SONICWALL®

SonicWall SuperMassive 시리즈

엔터프라이즈 네트워크를 위한 타협 없는 고성능 차세대 방화벽 보호 솔루션

SonicWall SuperMassive 시리즈는 대규모 네트워크가 다중 기가비트 속도로 거의 지연 시간 제로의 환경에서 확장성, 안정성, 튼튼한 보안 기능을 발휘하도록 돕기 위해 설계된 SonicWall의 NGFW(차세대 방화벽) 플랫폼입니다.

기업, 정부 기관, 교육 기관, 소매점, 의료 기관과 서비스 공급자의 요구 사항에 맞추기 위해 제작된 SuperMassive 시리즈는 분산된 엔터프라이즈 네트워크, 데이터 센터, 서비스 공급자를 보호하는 데 가장 적합합니다.

SuperMassive 9000 시리즈는 SonicWall의 SonicOS 운영 체제, 특허를 받은* RFIPI(Reassembly-Free Deep Packet Inspection®) 기술, 대규모 멀티 코어, 크게 확장 가능한 하드웨어 아키텍처의 조합으로 다중 기가비트 속도로 업계 최고 수준의 애플리케이션 제어, 침입 방지, 맬웨어 차단, TLS/SSL 암호 해독과 검사 기능을 수행할 수 있습니다. SuperMassive 시리즈는 PSC (전력, 공간, 냉각)을 염두에 두고 세심하게 설계되어 고성능 패킷과 데이터 처리, 애플리케이션 제어와 위협 방지를 위한 업계 최고의 와트당 Gbps의 NGFW(차세대 방화벽)를 가지고 있습니다.

SonicWall RFDPI 엔진은 모든 포트에서 모든 패킷의 모든 바이트를 스캔하여 전체 스트림에서 전체 컨텐츠를 검사할 수 있으며, 동시에 성능이 뛰어나고 지연 시간이 낮습니다. 이 기술은 안티 맬웨어 프로그램에 포함된 소켓을 사용하여 콘텐츠를 재구성하는 프록시 디자인보다 탁월합니다. 기존의 디자인은 비효율적이고 소켓 메모리 스레싱의 오버헤드로 인해 지연 시간이 길어지고 성능이 떨어지며 파일 크기 제한이 생깁니다. RFDPI 엔진은 완전한 컨텐츠 검사 기능을 통해 네트워크에 진입하기 전에 다양한 형태의 맬웨어를 제거하고, 파일 크기, 성능 또는 대기 시간 제한 없이 진화하는 위협에 대응하여 보호합니다.

또한 RFDPI 엔진은 TLS/SSL, SSH 암호화 트래픽은 물론 프록시가 허용되지 않는 애플리케이션에 대해서도 전체 암호 해독과 검사를 수행하므로 전송 방식이나 프로토콜에 관계없이 완벽한 보호가 가능합니다. 또한 모든 패킷(헤더와 데이터 부분)을 깊이 조사하여 프로토콜 비준수, 위협, 제로 데이, 침입을 검색하고, 조건을 정의하여 암호화된 트래픽 내부에 숨겨진 공격을 차단하고, 감염 전파를 막고, 명령 및 제어(C&C) 통신과 데이터 추출을 무력화합니다. 포함 규칙과 제외 규칙을 사용하면 전체 제어를 통해 특정 조직의 규정 준수 및/또는 법적 요구 사항에 따라 암호 해독과 검사의 대상이 되는 트래픽을 맞춤화할 수 있습니다.

애플리케이션 트래픽 분석을 사용하면 생산적인 애플리케이션과 비생산적인 애플리케이션 트래픽을 실시간으로 파알할 수 있으며, 강력한 애플리케이션 수준의 정책으로 트래픽을 제어할 수 있습니다. 애플리케이션 제어는 일정, 예외 목록을 사용하여 사용자별, 그룹별로 수행할 수 있습니다. 모든 애플리케이션, 침입 방지, 맬웨어 시그니처는 SonicWALL Capture Labs 위협 연구 팀에서 지속적으로 업데이트합니다. 또한 특별히 제작된 고급 운영 체제인 SonicOS는 맞춤형 애플리케이션을 파악하고 제어 할 수 있는 통합 도구를 갖추고 있습니다.

*미국 특허 7,310,815; 7,600,257; 7,738,380; 7,835,361

SuperMassive 9000 시리즈

장점:

- 고성능 침입 방지, 낮은 지연 시간의 맬웨어 방지, 클라우드 기반 샌드박싱을 포함한 완전한 위반 방지
- 완전하고 세밀한 애플리케이션 파악, 제어, 시각화 기능
- 성능 문제 없이 TLS/SSL과 SSH 암호화 트래픽의 암호를 해독하고 검사하여 숨겨진 위협을 찾아서 차단
- 10/40Gbps 데이터 센터의 보안 성능 향상
- 서비스 수준 증가에 적응하고 네트워크 서비스와 리소스를 사용 가능하며 보호되는 상태로 유지

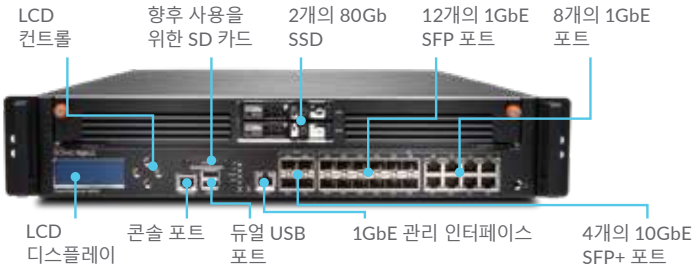
파트너 지원 서비스

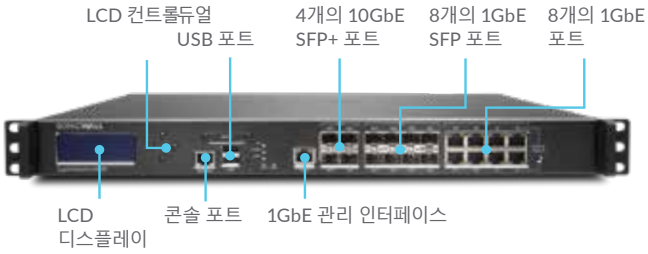
SonicWall 솔루션의 계획이나 배포, 최적화에 도움이 필요하세요? SonicWall Advanced Services Partner는 세계적 수준의 전문 서비스를 제공할 수 있도록 교육을 받았습니다. www.sonicwall.com/PES 에서 자세히 알아보세요.

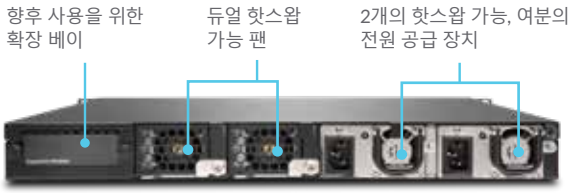
시리즈 라인업

SonicWall SuperMassive 9000 시리즈는 4개의 10GbE SFP+, 최대 12개의 1GbE SFP, 8개의 1GbE 쿠퍼와 1개의 GbE 관리 인터페이스, 추가로 2개의 10GbE SFP+ 인터페이스(이후 출시)로 구성됩니다. 9000 시리즈는 팬 모듈과 전원 공급 장치를 핫스왑 방식으로 교체할 수 있습니다.

