat Protection) 다중 엔진 샌드 박스로 전송됩니다. 향상된 Capture ATP는 특허 출원 중인 RTDMI™ (Real-Time Deep Memory Inspection) 기술을 포함합니다. Capture ATP의 엔진 중 하나 인 RTDMI는 메모리를 직접 검사하여 멀웨어 및 제로 데이 위협을 감지하고 차단합니다.

Gen7 TZ 시리즈 방화벽은 RTDMI 기술이 적용된 Capture ATP를 활용하고 RFDPI (Reassembly-Free Deep Packet Inspection), 안티 바이러스 및 안티 스파이웨어 보호, 침입 방지 시스템, 애플리케이션 인텔리전스 및 제어, 콘텐츠 필터링 서비스, DPI-SSL과 같은 보안 서비스를 활용하여 게이트웨이에서 멀웨어, 랜섬웨어 및 기타 지능형 위협을 차단합니다.

자세한 내용은 SonicOS 및 보안 서비스 데이터 시트를 참조하십시오.



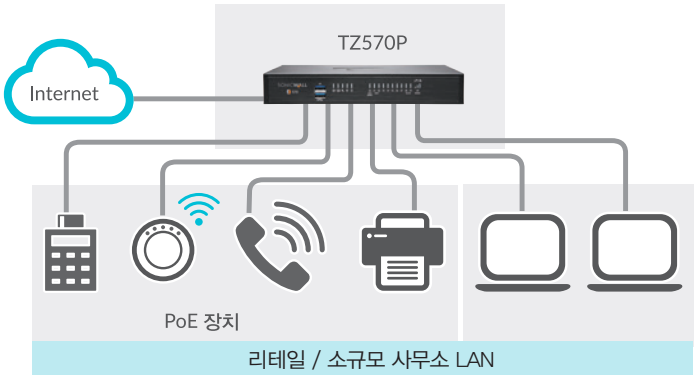
SonicWall TZ670 전, 후면

하이라이트:

- 데스크탑 폼 팩터에서 10/ 5/ 2.5/ 1GbE 인터페이스 제공
- SD-Branch 지원
- Secure SD-WAN 기능
- SonicExpress 모바일 앱을 통한 설정
- 제로 터치 배포
- 클라우드 또는 방화벽을 통한 단일 창 관리
- SonicWall 스위치, SonicWave 액세스 포인트 및 캡처 클라이언트 통합
- 내장 및 확장 가능한 스토리지
- 전원 이중화
- 높은 포트 집적도
- 셀룰러 모뎀을 통한 Failover
- SonicOS 7.0
- TLS 1.3 지원
- 획기적인 성능
- 높은 동시 세션 수
- 빠른 DPI 성능
- 낮은 TCO

