

SONICWALL 제품군: 개요



차세대 방화벽

고급형: NSsp 15700

대형 분산 기업, 데이터 센터 및 MSP를 위해 설계된 다중 인스턴스 방화벽으로 고속 보호, 고밀도 포트 및 통합 정책을 통한 진정한 테넌트 격리 제공



중급형: NSa Series

NSa 9650/9450/9250/
6650/5650/4650/3650/2650

중소규모 네트워크, 지사 및 분산되어 있는 대기업을 위한 제품으로서 업계 검증을 받은 보안 효과 및 성능



기본형: TZ Series

TZ670/TZ570/TZ400/TZ350

중소기업과 SD Branch 망에 대한 구성을 위한 통합된 위협 방지 SD-WAN 플랫폼



Virtual: NSv Series

공용 및 사설 클라우드 인프라의 모든 중요한 요소를 보호하기 위한 합리적인 라이선스 모델을 갖춘 가상 방화벽



무선 보안

SonicWave Series

SonicWave 432e/432i/432o/
231c/224w/231o

클라우드나 방화벽을 통해 관리되는 차세대 무선랜 솔루션



보안 모바일 액세스

SMA Series SMA 8200v/7210/
6210/500v/410/210

정책적으로 관리되는 네트워크와 클라우드 리소스 보안 액세스



액세스 스위치

SWS12-8/SWS12-8POE/SWS12-10FPOE/
SWS14-24/SWS14-24FPOE/SWS14-48/
SWS14-48FPOE

SMB 및 SD Branch 구성과 차세대 보안 연결을 위한 지능형 스위치 제공



이메일 보안 시리즈

ESA 9000/7000/5000/

VM 소프트웨어/클라우드 서비스

지능형 이메일 위협을 방지하는 다중 보호 솔루션



관리 및 분석

Capture Security Center

글로벌 관리 시스템 (GMS)

네트워크 보안 관리자

네트워크에 대해 알고 통제하는 것이 힘입니다



캡처 보안 어플라이언스 (CSa)

온프레미스 파일 검사 및 맬웨어 예방.



캡처 클라이언트

통합된 클라이언트 플랫폼으로서 지능형 맬웨어 방지, 샌드박스, 애플리케이션 취약성 인텔리전스 및 감염 시 롤백 등 여러 엔드포인트 보호 기능을 제공



클라우드 앱 보안

클라우드에서 규정을 준수하면서 지능형 위협으로부터 이메일과 데이터, 사용자 자격증명을 보호하고, Office 365와 G Suite과 같은 SaaS 애플리케이션을 위한 차세대 보안을 제공하는 CASB 솔루션

차세대 방화벽 구독 서비스

Essential Protection Services Suite 알려져 있거나 알려져 있지 않은 위협으로부터 보호하기 위해 필요한 모든 필수 보안 서비스를 제공합니다.

여기에는 RTDMI 기술을 사용한 캡처 고급 위협 보호, 게이트웨이 안티 바이러스, 침입 방지 및 애플리케이션 제어, 콘텐츠 필터링 서비스, 포괄적인 스팸 방지 서비스, 네트워크 가시성 및 24x7 지원이 포함됩니다.

Advanced Gateway Security Suite (AGSS) 가장 지능적이고 알려지지 않은 위협으로부터 보호하기 위해 모든 물리적 및 가상 SonicWall 방화벽에 대한 추가 서비스로 제공됩니다.