SuperMassive 9000 시리즈





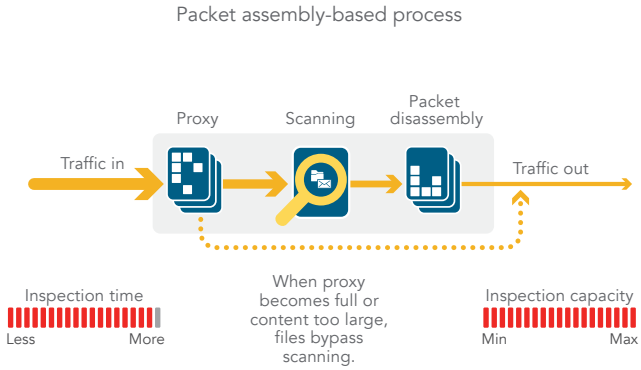


성능	9200	9400	9600	9800
프로세싱 코어	24	32	32	64
방화벽 처리량	15Gbps	20Gbps	20Gbps	31.8Gbps
애플리케이션 검사 처리량	5Gbps	10Gbps	11.5Gbps	23Gbps
IPS(침입 방지 시스템) 처리량	5Gbps	10Gbps	11.5Gbps	21.3Gbps
안티 맬웨어 검사 처리량	3.5Gbps	4.5Gbps	5Gbps	11Gbps
최대 DPI 연결	1.5M	1.5M	2.0M	8.0M
배포 모드	**9200**	**9400**	**9600**	**9800**
L2 브리지 모드	지원	지원	지원	지원
와이어 모드	지원	지원	지원	지원
게이트웨이/NAT 모드	지원	지원	지원	지원
탭 모드	지원	지원	지원	지원
투명 모드	지원	지원	지원	지원

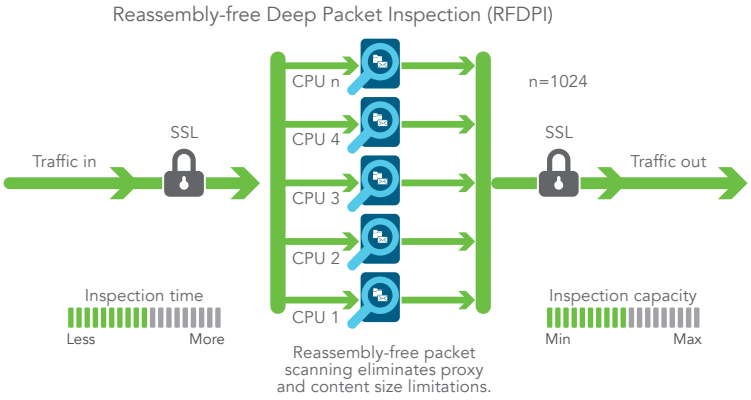
RFDPI(Reassembly-Free Deep Packet Inspection) 엔진

RFDPI는 일회 통과, 낮은 지연 시간의 검사 시스템으로, 프록시나 버퍼링없이 빠른 속도로 스트림 기반, 양방향 트래픽 분석을 수행하여 포트와 프로토콜에 관계없이 침입 시도, 맬웨어, 애플리케이션 트래픽을 효율적으로 파악합니다. 이 독점 엔진은 3-7 계층에서 위협을 탐지하기 위해 스트리밍 트래픽 페이로드 검사를 사용합니다. RFDPI 엔진은 탐지 엔진을 혼란스럽게 만들어 악성 코드를 네트워크에 몰래 넣으려는 지능형 난독화 및 회피 기술을 무력화하기 위해 네트워크 스트림이 광범위하고 반복되는 정규화와 암호 해독을 거치도록 합니다.

일단 패킷이 TLS/SSL 암호 해독을 포함하여 필요한 사전 처리를 거치면, 침입 공격, 맬웨어, 봇넷, 애플리케이션 등 여러 시그니처 데이터베이스를 나타내는 하나의 전용 메모리 표현과 비교하여 분석됩니다. 그러면 연결 상태가 공격 상태나 다른 " 일치" 이벤트가 발생할 때까지 이러한 데이터베이스를 기준으로 한 스트림의 위치를 나타내도록 설정되며, 공격 상태나 다른 일치 이벤트가 발생하면 미리 설정된 작업이 수행됩니다. 대부분의 경우 수행되는 작업은 연결을 끊고 적절한 로그 기록과 알림 이벤트가 만드는 것입니다. 하지만 검사만 하도록 엔진을 구성할 수도 있으며, 애플리케이션 탐지의 경우 애플리케이션이 파악되는 즉시 나머지 애플리케이션 스트림에 7계층 대역폭 관리 서비스를 제공하도록 구성할 수도 있습니다.



Competitive proxy-based architecture

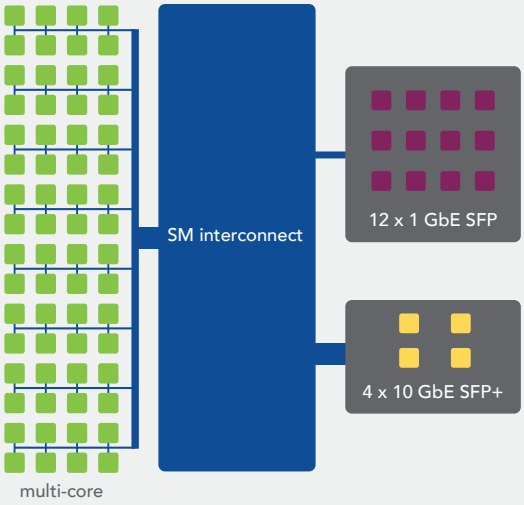


SonicWall stream-based architecture

극한의 확장성과 성능을 위한 확장 가능 아키텍처

RFDPI 엔진은 높은 수준의 성능으로 보안 검사를 수행하여, 기본적으로 병렬 방식이고 끊임없이 증가하는 네트워크 트래픽의 특성에 맞추는 데 주력하여 설계되었습니다. 이 병렬 처리 중심의 소프트웨어 아키텍처를 멀티 코어 프로세서 시스템과 결합하면 높은 트래픽 부하에서 DPI(딥 패킷 검사)의 수요를 해결할 수 있도록 완벽하게 확장됩니다. SuperMassive 플랫폼에서 사용하는 프로세서는 x86과 달리 패킷, 암호, 네트워크 처리에 최적화되어 있으며, 유연성과 현장 프로그래밍 가능성은 그대로 가진 프로세서입니다. ASIC에서는 이 부분에 약점이 있었습니다.

이러한 유연성은 업데이트와 더 정교한 탐지 기술이 필요한 새로운 공격으로부터 보호하기 위해 새로운 코드와 동작 업데이트가 필요한 때 필수적입니다. 이 플랫폼 설계의 또 다른 특징은 시스템의 어떤 코어로도 새 연결을 만들 수 있는 고유한 기능으로, 최고의 확장성을 확보하고 트래픽 급증을 처리할 수 있는 수단이 됩니다. 이 접근 방식은 딥 패킷 검사가 활성화된 상태에서도 매우 빠른 새 세션 생성 속도(초당 새 연결)를 가능하게 합니다. 기본 방식에서는 이 부분이 데이터 센터 배포 환경에서 병목 현상을 일으키는 주 원인이었습니다.



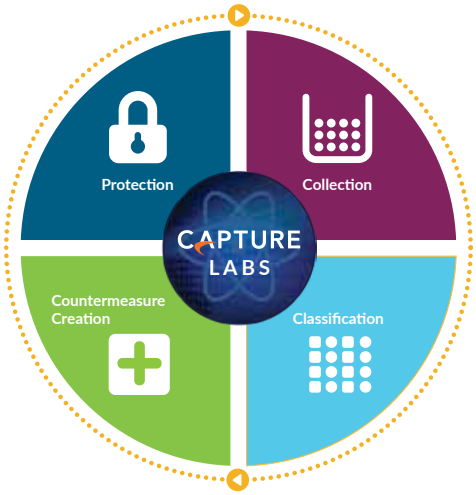
SONICWALL®

Capture Labs

SonicWall 전담 팀이자 내부 소속인 SonicWall Capture Labs 위협 연구 팀은 최신 상태의 보호를 위해 고객의 방화벽에 배포할 방어 대책을 연구하고 개발합니다. 이 팀은 여러 출처에서 잠재적 위협 데이터를 수집합니다. 출처로는 수상 경력이 있는 SonicWall의 네트워크 샌드박싱 서비스, Capture Advanced Threat Protection, 전 세계에 위치하여 최신 위협의 트래픽을 모니터링하는 백만 개 이상의 SonicWall 센서가 있습니다. 수집된 데이터는 SonicWall의 딥 러닝 알고리즘을 사용한 기계 학습을 통해 분석되고, 코드에서 DNA를 추출하여 알려진 악성 코드 형태와 관련이 있는지 확인합니다.