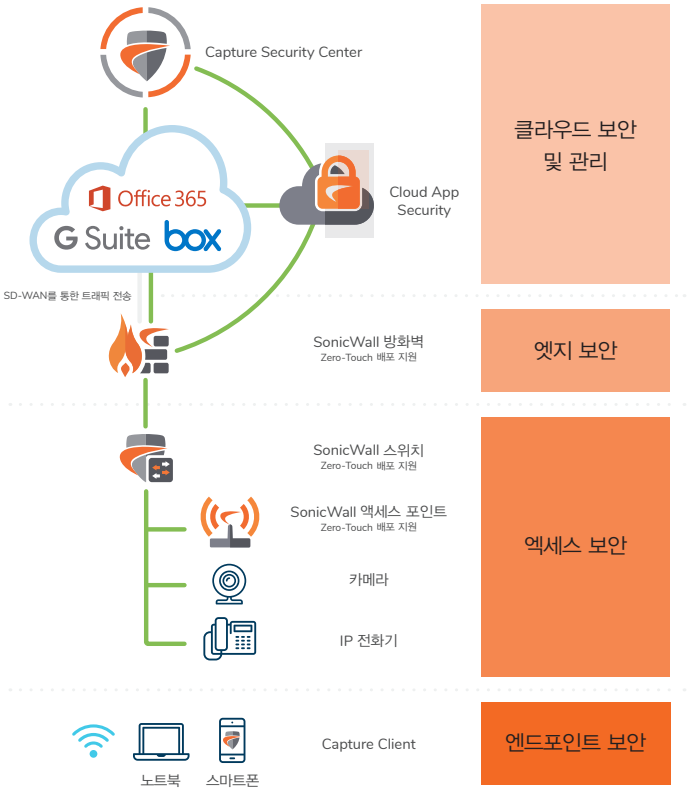
TZ 구성 방안 – 중소규모 비즈니스

- 방화벽, 스위칭 및 무선 기능을 갖춘 통합 게이트웨이 보안 솔루션으로 공간과 비용 절감
- SonicExpress 앱 및 제로 터치 배포를 사용하여 간편하게 설치하고 단일 창을 통해 간편히 관리하여 복잡성을 줄이고 비즈니스를 운영 할 수 있습니다.
- 셀룰러 연결에 대한 장애 조치를 제공하여 비즈니스 연속성 확보
- VPN, IPS, CFS, AV 등을 통합하는 포괄적인 보안 솔루션을 통해 공격으로부터 네트워크를 보호
- TZ570P의 높은 포트 집적도를 활용하여 IP 전화, IP 카메라와 같은 여러 PoE 장치에 전원 공급
- 트래픽 세분화 및 액세스 정책으로 무단 액세스를 차단하여 직원 생산성 향상



TZ 구성 방안 – 분산 기업 및 SD-Branch

- SD-Branch와의 차세대 지점 연결을 활성화하여 고객 경험을 향상시키고 변화하는 비즈니스 요구에 적응
- 변화하는 네트워크 및 보안 환경에 대비하여 멀티 기가비트 및 고급 보안 기능을 갖춘 차세대 제품에 투자하여 비즈니스 성장을 촉진
- 고급 보안 기능으로 최신 공격으로부터 네트워크를 보호하고 TLS 1.3과 같은 프로토콜을 사용하여 해독 된 트래픽에 대한 위협을 자동으로 차단
- SonicWave 액세스 포인트, SonicWall 스위치 및 캡처 클라이언트의 완벽한 통합을 통해 End-to-End 간 네트워크 보안 활용
- IT 관리자는 Hub & Spoke를 구성할 수 있는 간편한 VPN 연결을 통해 매장과 본사 간에 원활한 커뮤니케이션을 보장하고 모든 위치 간에 안전하게 데이터를 전송
- Gen 7 TZ의 하드웨어 및 소프트웨어 향상과 SD-WAN 기술과 같은 기능을 활용하여 비즈니스 효율성, 성능 개선 및 비용 절감
- SonicExpress 앱 및 제로 터치 배포로 빠르고 쉽게 확장
- 셀룰러 연결을 통해서 장애 조치를 제공하여 비즈니스 연속성을 보장
- 보안 기능에 대한 규정 준수를 유지하고 내장 및 확장 가능한 스토리지를 활용하여 감사 목적으로 로그를 저장



제품 세부 사양

Hardware overview	TZ270	TZ370	TZ470	TZ570	TZ670
Firewall General					
Operating System	SonicOS 7.0				
Interfaces	8x1GbE, 2 USB 3.0, 1 Console	8x1GbE, 2 USB 3.0, 1 Console	8x1GbE, 2x2.5GbE, 2 USB 3.0, 1 Console	8x1GbE, 2x5GbE, 2 USB 3.0, 1 Console	8x1GbE, 2x10GbE, 2 USB 3.0, 1 Console
Storage expansion slot	Optional up to 256GB				Optional up to 256GB, 32GB included
Access points supported (maximum)	16	16	32	32	32
Firewall/VPN performance					
Firewall inspection throughput	2.0 Gbps	3.0 Gbps	3.5 Gbps	4.0 Gbps	5.0 Gbps
Threat Prevention throughput	750 Mbps	1.0 Gbps	1.5 Gbps	2.0 Gbps	2.5 Gbps
Application inspection throughput	1.0 Gbps	1.5 Gbps	2.0 Gbps	2.5 Gbps	3.0 Gbps
IPS throughput	1.0 Gbps	1.5 Gbps	2.0 Gbps	2.5 Gbps	3.0 Gbps
TLS/SSL inspection and decryption throughput (DPI SSL)	300 Mbps	500 Mbps	600 Mbps	750 Mbps	800 Mbps
IPSec VPN throughput[3]	750 Mbps	1.3 Gbps	1.5 Gbps	1.8 Gbps	2.1 Gbps
Connections per second	6,000	9,000	12,000	16,000	25,000
Maximum connections (SPI)	750,000	900,000	1,000,000	1,250,000	1,500,000
Maximum connections (DPI)	150,000	200,000	250,000	400,000	500,000
Site-to-site VPN tunnels	50	100	150	200	250
IPSec VPN clients (maximum)	5 (200)	5 (200)	5 (200)	10 (500)	10 (500)
SSL VPN licenses (maximum)	1 (50)	2 (100)	2 (150)	2 (200)	2 (250)