Advanced Gateway Security Suite (AGSS)에 포함되어 있으며 TotalSecure Advanced Edition의 차세대 방화벽과 결합된 서비스

- Capture Advanced Threat Protection (ATP) 멀티 엔진 클라우드 기반 샌드박스
- 게이트웨이 바이러스 방지 및 스파이웨어 방지
- 침입 방지 서비스
- 애플리케이션 제어
- 콘텐츠/웹 필터링 서비스
- 매일 24시간 지원

서비스로서의 보안 (SECaaS)

턴키(turnkey) 솔루션으로 네트워크 보안을 아웃소싱하세요

관련 질문

차세대 방화벽

- 멀티 기가비트 성능 요구로 인한 대역폭 증가를 따라갈 수 있습니까?
- 현재 방화벽은 다가오는 위협의 속도에 따라 위협 검사를 수행할 수 있습니까?
- 성능 요건 기준은 무엇입니까?
- 방화벽 뒤의 사용자/네트워크 수는 총 몇입니까?
- 최대 세션/연결 수는 얼마나 됩니까?
- 얼마나 많은 원격 사이트와 사용자가 방화벽에 연결됩니까?
- 귀사의 보안 관리 효과를 어떻게 측정하고 계십니까?
- 어떤 종류의 인터넷 연결을 사용하십니까? 속도는 어떻습니까?
- 제로데이 공격과 같은 새로운 위협을 방지하기 위해 무엇을 하고 있습니까?
- 귀사의 샌드박스는 메모리 안에 숨겨진 위협을 탐지하고 차단할 수 있습니까?
- 귀하의 샌드박스에는 몇 개의 엔진이 포함되어 있습니까?
- 귀하의 샌드박스가 분석을 끝낼때까지 파일을 사용자에게 보내지 않게 구성할 수 있습니까?
- 귀사의 방화벽이 HTTPS 트래픽을 검사할 수 있는지 확인해 보셨습니까?
- HTTPS 트래픽 검사 때문에 네트워크 서비스가 중단된 적이 있었습니까?
- 귀사의 가상 방화벽이 물리적 방화벽 만큼 보호하니까?
- 귀사의 공용 또는 사설 클라우드 환경 보안을 얼마나 안전하게 지키고 있습니까?
- 가상 네트워크에서 적절한 보안 구역설정 및 세분화를 실행할 수 있습니까?
- 귀사의 가상 트래픽을 완벽하게 파악하고 제어할 수 있습니까?
- 보안 사설 네트워킹을 위해 MPLS를 SD-WAN으로 교체하여 비용을 줄이는 것을 고려하고 계십니까?

캡처 클라이언트

- 귀하의 엔드포인트를 랜섬웨어와 암호화된 위협으로부터 일관성 있게 보호하고 싶습니까?
- 모든 엔드포인트에서 정책 준수와 라이선스 관리를 얼마나 쉽게 할 수 있습니까?
- 엔드포인트의 파악과 보안 태세 관리에 어려움을 겪고 있습니까?
- 귀하의 엔드포인트 보안 제품이 샌드박스 환경에 연결되어 있습니까?
- 엔드포인트에 설치된 애플리케이션을 분류할 수 있고, 그 속에 얼마나 많은 취약점이 있는지 아십니까?
- 현재 이용 중인 솔루션이 지속적으로 귀하의 시스템 안정성을 모니터링합니까?
- 랜섬웨어로 인한 손상을 이전에 알던 무결 상태로 복원시킬 수 있습니까?
- 알 수 없는 잠재적으로 감염된 기기가 엔드포인트에 연결되지 않도록 차단할 능력을 가지고 계십니까?

클라우드 앱 보안

- O365 또는 G Suite를 사용하십니까?
- O365/G Suite의 보안을 위해 Proofpoint 또는 Mimecast를 사용하십니까?
- 내부 O365 이메일을 스캔하고 있습니까?
- 귀사는 몇 개의 승인된 SaaS 앱을 사용하고 계십니까?
- SaaS 애플리케이션에 저장된 데이터에 대해 규정준수를 시행하는 데 어려움을 겪고 계십니까?
- 사용자의 자격증명이 위협한 상태에 있는지 어떻게 알 수 있습니까?
- 누가 언제 어디서 데이터에 접근하고 있는지 파악할 수 있습니까? (BYOD)

딥 메모리 검사

특히 출원 중인 기술인 SonicWall Real-Time Deep Memory Inspection(RTDMI™) 엔진이 실시간 딥 메모리 검사를 하여, 일반 대중 대상의 알려지지 않은 맬웨어를 사전에 탐지하여 차단합니다. 이 엔진은 현재 SonicWall Capture Advanced Threat Protection(ATP) 클라우드 샌드박스 서비스와 함께 이용 가능하며, 미래의 유출 사고를 비롯하여 가장 교묘한 현대의 위협마저도 식별하여 방지합니다.