최신 보안 기능이 포함된 SonicWall NGFW(차세대 방화벽) 고객은 24시간 보호 환경에 대한 지속적인 업데이트를 받을 수 있습니다. 새 업데이트는 재부팅이나 작동 중단 없이 즉시 적용됩니다. 어플라이언스의 시그너처는 다양한 종류의 공격을 방어하며, 하나의 시그니처로 최대 수만 개의 개별 위협을 처리할 수 있습니다.

어플라이언스 차원의 보호 방법 외에 SuperMassive 방화벽은 SonicWall CloudAV[1]에도 액세스할 수 있습니다. 이를 통해 기본 시그니처 인텔리전스를 수천만 개의 시그니처로 확장할 수 있으며, 그 수는 매년 수백만 개씩 늘어납니다. 방화벽은 어플라이언스에서 수행되는 검사를 강화하기 위해 독점, 경량 프로토콜을 사용하여 이 CloudAV 데이터베이스에 액세스합니다. 기업은 클라우드 기반의 다중 엔진 샌드박스인 Capture Advanced Threat Protection[1]을 사용하여 의심스러운 파일과 코드를 격리된 환경에서 검사함으로써, 제로 데이 공격과 같은 지능형 위협을 막을 수 있습니다.



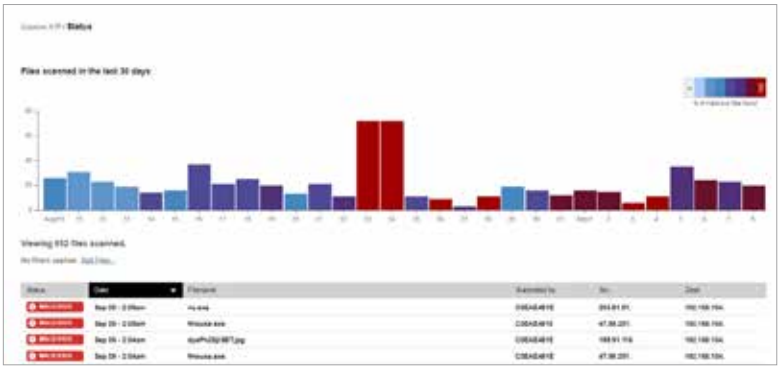
[1] *추가 구독이 필요합니다.*

고급 위협 방지

SonicWall Capture Advanced Threat Protection 서비스[1]는 방화벽 위협 보호 기능을 확장하여 제로 데이 위협을 탐지하고 방지하는 클라우드 기반의 다중 엔진 샌드박스입니다. 의심스러운 파일은 분석을 위해 클라우드로 전송되며, 필요하다면 판결이 내려질 때까지 게이트웨이에서 파일을 보관하도록 선택할 수 있습니다. 가상화된 샌드박싱, 전체 시스템 에뮬레이션, 하이퍼바이저 수준의 분석 기술을 가진 다중 엔진 샌드박스 플랫폼은 의심스러운 코드를 실행하여 동작을 분석합니다. 악성 파일로 확인되면 Capture에서 해시가 즉시 생성되고, 나중에 후속 공격을 막기 위해 시그니처가 방화벽으로 전송됩니다.

서비스는 실행 프로그램, DLL, PDF, MS Office 문서, 아카이브, JAR, APK를 포함하여 광범위한 운영 체제와 파일 형식을 분석합니다.

Capture는 한눈에 볼 수 있는 위협 분석 대시보드와 보고서를 제공합니다. 여기에는 출처, 목적지, 요약 내용과 막지 못했을 때 맬웨어가 할 행동의 자세한 내용을 포함하여 서비스로 전송된 파일에 대한 상세한 분석 결과가 포함되어 있습니다.



SONICWALL

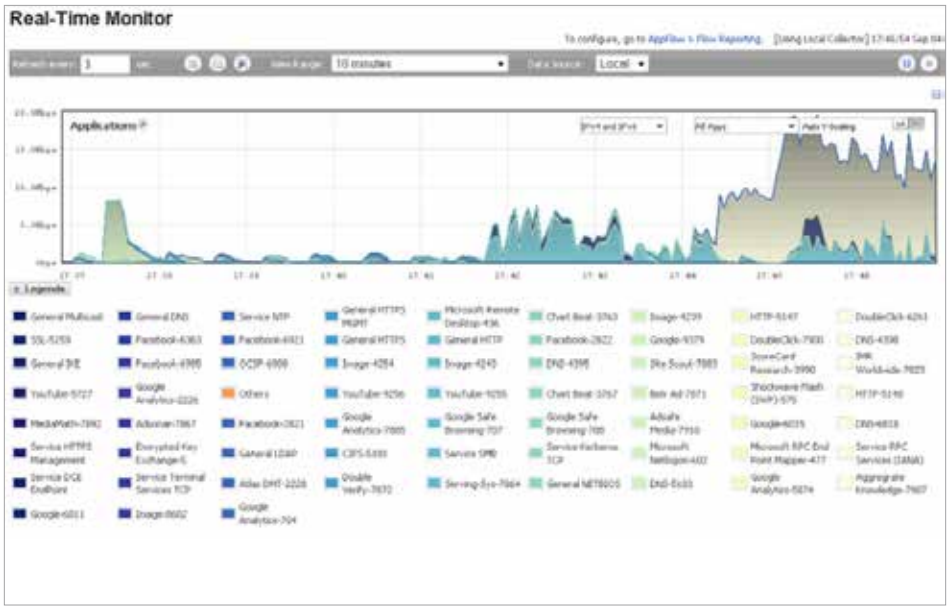
애플리케이션 인텔리전스와 제어

애플리케이션 인텔리전스는 관리자에게 네트워크를 따라 전달되는 애플리케이션 트래픽을 알려서 관리자가 비즈니스 우선 순위에 따라 애플리케이션 제어를 예약하고, 비생산적인 애플리케이션을 차단하고, 위험 가능성이 있는 애플리케이션을 차단할 수 있도록 합니다. 실시간 시각화 기능을 통해 트래픽 이상 현상이 발생하면 바로 파악하고, 인바운드 또는 아웃바운드 공격이나 성능 병목 현상의 원인이 될 수 있는 대상에 즉각적인 조치를 취할 수 있습니다.