SONICWALL®

SonicWall Switch 시리즈

SD-Branch 구성을 위한 고성능 스위치 시리즈

SonicWall 스위치는 탁월한 성능과 관리 편이성을 제공하면서 고속의 네트워크 스위칭 성능을 제공합니다. 통합 보안 태세, 높은 포트 밀도, PoE (Power over Ethernet) 옵션 및 멀티 기가비트 성능은 중소기업 (SMB) 및 소프트웨어 정의 브랜치 (SD-Branch) 구성에 매우 이상적입니다. 이를 통해 네트워크 규모에 관계없이 기업이 디지털 전환을 수행하고 변화하는 네트워크 및 보안 환경에 대응해 나갈 수 있습니다.

SonicWall Secure SD-Branch 솔루션은 몇 분 만에 지점 사무실을 구성하고 단일 창에서 통합된 가시성과 위협 탐지를 제공하는 통합 플랫폼을 제공하여 지점에서 사용자 경험을 혁신합니다. SonicWall SDBranch 구성 요소는 Secure SD-WAN이 포함 된 SonicWall 차세대 방화벽, Zero-Touch 배포가 포함 된 Capture Security Center, SonicWall 스위치, SonicWave 액세스 포인트 (AP), Capture Client 및 Cloud App Security로 구성됩니다.

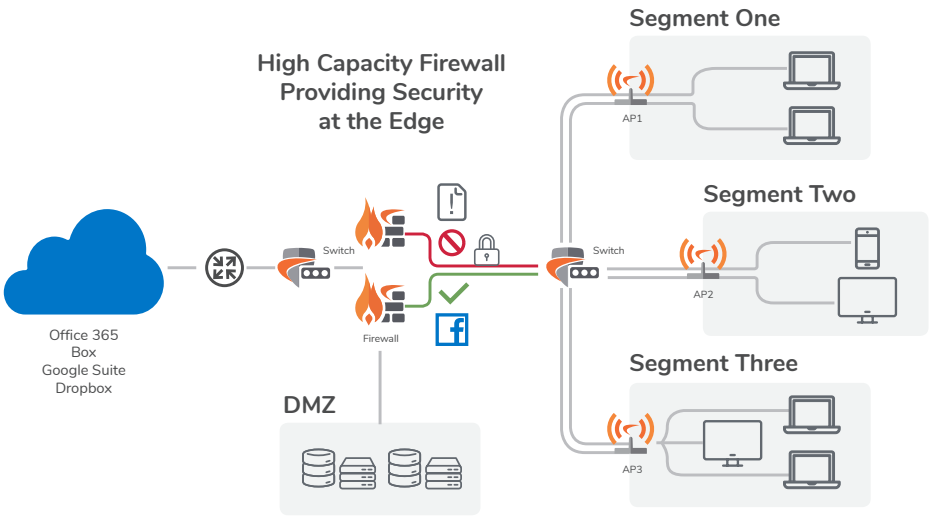
SonicWall Secure SD-Branch가 제공하는 유연성을 통해 조직은 이제 더 민첩하고 개방적이며 클라우드 중심이 될 수 있습니다. 차세대 브랜치 전환의 필수 요소 인 SonicWall 스위치는 방화벽을 통해 관리되며 전체 SonicWall 인프라는 단일 창에서 통합 관리됩니다. 방화벽과 긴밀하게 통합함으로써 이 솔루션은 통합 보안 태세의 이점을 누리고 배포, 관리 및 문제 해결을 단순화하는 장점을 제공합니다.

이는 원활한 보안을 보장하고 타사 스위치에서 발생할 수 있는 보안 태세의 공백을 제거합니다.