무선 보안

- 귀사의 직원/협력사/고객이 느린 Wi-Fi 성능에 대해 불평합니까?
- 동시 사용하는 무선 사용자의 최대 수가 얼마나 됩니까?
- 네트워크에 안전한 무선 솔루션을 추가하는 비용에 대해 걱정이 되십니까?
- 802.11ac Wave 2 무선 표준에 대해 얼마나 잘 알고 계십니까?
- 액세스 포인트 관리 - 클라우드 vs 방화벽 관리를 위해 융통성이 필요하십니까?
- WiFi 네트워크를 효과적으로 계획하셨습니까?
- AP를 방화벽으로부터 분리해야 합니까?
- WiFi 네트워크에 보안 기능을 강화하는 것에 대해 걱정이 있습니까?
- 귀하에게는 게스트 서비스가 중요합니까?
- 게스트 온보딩을 위한 게스트 로그인 포털을 맞춤화할 필요가 있습니까?

액세스 스위치

- PoE 지원 장비에 전원을 공급하려면 기가비트 지원 액세스 스위치가 필요하니까?
- 통합된 가시성과 관리 기능을 갖춘 통합 보안 구성이 중요하니까?
- SonicWall 에코시스템과 함께 작동하는 타사 스위치에 대한 솔루션 문제가 있습니까?

보안 모바일 액세스

- 귀사의 현재 원격지 근무자에 대한 보안 전략은 무엇입니까?
- 제로 트러스트 네트워크 접근 방법을 이용하는 것에 대한 귀하의 생각은 어떻습니까?
- 귀사는 사내와 클라우드에서 호스팅되는 회사 자료와 애플리케이션에 대해 이용자에게 보안 접근을 제공하고 계십니까?
- 귀사의 네트워크에 접근하는 모든 이용자와 기기를 파악하고 계십니까?
- 업무상 대단히 중요한 웹 속성과 웹 서버를 현재 어떻게 보호하고 계십니까?

이메일 보안

- 랜섬웨어, 스피어 피싱 및 기업 이메일 침해와 같은 지능형 이메일 위협에 대해 걱정이 되십니까?
- 귀사의 현재 이메일 보안 솔루션은 Advanced Threat Protection 기능을 제공합니까?
- 비밀 정보가 담긴 이메일이 유출될까봐 걱정되십니까?
- GDPR, Sarbanes-Oxley, GLBA 또는 HIPAA와 같은 규정을 어떻게 준수하십니까?
- 클라이언트에게 관리형 이메일 보안 서비스를 제공하는 데 관심이 있습니까? (MSSP)

관리 및 분석

- 귀사의 보안 솔루션을 단일창 경험을 가진 하나의 공동 관리 플랫폼으로 통합함으로써 어떤 문제를 해결할 수 있었습니까?
- 보안 인포스 관리에서 어떤 경제적, 운영상의 어려움을 겪고 계십니까?
- PCI, HIPAA 및 GDPR과 같은 사이버 보안 규정을 준수하고 있음을 증명할 수 있다고 얼마나 자신하십니까?
- 속도와 정확성을 갖추고 위협과 위험을 더 잘 탐지하여 대응할 수 있다면 보안 태세가 어떻게 바뀌겠습니까?
- 귀사의 비즈니스에 대한 사이버 위협과 위험을 완전히 파악할 수 있다면 귀사와 지도부는 어떤 가치를 얻을 수 있었습니까?

자세한 정보는 sonicwall.com에서 확인하세요