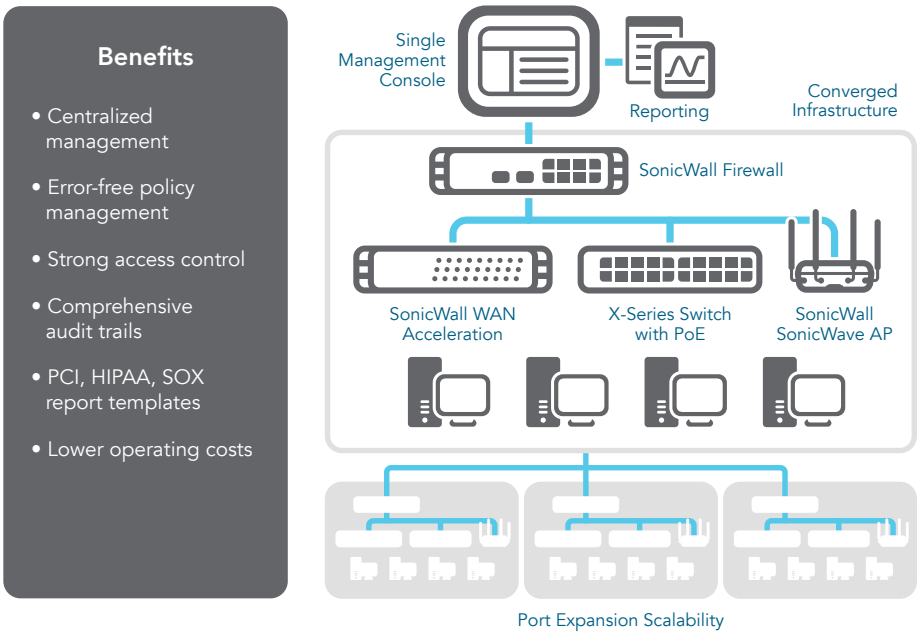
SonicWall Application Traffic Analytics[1]는 애플리케이션 트래픽, 대역폭 사용, 보안 위협은 물론 강력한 문제 해결과 포렌식 분석 기능을 가능하게 하는 구체적인 통찰력을 제공합니다. 또한 보안 SSO(싱글 사인온) 기능으로 사용자 환경을 편리하게 만들어 생산성은 높이고 지원 요청은 줄입니다. 애플리케이션 인텔리전스와 제어는 직관적인 웹 기반 인터페이스로 간단하게 관리할 수 있습니다.

글로벌 관리와 보고

보안 관리, 규정 준수, 위험 관리 전략을 완전하게 따르고자 하는 엄격하게 규제되는 기업의 경우, 옵션으로 선택할 수 있는 SonicWall Global Management System[1](GMS®)을 사용하면 됩니다. GMS는 관리자가 상호 연결되고 감사 가능한 업무 흐름 프로세스로 SonicWall 방화벽, 무선 액세스 포인트, 스위치를 관리할 수 있는 통합되고 안전하며 확장 가능한 플랫폼을 제공합니다. GMS를 사용하면 기업에서는 보안 어플라이언스 관리를 손쉽게 통합하고, 관리 과정에서 발생할 수 있는 복잡한 절차와 복잡한 문제 해결 절차를 줄이며, 보안 인프라의 모든 운영 활동을 관리할 수 있습니다. 관리할 수 있는 활동에는 중앙 집중식 정책 관리와 시행, 실시간 이벤트 모니터링, 사용자 활동, 애플리케이션 식별, 흐름 분석과 포렌식, 규정 준수와 감사 보고 등이 있습니다. 또한 GMS는 워크플로 자동화 기능을 사용하여 기업의 방화벽 변경 관리 요구 사항을 충족시킵니다. GMS 워크플로 자동화를 통해 모든 기업은 적시에 규정에 따라 올바른 방화벽 정책을 신속하게 배포할 수 있는 민첩성을 확보하여 안심할 수 있게 됩니다. GMS는 비즈니스 프로세스와 서비스 수준별로 네트워크 보안을 관리할 수 있는 일관된 방법을 제공하므로, 장치별로 관리하는 것보다 전체 보안 환경의 라이프 사이클 관리가 크게 간소화됩니다.



SonicWall GMS Secure Compliance Enforcement



[1] *추가 구독이 필요합니다.*

SONICWALL®

기능

RFDPI 엔진	
기능	설명
RFDPI(Reassembly-Free Deep Packet Inspection)	이 고성능, 독점, 특허 보유 검사 엔진은 프록시나 버퍼링없이 스트림 기반의 양방향 트래픽 분석을 수행하여 침입 시도와 맬웨어를 발견하고, 포트에 관계없이 애플리케이션 트래픽을 파악합니다.
양방향 검사	인바운드와 아웃바운드 트래픽의 위협을 동시에 검색하여 네트워크가 맬웨어를 배포하는 데 사용되지 않도록 하고, 감염된 시스템이 내부에 들어올 경우 공격의 시작 플랫폼이 되지 않도록 합니다.
스트림 기반 검사	프록시가 없고 버퍼링을 하지 않는 검사 기술로, 파일과 스트림 크기에 제한 없이 수백만 개의 동시 네트워크 스트림의 DPI를 수행해도 지연 시간이 아주 짧고, 원시 TCP 스트림뿐만 아니라 일반적인 프로토콜에도 적용할 수 있습니다.
놓은 병렬 처리 능력과 확장성	RFDPI 엔진의 고유한 설계는 멀티 코어 아키텍처에 아주 잘 맞습니다. 이 둘을 결합하면 DPI 처리량이 높아지고 새 세션을 만드는 속도가 매우 빨라져서 처리량이 많은 네트워크에서 트래픽 급증을 처리할 수 있습니다.
일회 통과 검사	일회 통과 DPI 아키텍처는 맬웨어와 침입을 검사하고 애플리케이션을 파악하는 일을 동시에 수행하여 DPI 지연 시간을 대폭 단축하고, 모든 위협 정보가 한 아키텍처 내에서 서로 연관되도록 합니다.

방화벽과 네트워킹	
기능	설명
REST API	방화벽이 제로 데이, 악의적인 내부자, 위조된 자격 증명, 랜섬웨어, 지능형 지속 위협과 같은 지능형 위협에 대처하기 위해 원래 장비의 독점 제조업체와 타사 인텔리전스 피드를 받아 활용하도록 합니다.
상태 보존형 패킷 검사	모든 네트워크 트래픽을 검사하고 분석하여 방화벽 액세스 정책을 준수하도록 합니다.
고가용성/클러스터링	SuperMassive 시리즈는 액티브/패시브(A/P) 상태 동기화, 액티브/액티브(A/A) DPI, 액티브/액티브 클러스터링 고가용성 모드를 지원합니다. 액티브/액티브 DPI는 딥 패킷 검사 부하를 패시브 어플라이언스로 분산하여 처리량을 높입니다.
DDoS/DoS 공격 방지	SYN 플러드 방지는 3계층 SYN 프록시와 2계층 SYN 블랙리스트 기술을 사용하는 DOS 공격을 방어합니다. 또한 UDP/ICMP 플러드 방지와 연결 속도 제한을 통해 DOS/DDoS로부터 보호합니다.
IPv6 지원	인터넷 프로토콜 버전 6(IPv6)은 IPv4를 대체할 초기 단계입니다. 최신 SonicOS 6.2를 사용하면 하드웨어가 필터링과 와이어 모드 구현을 지원합니다.
유연한 배포 옵션	SuperMassive 시리즈는 기존의 NAT, 2계층 브리지, 와이어와 네트워크 탭 모드로 배포할 수 있습니다.
WAN 부하 분산	라운드 로빈, 스필오버, 퍼센테이지 방식을 사용하여 여러 WAN 인터페이스의 부하를 분산합니다. 정책 기반 라우팅을 사용하면 프로토콜에 따라 선호하는 WAN 연결로 트래픽을 보낼 경로를 만들 수 있으며, 경로를 사용할 수 없을 때는 보조 WAN으로 장애 복구될 수 있습니다.
고급 서비스 품질(QoS)	네트워크에서 802.1p, DSCP 태깅, VoIP 트래픽 리매핑을 통한 중요 통신을 보장합니다.
H.323 게이트키퍼와 SIP 프록시 지원	모든 수신 호출이 H.323 게이트키퍼나 SIP 프록시에 의해 허가되고 인증되도록 함으로써 스팸 호출을 차단합니다.
단일 및 계단식 Dell X-시리즈 네트워크 스위치 관리	Dell의 X-시리즈 네트워크 스위치용 방화벽 관리 대시 보드를 사용하여 하나의 창에서 포트쉴드, HA, POE, POE+를 포함한 추가 포트의 보안 설정을 관리합니다.
생체 인증	지문 인식과 같이 쉽게 복제되거나 공유될 수 없는 모바일 장치 인증을 네트워크 액세스를 위한 사용자 ID 인증에 사용할 수 있도록 지원합니다.
공개 인증과 소셜 로그인	게스트 사용자가 페이스북, 트위터 또는 Google+와 같은 소셜 네트워킹 서비스의 자격 증명을 사용하여 로그인하고, 통과 인증을 사용하여 호스트의 무선, LAN 또는 DMZ 영역을 통해 인터넷과 기타 게스트 서비스에 액세스할 수 있도록 합니다.
다중 도메인 인증	모든 네트워크 도메인에서 보안 정책을 간단하고 신속하게 관리할 수 있도록 합니다. 개별 정책을 하나의 도메인에 적용하거나 도메인 그룹에 적용할 수 있습니다.