이와 함께 SonicWall 스위치는 전 세계에 퍼져 있는 지사에 장치를 빠르게 롤아웃 할 수 있는 기능과 함께 제로 터치 배포 기능을 제공합니다. 관리자는 비용이 많이 드는 현장 IT 인력 없이도 새 위치에 이러한 스위치를 빠르고 안전하게 배포 할 수 있습니다.

다양한 기능이 포함 된 이 스택 형 스위치는 에너지 효율적인 설계의 소형 폼 팩터로 제공됩니다. 기가비트 및 10 기가비트 이더넷 포트가 8 개에서 48 개까지 포함 되는 7개의 모델로 제공되며, 이 스위치는 SonicWall 차세대 방화벽 및 SonicWave AP와 원활하게 작동하여 종단 간 다중 기가비트 보안 네트워크를 생성합니다. 이더넷 포트는 AP, VOIP 전화 및 IP 카메라와 같은 다양한 장치에 전원을 공급할 수 있는 PoE 옵션을 제공합니다.

QoS와 같은 기능을 사용하여 집에서 작업하는 동안 화상 회의를 위한 VOIP와 같은 네트워크의 특정 트래픽에 우선 순위를 부여합니다. 네트워크에서 장치를 쉽게 분할하고 규정 준수를 유지합니다. 정책 또는 VLAN을 생성하여 분리를 수행 할 수 있고, 802.1X 인증과 같은 기능을 통해 기업은 PCI 준수를 유지할 수 있습니다.



하이라이트:

- SD-Branch
- 방화벽 통합 관리
- Zero-Touch 배포
- 통합 보안 태세
- Layer 2 스위칭
- Multi-gigabit 성능
- 8/24/48-port 모델
- 다양한 PoE 옵션
- QoS 지원
- Switch 스택 지원
- 네트워크 세분화 및 규정 준수
- 콤팩트한 크기
- 에너지 효율 설계

SonicWall 스위치 시리즈 기능:

Management and Configuration
- Switch Auto-Discovery
- Daisy chaining
- Software Upgrade of Switches (From Firewall)
- Centralized VLAN Configuration
- Static/Dynamic LAG
- STP
- LLDP/MED
- IGMP Snooping
- Static Routing

Security and Visibility
- 802.1x Authentication
- Syslog Collection
- DHCP Snooping
- Device Detection (In Firewall)
- IP/MAC ACL

Firewall Features Enforced on Management Firewall
- Firewall
- IPS, AV, Application Control, Botnet

Layer 2
- Jumbo Frames
- Auto-negotiation for Port Speed and Duplex
- MDI/MDIX Auto-crossover
- MAC Bridging/STP
- Rapid Spanning Tree Protocol (RSTP)
- Multiple Spanning Tree Protocol (MSTP)
- STP Root Guard
- STP BPDU Guard
- Edge Port / Port Fast
- VLAN Tagging
- Guest VLAN and Voice VLAN
- Link Aggregation with LACP
- Unicast/Multicast traffic balance over trunking port
- Spanning Tree Instances (MSTP/CST)
- Flow Control and Back-pressure
- 10Base-T
- 100Base-TX
- 1000Base-SX/LX
- 1000Base-T
- Gigabit Ethernet support
- 10 Gigabit Ethernet (available on 24 and 48-port models only)
- CSMA/CD Access Method and Physical Layer Specifications
- Storm Control
- MAC, IP, Ethertype-based VLANs
- Port Mirroring
- Static Routing
- DHCP Relay
- IGMP Snooping

Security and Visibility
- ACL
- Port Mirroring
- Admin Authentication Via RFC 2865 RADIUS
- IEEE 802.1x authentication Port-based
- IEEE 802.1x Authentication MAC-based
- IEEE 802.1x Guest and Fallback VLAN
- IEEE 802.1ab Link Layer Discovery Protocol (LLDP)
- IEEE 802.1ab LLDP-MED
- DHCP-Snooping

Quality of Service
- IEEE 802.1p Based Priority Queuing
- IP TOS/DSCP Based Priority Queuing

Management
- IPv4 Management
- SSH
- HTTPS
- SNMP v1/v2c/v3
- Firewall Management, Standard CLI and
- Web GUI Interface
- Software download/upload: TFTP/ Firewall/GUI
- Managed through Capture Security Center

Management
- RFC 2571 Architecture for Describing SNMP
- DHCP Client
- RADIUS
- Ethernet-like Interface MIB
- MIB-II
- IP Forwarding Table MIB
- SNMP Message Processing and Dispatching
- SNMP MIB II
- SNMPv1/v2c

제품 세부 사양

Hardware	SWS12-8	SWS12-8POE	SWS12-10FPOE	SWS14-24	SWS14-24FPOE	SWS14-48	SWS14-48FPOE
1G Copper	8	8	10	24	24	48	48
1G SFP	2	2	2	-	-	-	-
10G SFP+	-	-	-	4	4	4	4
Total Interfaces	10	10	12	28	28	52	52
Memory(MB)	256	256	256	512	512	512	512
Flash(MB)	32	32	32	128	128	128	128
Packet 버퍼	512K	512K	512K	1.5M	1.5M	2M	2M
Mac 테이블	8K	8K	8K	32K	32K	32K	32K
스위칭 성능	20 Gbps	20 Gbps	24 Gbps	128 Gbps	128 Gbps	176 Gbps	176 Gbps
PoE Standard	-	802.3af	802.3af	-	802.3af/at	-	802.3af/at
PoE Power(Watts)	-	55	130	-	410	-	740
FAN	-	-	1	-	2	1	3

SONICWALL®

SonicWall Network Security appliance(NSa) series

중견기업, 분산된 기업 및 데이터 센터를 위한 업계에서 검증된 보안 효율성 및 성능

SonicWall Network Security Appliance(NSa) 시리즈는 고급 위협 방지 기능을 갖춘 고성능 보안 플랫폼에서 중간 규모 네트워크부터 분산된 기업 및 데이터 센터에 이르기까지 규모에 맞는 성능을 제공합니다. SonicWall Capture Cloud Platform에서 혁신적인 딥러닝 기술을 활용하여 NSa 시리즈는 조직이 필요로 하는 자동 실시간 침해 감지 및 예방 기능을 제공합니다.

뛰어난 위협 예방 및 성능

NSa 시리즈의 차세대 방화벽 (NGFW)은 다양한 보안기능을 수행하기 위해 특허를 받은 단일 패스 형태의 RFDPI 위협 방지 엔진을 사용합니다. 이 엔진은 모든 패킷을 바이트 단위로 검사하고, 인바운드 및 아웃 바운드 트래픽을 동시에 검사합니다.
SonicWALL NGFW의 보안 아키텍처는 NSS Labs의 보안 효율성 테스트를 통하여 지속적으로 업계 최고의 제품임을 입증하였습니다.

네트워크 제어 및 유연성

NSa 시리즈의 핵심은 SonicWall의 다양한 기능이 탑재된 SonicOS 운영체제 입니다. SonicOS는 애플리케이션 인텔리전스 및 제어, 실시간 시각화, 정교한 회피 차단 기술을 갖춘 IPS, 멀웨어 방지 및 웹/URL 필터링, 고속 가상 사설망 (VPN), 가상 LAN(VLAN) 및 기타 강력한 보안 기능을 통해 네트워크 제어와 유연성을 제공합니다.

손쉬운 배치, 설정 및 지속적인 관리

NSa 시리즈는 주요 보안, 연결 및 유연성 기술을 단 하나의 종합 솔루션으로 긴밀하게 통합합니다. 여기에는 SonicWave 무선 액세스 포인트와 SonicWall WAN 가속 기기 (WXA) 시리즈가 포함되며, 둘 다 자동으로 감지 및 관리 되어집니다.

Capture Security Center의 제로터치 배포를 통하여 원격 사무소 및 지사 위치에서 SonicWall 방화벽의 배포 및 프로비저닝을 단순화하고 가속화합니다. 단순화된 구축 및 설정과 함께 관리 용이성을 통해 조직은 총 소유 비용을 낮추고 높은 투자 수익률을 실현할 수 있습니다.