관리와 보고	
기능	설명
GMS(글로벌 관리 시스템)[1]	SonicWALL GMS는 직관적인 인터페이스를 가진 하나의 콘솔을 통해 여러 SonicWALL 어플라이언스를 모니터링, 구성, 보고하여 관리 비용과 복잡성을 줄입니다.
강력한 단일 장치 관리	직관적인 웹 기반 인터페이스로 빠르고 편리하게 구성할 수 있으며, 포괄적인 명령줄 인터페이스와 SNMPv2/3도 지원됩니다.
IPFIX/NetFlow 애플리케이션 흐름 보고	IPFIX 또는 NetFlow 프로토콜을 통해 애플리케이션 트래픽 분석과 사용 데이터를 내보내 SonicWall Scrutinizer나 IPFIX와 NetFlow 확장 기능을 지원하는 도구 등으로 실시간 모니터링과 내역 모니터링을 진행합니다.

기능

가상 사설망(VPN)	
기능	설명
자동 프로비저닝 VPN	SonicWall 방화벽 사이의 초기 사이트 간 VPN 게이트웨이 프로비저닝을 자동화하여 복잡한 분산형 방화벽 배포를 간소화하고 필요한 작업을 줄이며, 보안과 연결이 즉시, 자동으로 이루어지도록 합니다.
사이트 간 연결을 위한 VPN	SuperMassive 시리즈가 수천 개의 다른 대규모 사이트, 지사 또는 본사의 VPN 집중 장치 역할을 할 수 있도록 하는 고성능 IPSec VPN입니다.
SSL VPN 또는 IPSec 클라이언트 원격 액세스	클라이언트가 없는 SSL VPN 기술이나 관리하기 쉬운 IPSec 클라이언트를 활용하여 다양한 플랫폼의 이메일, 파일, 컴퓨터, 인트라넷 사이트, 애플리케이션에 쉽게 액세스합니다.
여분의 VPN 게이트웨이	여러 WAN을 사용할 때는 모든 VPN 세션의 원활한 자동 장애 조치와 장애 복구가 가능하도록 기본과 보조 VPN을 구성할 수 있습니다.
경로 기반 VPN	VPN 링크를 통해 동적으로 라우팅하는 기능입니다. 엔드포인트 사이에서 대체 경로를 사용하여 다시 트래픽을 라우팅할 수 있도록 하여 일시적으로 VPN 터널 장애가 발생해도 계속 가동할 수 있도록 합니다.

콘텐츠/정황 인식	
기능	설명
사용자 활동 추적	사용자 ID와 활동은 매끄러운 AD/LDAP/Citrix1/Terminal Services1 SSO 통합과 DPI를 통해 얻은 광범위한 정보를 결합하여 추적할 수 있습니다.
GeoIP 국가별 ID	특정 국가로 가거나 그 국가에서 오는 네트워크 트래픽을 파악하고 제어하여 위협 활동의 알려지거나 의심되는 출처로부터의 공격을 차단하거나, 네트워크에서 발생한 의심스러운 트래픽을 조사합니다. 국가와 봇넷의 맞춤형 목록을 작성하여 IP 주소에 연결된 잘못된 국가나 봇넷 태그를 무시할 수 있습니다.
정규식 DPI 필터링	정규식 검색을 통해 네트워크를 오가는 컨텐츠를 파악하고 제어함으로써 데이터 유출을 방지합니다.

Capture 지능형 위협 방지[1]	
기능	설명
다중 엔진 샌드박싱	가상화된 샌드박싱, 전체 시스템 에뮬레이션, 하이퍼바이저 수준의 분석 기술을 가진 다중 엔진 샌드박스 플랫폼은 의심스러운 코드를 실행하여 동작을 분석합니다. 이를 통해 악성 활동에 대한 포괄적인 가시성을 얻을 수 있습니다.
판결까지 차단	국가와 봇넷의 맞춤형 목록을 작성하여 IP 주소에 연결된 잘못된 국가나 봇넷 태그를 무시할 수 있습니다.
다양한 파일 형식 분석	실행 프로그램(DLL), PDF, MS Office 문서, 아카이브, JAR, APK, 그리고 Windows, Android, Mac OS와 여러 브라우저 환경을 포함한 여러 운영 체제의 광범위한 파일 형식을 분석할 수 있도록 지원합니다.
시그니처의 신속한 배포	파일이 악의적인 것으로 확인되면 시그니처가 SonicWALL Capture 구독이 있는 방화벽, GRID 게이트웨이 안티 바이러스, IPS 시그니처 데이터베이스와 URL, IP, 도메인 평판 데이터베이스에 48시간 이내에 즉시 배포됩니다.
Capture 클라이언트	Capture 클라이언트는 고급 맬웨어 보호, 암호화된 트래픽 확인 기능을 비롯한 여러 엔드포인트 보호 기능을 가진 통합된 클라이언트 플랫폼입니다. 이 솔루션은 계층화된 보호 기술, 포괄적인 보고 기능, 엔드 포인트 보호 시행 기능을 활용합니다.

암호화된 위협 방지[1]	
기능	설명
TLS/SSL 암호 해독과 검사	맬웨어, 침입, 데이터 유출에 대해 즉석에서 SSL/TLS 트래픽을 암호 해독하고 검사하며, TLS/SSL 암호화 트래픽에 숨어 있는 위협으로부터 시스템을 보호하기 위해 애플리케이션, URL, 콘텐츠 제어 정책을 적용합니다. 모든 모델의 보안 구독에 포함됩니다.
SSH 검사	DPI-SSH(SSH의 딥 패킷 검사)는 SSH 터널을 통해 이동하는 데이터를 암호 해독하고 검사하여 SSH를 이용하는 공격을 방지합니다.

침입 방지[1]	
기능	설명
대응책 기반 보호	긴밀하게 통합된 IPS(침입 방지 시스템)은 시그니처와 기타 대응책을 활용하여 패킷 페이로드에서 취약성과 악용을 검사하고 광범위한 공격과 취약점을 처리합니다.
자동 시그니처 업데이트	SonicWall 위협 조사 팀은 50개가 넘는 공격 범주가 있는 광범위한 IPS 대응책 목록을 계속 연구하여 업데이트를 배포합니다. 새 업데이트는 재부팅이나 서비스 중단 없이 즉시 적용됩니다.
영역 내 IPS 보호	네트워크를 여러 보안 영역으로 나누고 위협이 영역 경계를 넘어 전파되는 것을 침입 방지 서비스로 방지함으로써 내부 보안을 강화합니다.
봇넷 명령 및 제어(CnC) 탐지와 차단	로컬 네트워크의 봇에서 발생하는 명령 및 제어 트래픽, 맬웨어를 전파하는 것으로 파악된 IP나 도메인, 알려진 CnC 지점을 파악하여 차단합니다.
프로토콜 남용/이상 탐지와 예방	IPS를 숨어서 지나가기 위해 프로토콜을 악용하는 공격을 파악하고 차단합니다.
제로 데이 보호	수천 가지 개별 악용 사례를 활용하는 교묘한 최신 악용 방법과 기법에 대응하여 지속적으로 업데이트된 기술을 사용하여 제로 데이 공격으로부터 보호합니다.
회피 차단 기술	다양한 스트림 정규화, 디코딩, 기타 기술을 활용하여 위협이 2-7계층의 회피 기술을 사용하여 탐지되지 않고 네트워크에 진입하지 못하도록 합니다.