재조합이 필요 없는 RFDPI 엔진

혁신적인 멀티 코어 아키텍처와 특허 기술인 Reassembly-Free Deep Packet Inspection® (RFDPI) 기반의 싱글 패스 위협 차단 엔진이 통합 적용되어 있습니다. 이를 통해 업계 최고 수준의 보호와 성능, 확장성을 보장하며 높은 동시 커넥션 및 낮은 레이턴시와 함께 파일 크기에 제한 없이 최고 수준의 초당 연결 속도를 제공합니다.
또한, 시중의 레거시 방화벽 및 침입 방지 기술과 다르게 포트나 프로토콜에 관계없이 TLS/SSH 암호화된 연결의 완전한 암호 해독 및 검사도 수행하여 완전한 보호를 제공합니다.

최첨단 위협 방지

Capture Advanced Threat Protection(ATP) 서비스를 강화한 특허 출원 중인 RTDMI(Real-Time Deep Memory Inspection) 기술로 메모리에서 직접 검사하여 제로 데이 위협 및 알 수 없는 악성 프로그램을 사전에 감지하고 차단합니다.

Benefits:

뛰어난 위협 예방 및 성능

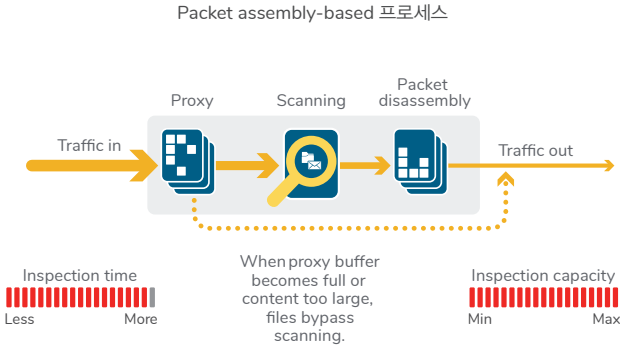
- 특허를 획득 한 재 조립이 필요 없는 Deep Packet 검사 기술
- 특허 출원 중인 실시간 딥 메모리 검사 기술
- On-box 및 클라우드 기반 위협 예방
- TLS / SSL 복호화 및 검사
- 업계에서 검증 된 보안 효과
- 멀티 코어 하드웨어 아키텍처
- 전문 Capture Labs 위협 연구 팀

네트워크 제어 및 유연성

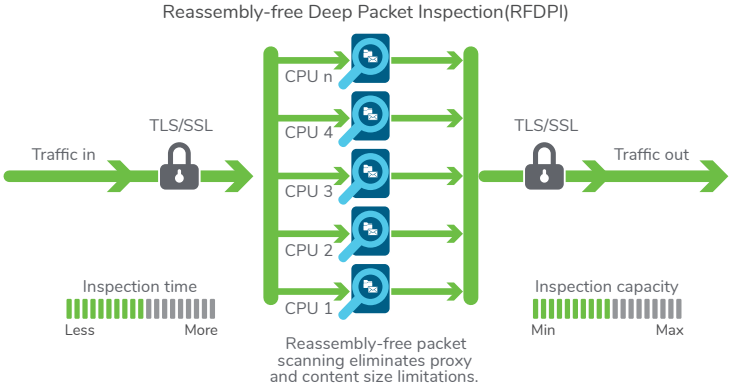
- Secure SD-WAN
- 강력한 SonicOS 운영 체제
- 응용 프로그램 인텔리전스 및 제어
- VLAN을 사용한 네트워크 세분화
- 고속 무선 보안

손쉬운 배치, 설정 및 지속적인 관리

- 긴밀하게 통합 된 솔루션
- 클라우드 및 on-premises 중앙 집중식 관리
- 여러 하드웨어 플랫폼을 통한 확장성
- 총 소유 비용 (TCO) 절감



프록시 기반의 아키텍처



SonicWall 스트리밍 기반의 아키텍처

NSa 시리즈 차세대 방화벽(NGFW)은 RFDPI 엔진과 RTDMI 이 두 가지 고급 보안 기술을 통합하여 한 단계 앞서가는 첨단 위협 방지 기능을 제공합니다.

안전한 고속 무선

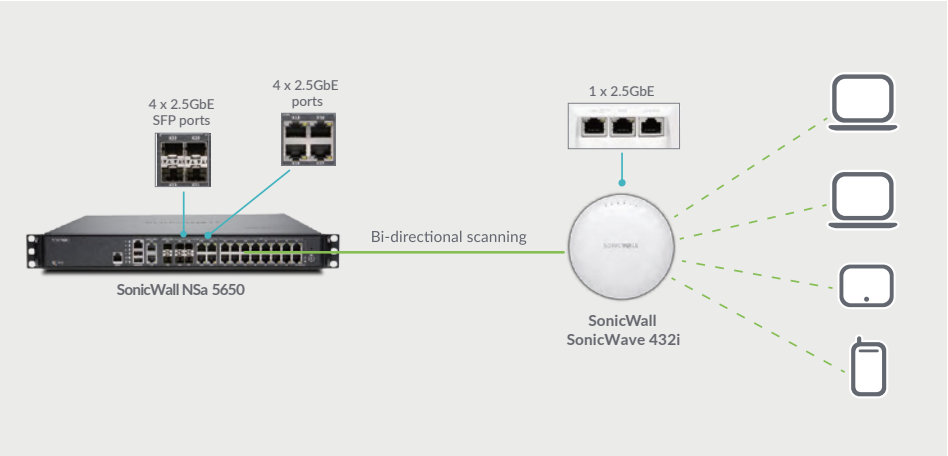
NSa 시리즈 차세대 방화벽과 SonicWall SonicWave 802.11ac Wave 2 무선 액세스 포인트를 결합하여 고속 무선 네트워크 보안 솔루션을 구축하십시오. NSa시리즈 방화벽과 SonicWave 액세스 포인트는 모두 웨이브 2 무선 기술에서 제공하는 멀티 기가비트 무선 처리가 가능한 2.5 GbE 포트를 갖추고 있습니다.

APT 방어

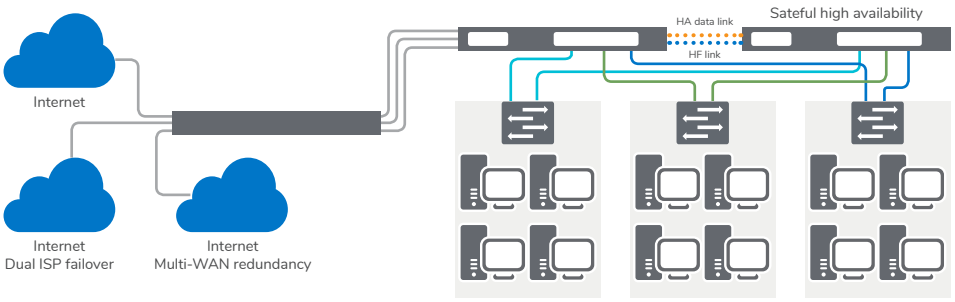
SonicWall Capture 고급 위협 방지 서비스는 방화벽 위협 보호 기능을 확장하여 제로 데이 위협을 방지합니다. 의심스러운 파일은 분석을 위해 클라우드 샌드박스로 전송되고, 평결이 결정될 때까지 방화벽에 보관할 수 있는 옵션을 제공합니다. 샌드 박스 플랫폼은 의심스러운 코드를 실행하고 동작을 분석하여 공격을 막기 위한 해시 시그니처를 방화벽으로 전송 합니다.

중앙관리 및 보고서

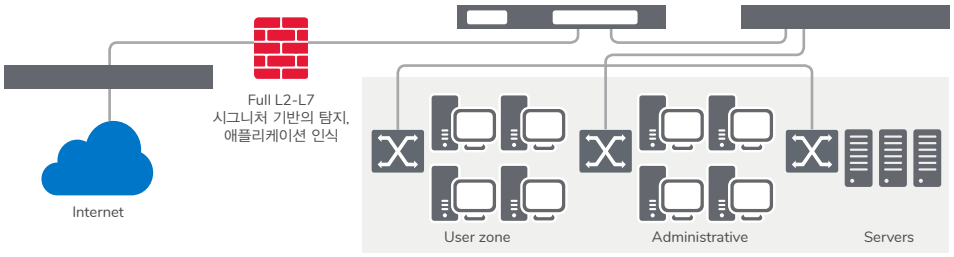
규모가 큰 분산 형 엔터프라이즈 배포의 경우, SonicWall GMS (Global Management System) 와 클라우드에서 제공되는 Capture Security Center를 통해 SonicWall 보안 장비를 중앙에서 관리 할 수 있어 관리의 용이성, 단순화 된 배포 및 설정을 통해 총 소유 비용을 낮추고 높은 투자 수익 (ROI)을 실현할 수 있습니다. 기업은 보안 어플라이언스 관리를 손쉽게 통합하고 관리 및 문제 해결의 복잡성을 줄일 수 있습니다.