기능

위협 방지[1]	
기능	설명
게이트웨이 안티 맬웨어	RFDPI 엔진은 모든 포트와 TCP 스트림에서 파일을 길이와 크기 제한 없이 검사하여 모든 인바운드, 아웃바운드, 영역 내 트래픽에 바이러스, 트로이 목마, 키 로거와 기타 맬웨어가 있는지 확인합니다.
CloudAV 맬웨어 방지	수천만 개의 위협 시그니처가 지속적으로 업데이트되는 데이터베이스로, SonicWall 클라우드 서버에 상주하며 광범위한 위협 처리 범위를 가지고 있어, 온보드 시그니처 데이터베이스의 기능을 보완해야 할 때 참조합니다.
24시간 보안 업데이트	새로운 위협 업데이트는 능동적인 보안 서비스로 현장의 방화벽에 자동으로 전송되어 재부팅이나 실행 중단없이 즉시 적용됩니다.
양방향 원시 TCP 검사	RFDPI 엔진은 모든 포트에서 양방향으로 원시 TCP 스트림을 검사할 수 있어, 잘 알려진 몇 개의 포트를 보호하는 데 주력하는 오래된 보안 시스템으로 몰래 들어가는 공격을 방지할 수 있습니다.
광범위한 프로토콜 지원	원시 TCP로 데이터를 보내지 않는 HTTP/S, FTP, SMTP, SMBv1/v2 등의 일반적인 프로토콜을 파악하고, 잘 알려진 표준 포트에서 실행되지 않더라도 맬웨어 검사를 위해 페이로드를 디코딩합니다.

애플리케이션 인텔리전스와 제어[1]	
기능	설명
애플리케이션 제어	RFDPI 엔진이 지속적으로 확장되는 수천 개의 애플리케이션 시그니처와 비교하여 파악한 애플리케이션이나 각 애플리케이션 기능을 제어하여 네트워크 보안과 네트워크 생산성을 향상시킵니다.
맞춤형 애플리케이션 파악	네트워크를 더 잘 제어할 수 있도록 각각의 고유한 매개 변수나 패턴을 기반으로 시그니처를 만들어 맞춤형 애플리케이션을 제어합니다.
애플리케이션 대역폭 관리	불필요한 애플리케이션 트래픽은 차단하면서 중요한 애플리케이션이나 애플리케이션 범주를 위해 이용 가능한 대역폭을 세밀하게 할당하고 조정합니다.
세밀한 제어	애플리케이션이나 특정 구성 요소를 일정, 사용자 그룹, 제외 목록, 다양한 작업을 기준으로 제어합니다. 작업에는 LDAP/AD/터미널 서비스/Citrix 통합을 통해 파악할 수 있는 전체 SSO 사용자 ID를 사용할 수 있습니다.

콘텐츠 필터링[1]	
기능	설명
내부/외부 콘텐츠 필터링	수용할 수 있는 사용 정책을 적용하고, 콘텐츠 필터링 서비스로 불쾌하거나 비생산적인 정보나 이미지가 포함된 웹 사이트에 액세스하지 못하도록 합니다.
강제 콘텐츠 필터링 클라이언트	정책 적용 범위를 확대하여 방화벽 경계 외부에 있는 Windows, Mac OS, Android, Chrome 기기의 인터넷 콘텐츠를 차단합니다.
세밀한 제어	사전 정의된 카테고리나 카테고리의 조합을 사용하여 콘텐츠를 차단합니다. 필터링은 학교 수업 시간이나 회사 업무 시간과 같이 특정한 시간별로 예약할 수 있고, 개별 사용자나 그룹에 적용할 수 있습니다.
웹 캐싱	SonicWall 방화벽에 로컬로 캐시되는 URL 평점으로, 자주 방문하는 사이트에 다시 액세스하면 몇 초 내에 응답을 받을 수 있도록 합니다.

안티 바이러스와 안티 스파이웨어 필수 정책[1]	
기능	설명
다중 계층 보호	방화벽 기능을 경계 지점의 첫 번째 방어 계층으로 활용하고, 엔드 포인트 보호 기능과 결합하여 랩톱, 썸 드라이브와 기타 보호되지 않는 시스템을 통해 네트워크에 들어오는 바이러스를 차단합니다.
자동화된 시행 옵션	네트워크에 액세스하는 모든 컴퓨터에 가장 최신 버전의 안티 바이러스와 안티 스파이웨어 시그니처가 설치되고 활성화되도록 하여 데스크톱 안티 바이러스와 안티 스파이웨어 관리에 관련된 비용이 발생하지 않도록 합니다.
자동화된 배포와 설치 옵션	안티 바이러스와 안티 스파이웨어 클라이언트의 컴퓨터별 배포와 설치를 네트워크를 통해 자동으로 수행하여 관리 업무를 최소화합니다.
상시 실행, 자동 바이러스 방지	자주 업데이트되는 안티 바이러스와 안티 스파이웨어 기능은 최종 사용자의 생산성을 높이고 보안 관리 업무를 줄이기 위해, 사용자가 신경을 쓸 필요가 없도록 모든 데스크톱과 파일 서버에 투명하게 적용됩니다.
차세대 안티 바이러스	Capture 클라이언트는 AI(인공 지능) 엔진을 사용하여 위협이 실행되기 전에 파악하고, 감염될 경우 이전에 감염되지 않은 상태로 롤백합니다.
스파이웨어 방지	강력한 스파이웨어 방지 기능은 스파이웨어가 기밀 데이터를 전송하기 전에 데스크톱과 랩톱에 설치되는 스파이웨어 프로그램을 검사하여 차단함으로써 뛰어난 데스크톱 보안과 성능을 이룰 수 있도록 합니다.

[1] *추가 구독이 필요합니다.*

기능 요약

방화벽

- 상태 보존형 패킷 검사
- RFDPI(Reassembly-Free Deep Packet Inspection)
- DDoS 공격 방어 (UDP/ICMP/SYN 플러드)
- IPv4/IPv6 지원
- 원격 액세스를 위한 생체 인증
- DNS 프록시
- REST API

SSL/SSH 암호 해독과 검사[2]

- TLS/SSL/SSH에 대한 딥 패킷 검사
- 개체, 그룹 또는 호스트 이름의 포함/제외
- SSL 제어

Capture 지능형 위협 방지[2]

- 클라우드 기반 다중 엔진 분석
- 가상화된 샌드박싱
- 하이퍼바이저 수준 분석
- 전체 시스템 에뮬레이션
- 광범위한 파일 형식 검사
- 자동 및 수동 제출
- 실시간 위협 인텔리전스 업데이트
- 판결까지 차단
- Capture 클라이언트

침입 방지[2]

- 시그니처 기반 검사
- 자동 시그니처 업데이트
- 양방향 검사 엔진
- 세부적인 IPS 규칙 집합
- GeoIP 시행
- 동적 목록을 사용한 봇넷 필터링
- 정규식 일치

안티 맬웨어[2]

- 스트림 기반 맬웨어 검사
- 게이트웨이 안티 바이러스
- 게이트웨이 안티 스파이웨어
- 양방향 검사
- 파일 크기 제한 없음
- 클라우드 맬웨어 데이터베이스

애플리케이션 파악[2]