중앙 게이트웨이 형태의 NSa Series



인라인 형태의 차세대 방화벽 NSa Series



제품 세부 사양

Hardware overview	NSa 2700	NSa 3700	NSa 4650	NSa 5650	NSa 6650	NSa 9250	NSa 9450	NSa 9650
Firewall General								
Operating System	SonicOS 7.0	SonicOS 7.0.1	SonicOS 6.5.4					
Interfaces	16x1GbE, 3x10G SFP+, 2 USB 3.0, 1 Console, 1 Management port	24x1GbE, 6x10G SFP+, 4x5G SFP+, 2 USB 3.0, 1 Console, 1 Mgmt. port	2 x 10-GbE SFP+, 4 x 2.5-GbE SFP, 4 x 2.5-GbE, 16 x 1-GbE, 1 GbE Management, 1 Console	2 x 10-GbE SFP+, 2 x 10-GbE, 4 x 2.5-GbE SFP, 4 x 2.5-GbE, 16 x 1-GbE, 1 GbE Management, 1 Console	6 x 10-GbE SFP+, 2 x 10-GbE, 4 x 2.5-GbE SFP, 8 x 2.5-GbE, 8 x 1-GbE, 1 GbE Management, 1 Console	10 x 10-GbE SFP+, 2 x 10-GbE, 8 x 2.5-GbE, 8 x 1-GbE, 1 GbE Management, 1 Console	10 x 10-GbE SFP+, 2 x 10-GbE, 8 x 2.5-GbE, 8 x 1-GbE, 1 GbE Management, 1 Console	10 x 10-GbE SFP+, 2 x 10-GbE, 8 x 2.5-GbE, 8 x 1-GbE, 1 GbE Management, 1 Console
Built-in storage (SSD)	64GB M.2	128GB M.2	32 GB	64 GB	64 GB	1TB, 128 GB	1TB, 128 GB	1TB, 128 GB
Access points supported (maximum)	32	32	128	192	192	192	192	192
Firewall/VPN performance								
Firewall inspection throughput	5.2 Gbps	5.5 Gbps	6.0 Gbps	6.25 Gbps	12.0 Gbps	12.0 Gbps	17.1 Gbps	17.1 Gbps
Threat Prevention throughput	3.0 Gbps	3.5 Gbps	2.5 Gbps	3.4 Gbps	5.5 Gbps	6.5 Gbps	9.0 Gbps	9.4 Gbps
Application inspection throughput	3.6 Gbps	4.2 Gbps	3.0 Gbps	4.25 Gbps	6.0 Gbps	7.8 Gbps	10.8 Gbps	11.5 Gbps
IPS throughput	3.4 Gbps	3.8 Gbps	2.3 Gbps	3.4 Gbps	6.0 Gbps	7.2 Gbps	10.2 Gbps	10.3 Gbps
TLS/SSL inspection and decryption throughput (DPI SSL)	800 Mbps	850 Mbps	675 Mbps	800 Mbps	1.45 Gbps	1.5 Gbps	2.1 Gbps	2.25 Gbps
IPSec VPN throughput[3]	2.10 Gbps	2.2 Gbps	3.0 Gbps	3.5 Gbps	6.0 Gbps	6.75 Gbps	10.0 Gbps	10.0 Gbps
Connections per second	21,500	22,500	40,000	40,000	90,000	90,000	130,000	130,000
Maximum connections (SPI)	1,5M	2M	3M	4M	5M	7.5M	10M	12.5M
Maximum connections (DPI)	0.5M	0.75M	1M	1.5M	2M	3M	4M	5M
Site-to-site VPN tunnels	2,000	3,000	4,000	6,000	8,000	12,000	12,000	12,000
IPSec VPN clients (maximum)	50 (1,000)	50 (1000)	2,000 (4,000)	2,000 (6,000)	2,000 (6,000)	2,000 (6,000)	2,000 (6,000)	2,000 (6,000)
SSL VPN licenses (maximum)	2 (500)	2 (500)	2 (1,000)	2 (1,500)	2 (2,000)	2 (3,000)	2 (3,000)	50 (3,000)

SONICWALL®