- 애플리케이션 제어
- 애플리케이션 트래픽 시각화
- 애플리케이션 구성 요소 차단
- 애플리케이션 대역폭 관리
- 맞춤형 애플리케이션 시그니처 만들기
- 데이터 유출 방지
- NetFlow/IPFIX를 통한 애플리케이션 보고
- 사용자 활동 추적(SSO)
- 포괄적인 애플리케이션 시그니처 데이터베이스

웹 콘텐츠 필터링[2]

- URL 필터링
- 프록시 회피
- 키워드 차단
- HTTP 헤더 삽입
- 대역폭 관리 CFS 범주
- 앱 제어 기능을 갖춘 통합 정책 모델
- 콘텐츠 필터링 클라이언트

VPN

- 자동 프로비저닝 VPN
- 사이트 간 연결을위한 IPSec VPN
- SSL VPN과 IPSEC 클라이언트 원격 액세스
- 여분의 VPN 게이트웨이
- iOS, Mac OS X, Windows, Chrome, Android, Kindle Fire를 위한 모바일 연결
- 경로 기반 VPN(OSPF, RIP, BGP)

네트워킹

- LACP를 사용한 동적 LAG
- PortShield
- 점보 프레임
- 경로 MTU 검색
- 향상된 로깅
- VLAN 트렁킹
- 포트 미러링
- 2계층 QoS
- 포트 보안
- 동적 라우팅(RIP/OSPF/BGP)
- SonicWall 무선 컨트롤러
- 정책 기반 라우팅(ToS/메트릭 및 ECMP)
- NAT
- DHCP 서버
- 대역폭 관리
- 링크 집선(정적/동적)
- 포트 여분
- A/P 고가용성, 상태 동기화
- A/A 클러스터링
- 인바운드/아웃바운드 부하 분산
- L2 브리지, 와이어/가상 모드, 탭 모드, NAT 모드
- 3G/4G WAN 장애 조치(SuperMassive 9800에는 없음)
- 비대칭 라우팅
- CAC(일반 액세스 카드) 지원

무선

- WIDS/WIPS
- RF 스펙트럼 분석
- 비인증 AP 방지
- 빠른 로밍(802.11k/r/v)
- 평면도/토폴로지 뷰
- 대역 조향
- 빔포밍
- 에어타임 페어니스
- MiFi 확장기
- 게스트 주기적 할당량
- LHM 게스트 포털

VoIP

- 세밀한 QoS 제어
- 대역폭 관리
- VoIP 트래픽용 DPI
- H.323 게이트키퍼와 SIP 프록시 지원

관리와 모니터링

- GMS, 웹, UI, CLI, REST API, SNMPv2/v3
- 로깅
- Netflow/IPFix 내보내기
- 클라우드 기반 구성 백업
- BlueCoat 보안 분석 플랫폼
- SonicWall 액세스 포인트 관리
- Dell N-시리즈와 X-시리즈 스위치 관리[1]

[1] SuperMassive 9800에서는 지원되지 않습니다.
[2] 추가 구독이 필요합니다.

SONICWALL®

SuperMassive 9000 시리즈 시스템 사양

방화벽 일반	9200	9400	9600	9800
운영 체제	SonicOS			
보안 프로세싱 코어	24	32		64
인터페이스	4개의 10GbE SFP+, 8개의 1GbE SFP, 8개의 1GbE, 1GbE 관리, 1개 콘솔			4개의 10GbE SFP+, 12개의 1GbE SFP, 8개의 1GbE, 1GbE 관리, 1개 콘솔
메모리(RAM)	8GB	16GB	32GB	64GB
스토리지	플래시			2개의 80GB SSD, 플래시
확장	1개의 확장 슬롯(뒷면)*, SD 카드*			
관리	CLI, SSH, GUI, GMS			
SSO 사용자	80,000	90,000	100,000	110,000
지원하는 최대 액세스 포인트	128			-
로깅	분석기, 로컬 로드, Syslog			
고가용성	액티브/패시브와 상태 동기화, 액티브/액티브 DPI와 상태 동기화			
방화벽/VPN 성능	**9200**	**9400**	**9600**	**9800**
방화벽 검사 처리량[1]	15Gbps	20Gbps	20Gbps	31.8Gbps
위협 방지 처리량[2]	3Gbps	4.4Gbps	4.5Gbps	10.5Gbps
애플리케이션 검사 처리량[2]	5Gbps	10Gbps	11.5Gbps	23Gbps
IPS 처리량[2]	5Gbps	10Gbps	11.5Gbps	21.3Gbps
안티 맬웨어 검사 처리량[1]	3.5Gbps	4.5Gbps	5.0Gbps	11Gbps
IMIX 처리량	4.4Gbps	5.5Gbps	5.5Gbps	7.3Gbps
SSL 검사와 암호 해독 처리량(DPI SSL)[2]	1.0Gbps	2.0Gbps	2.0Gbps	3.5Gbps
VPN 처리량[3]	5Gbps	10Gbps	11.5Gbps	14.3Gbps
초당 연결	100,000/초	130,000/초	130,000/초	229,000/초
최대 연결(SPI)	5.0M	7.5M	10.0M	20.0M
최대 연결(DPI)	1.5M	1.5M	2.0M	8.0M
DPI SSL 연결*(최대)	8,000(15,500[6])	10,000(17,500[6])	12,000(22,500[6])	400,000
VPN	**9200**	**9400**	**9600**	**9800**
사이트 간 VPN 터널		10,000		25,000
IPSec VPN 클라이언트(최대)	2,000(4,000)	2,000(6,000)	2,000(10,000)	
SSL VPN NetExtender 클라이언트(최대)	2(3,000)	2(3,000)	50(3,000)	50(3,000)
암호화/인증	DES, 3DES, AES (128, 192, 256비트)/MD5, SHA-1, Suite B, CAC(일반 액세스 카드)			
키 교환	Diffie Hellman Groups 1, 2, 5, 14v			
경로 기반 VPN	RIP, OSPF			
네트워킹	**9200**	**9400**	**9600**	**9800**
IP 주소 할당	고정, DHCP, PPPoE, L2TP, PPTP 클라이언트, 내부 DHCP 서버, DHCP 릴레이[4]			
NAT 모드	일대일, 다대일, 일대다, 유연한 NAT(중첩 IP), PAT, 투명 모드			
VLAN 인터페이스	512			
라우팅 프로토콜	BGP, OSPF, RIPv1/v2, 고정 라우팅, 정책 기반 라이팅, 멀티캐스트			
QoS	대역폭 우선, 최대 대역폭, 대역폭 보장, DSCP 마킹, 802.1p			
인증	LDAP(다중 도메인), XAUTH/RADIUS, SSO, Novell, 내부 사용자 데이터베이스, 터미널 서비스[5], Citrix[5]			
VoIP	전체 H323-v1-5, SIP			
표준	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
인증	UC APL[4], ICSA 엔터프라이즈 방화벽, IPV6 Phase 2, VPNC, VPAT, FIPS 140-2[4], 공통 기준 NDPP[4], ICSA 안티 바이러스[4]			
하드웨어	**9200**	**9400**	**9600**	**9800**
전원 공급 장치	듀얼, 여분, 핫스왑 가능, 300 W			듀얼, 여분, 핫스왑 가능, 500 W
팬	듀얼, 여분, 핫스왑 가능			
디스플레이	전면 LED 디스플레이			
입력 전력	100-240VAC, 50-60Hz			
최대 소비 전력(W)	200			350
25°C에서 시간당 MTBF	188,719	187,702	186,451	126,144
@25°C에서 연간 MTBF	21.53	21.43	21.28	14.40
폼 팩터	1U 랙 마운트 가능			2U 랙 마운트 가능
치수	43.3x48.5x4.5cm(17x19.1x1.75인치)			9x60x43cm(17x24x3.5인치)
무게	8.2kg(18.1파운드)			18.38 kg(40.5파운드)
WEEE 무게	10.4kg(23파운드)			22.4kg(49.5파운드)
배송 무게	13.3kg(29.3파운드)			29.64kg(65파운드)
주요 규정	FCC Class A, CE(EMC, LVD, RoHS), C-Tick, VCCI Class A, MSIP/KCC Class A, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH, ANATEL, BSMI, CU			
환경	섭씨 15-40도			
습도	10-90% 비응축			

*[1] 테스팅 방법론: 최대 성능은 RFC 2544(방화벽용)를 기반으로 합니다. 실제 성능은 네트워크 상태와 활성화된 서비스에 따라 달라질 수 있습니다. [2] 위협 방지/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. 위협 방지 처리량은 게이트웨이 AV, 안티 스파이웨어, IPS, 애플리케이션 제어를 활성화한 상태에서 측정되었습니다. [3] VPN 처리량은 1280바이트 패킷에서 UDP 트래픽으로 측정되었습니다. [4] SuperMassive 9200, 9400, 9600에 적용됩니다. SuperMassive 9800 UC APL 인증은 대기 중입니다. [5] SonicOS 6.1과 6.2에서 지원됩니다. [6]DPI 연결이 125,000번 감소하면 이용 가능한 DPI SSL 연결이 750 늘어납니다. *나중에 사용됩니다. 모든 사양과 기능, 이용 가능성은 변경될 수 있습니다.*

SONICWALL®

SuperMassive 9000 시리즈 주문 정보

제품	SKU
SuperMassive 9800 Total Secure Advance Edition(1년)	01-SSC-0312
SuperMassive 9600 Total Secure Advance Edition(3년)	02-SSC-0410
SuperMassive 9400 Total Secure Advance Edition(3년)	02-SSC-0409
SuperMassive 9200 Total Secure Advance Edition(3년)	02-SSC-0408
SuperMassive 9200 지원과 보안 구독	**SKU**
Advanced Gateway Security Suite – SuperMassive 9200용 Capture ATP, 위협 방지, 콘텐츠 필터링, 연중무휴 24시간 지원(1년)	01-SSC-1570
SuperMassive 9200용 Capture Advanced Threat Protection(1년)	01-SSC-1575
Comprehensive Gateway Security Suite: 9200용 애플리케이션 인텔리전스, 위협 방지, 콘텐츠 필터링, 지원(1년)	01-SSC-4172
SuperMassive 9200용 위협 방지, 안티 맬웨어, CloudAV, 애플리케이션 인텔리전스, 제어와 시각화(1년)	01-SSC-4202
9200용 Content Filtering Premium Business Edition(1년)	01-SSC-4184
SuperMassive 9200용 Platinum Support(1년)	01-SSC-4178
SuperMassive 9400 지원과 보안 구독	**SKU**
Advanced Gateway Security Suite – SuperMassive 9400용 Capture ATP, 위협 방지, 콘텐츠 필터링, 연중무휴 24시간 지원(1년)	01-SSC-1580
SuperMassive 9400용 Capture Advanced Threat Protection(1년)	01-SSC-1585
Comprehensive Gateway Security Suite: 9400용 애플리케이션 인텔리전스, 위협 방지, 콘텐츠 필터링, 지원(1년)	01-SSC-4136
SuperMassive 9400용 위협 방지, 안티 맬웨어, CloudAV, 애플리케이션 인텔리전스, 제어와 시각화(1년)	01-SSC-4166
9400용 Content Filtering Premium Business Edition(1년)	01-SSC-4148
SuperMassive 9400용 Platinum Support(1년)	01-SSC-4142
SuperMassive 9600 지원과 보안 구독	**SKU**
Advanced Gateway Security Suite – SuperMassive 9600용 Capture ATP, 위협 방지, 콘텐츠 필터링, 연중무휴 24시간 지원(1년)	01-SSC-1590
SuperMassive 9600용 Capture Advanced Threat Protection(1년)	01-SSC-1595
Comprehensive Gateway Security Suite: 9600용 애플리케이션 인텔리전스, 위협 방지, 콘텐츠 필터링, 지원(1년)	01-SSC-4100
SuperMassive 9600용 위협 방지, 안티 맬웨어, CloudAV, 애플리케이션 인텔리전스, 제어와 시각화(1년)	01-SSC-4130
9600용 Content Filtering Premium Business Edition(1년)	01-SSC-4112
SuperMassive 9600용 Platinum Support(1년)	01-SSC-4106
SuperMassive 9800 지원과 보안 구독	**SKU**
Advanced Gateway Security Suite: SuperMassive 9800용 Capture ATP, 위협 방지, 콘텐츠 필터링, 연중무휴 24시간 지원(1년)	01-SSC-1183
SuperMassive 9800용 Capture Advanced Threat Protection(1년)	01-SSC-1188
Comprehensive Gateway Security Suite: 9800용 애플리케이션 인텔리전스, 위협 방지, 콘텐츠 필터링, 지원(1년)	01-SSC-0809
SuperMassive 9800용 위협 방지, 안티 맬웨어, CloudAV, 애플리케이션 인텔리전스, 제어와 시각화(1년)	01-SSC-0827
9800용 Content Filtering Premium Business Edition(1년)	01-SSC-0821
SuperMassive 9800용 Gold 연중무휴 24시간 지원(1년)	01-SSC-0815
모듈과 액세서리*	**SKU**
SonicWall SuperMassive 9800 시리즈 시스템 팬 FRU	01-SSC-0204
SonicWall SuperMassive 9800 시리즈 전원 공급 장치 AC FRU	01-SSC-0203
SonicWall SuperMassive 9000 시리즈 시스템 팬 FRU	01-SSC-3876
SonicWall SuperMassive 9000 시리즈 전원 공급 장치 AC FRU	01-SSC-3874
10GBASE-SR SFP+ 짧은 도달 거리 모듈	01-SSC-9785
10GBASE-LR SFP+ 긴 도달 거리 모듈	01-SSC-9786
1000BASE-SX SFP 단거리 모듈	01-SSC-9789
1000BASE-LX SFP 장거리 모듈	01-SSC-9790
1000BASE-T SFP 쿠퍼 모듈	01-SSC-9791
관리와 보고	**SKU**
SonicWall GMS 10개 노드 소프트웨어 라이센스	01-SSC-3363
SonicWall GMS E-Class 10개 노드에 대한 연중무휴 24시간 소프트웨어 지원(1년)	01-SSC-6514
SonicWall Scrutinizer 가상 어플라이언스, 최대 5개 노드를 위한 흐름 분석 모듈 소프트웨어 라이센스(1년의 연중무휴 24시간 소프트웨어 지원 포함)	01-SSC-3443
SonicWall Scrutinizer, 최대 5개 노드를 위한 흐름 분석 모듈 소프트웨어 라이센스(1년의 연중무휴 24시간 소프트웨어 지원 포함)	01-SSC-4002
SonicWall Scrutinizer, 최대 5개 노드를 위한 고급 보고 모듈 소프트웨어 라이센스(1년의 연중무휴 24시간 소프트웨어 지원 포함)	01-SSC-3773

**지원되는 SFP와 SFP+ 모듈의 전체 목록은 SonicWall SE에 문의하세요.*

SONICWALL®

회사 소개

SonicWall은 전 세계 중소기업과 대기업을 보호하면서 25년 넘게 사이버 범죄와 싸우고 있습니다. 우리의 제품과 파트너 제품의 조합으로 150개 이상의 국가에서 50만 개 이상의 기업이 각자의 요구 사항에 맞는 실시간 사이버 방어 솔루션을 마련하여 안심하고 더 많은 업무를 하고 있습니다.

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

Datasheet-SuperMassive-US-KJ-MKTG4043