SonicWall 제품군: 개요

차세대 방화벽

하이엔드: NS*sp* 시리즈
대형 분산 기업, 데이터 센터 및 MSSP에 적합하게 설계된 방화벽으로, 빠른 속도, 높은 포트 밀도 지원, 최대 100Gbps의 방화벽 검사 처리량을 자랑합니다.

중급형: NS*a* 시리즈
업계에서 검증받은 보안성과 더불어, 중규모 네트워크, 지사 사무실, 분산 기업에 적합한 성능을 지녔습니다.

기본형: TZ 시리즈
통합된 위협 보호 능력을 갖춘 SD-WAN 플랫폼으로, 소호 사무실, 중소기업, SD-Branch 배포에 적합합니다.

NS*v*

가상: NS*v* 시리즈
퍼블릭 및 프라이빗 클라우드 인프라의 모든 중요한 요소를 보호하기 위한 유연성 높은 라이선스 모델을 갖춘 가상 방화벽입니다.

SonicWall 방화벽은 DNS 및 평판 기반 콘텐츠 필터링으로 악성 웹사이트 및 애플리케이션을 차단하며, 평판 점수를 사용한 웹 콘텐츠 표시 정책의 방향을 제시해줍니다. 풍부한 감사 파일 용량, 네트워크 액세스 제어(NAC) 통합, 자동화된 업데이트로 사용 용이성이 높아졌습니다.

SonicWave 시리즈

지능형 보안, 성능, Wi-Fi 6 지원을 통한 뛰어난 확장성이 특징으로, SonicWall Wireless Network Manager 또는 Network Security Manager로 클라우드 및 방화벽을 통해 관리 가능합니다.

SMA 시리즈

네트워크와 클라우드 리소스에 간편하게 정책을 강제해 액세스 보안을 강화합니다.

SonicWall 스위치

지능적인 스위칭으로 중소기업 및 SD-Branch 배포의 차세대 보안 연결을 가능하게 해줍니다.

이메일 보안

ESA 시리즈
고도화된 이메일 위협으로부터 보호해주는 다중 보호 솔루션으로, 어플라이언스, VM, SaaS 폼 팩터로 제공됩니다.

Capture Security appliance (CS*a*)

온프레미스 파일 검사 및 맬웨어 방지가 특징입니다.

관리 및 분석

Network Security Manager
Wireless Network Manager
중앙 집중식으로 위험과 규정 준수를 관리합니다. 보고를 통해 트래픽과 위협에 대한 인사이트를 제공합니다. 워크플로 및 업데이트를 자동화합니다.

Capture Client

통합된 클라이언트 플랫폼으로, 지능형 맬웨어 방지, 샌드박싱, 애플리케이션 취약성 인텔리전스 및 감염 시 롤백 등 여러 엔드포인트 보호 기능을 제공합니다.

Cloud Edge Secure Access

AWS, Azure, Google 클라우드로의 사이트-투-사이트 및 하이브리드 클라우드 연결성을 위한 간편한 NaaS(Network-as-a-Service)를 제공하는 강력한 SaaS 애플리케이션입니다. 제로 트러스트와 최소 권한 보안 접근법을 하나의 통합된 오퍼링에 담았습니다.

클라우드 앱 보안

클라우드에서 규정을 준수하면서 지능형 위협으로부터 이메일과 데이터, 사용자 자격증명을 보호하고, Office 365와 G Suite과 같은 SaaS 애플리케이션을 위한 차세대 보안을 제공하는 클라우드 네이티브 솔루션입니다.

차세대 방화벽 구독 서비스

Threat Protection Service Suite는 네트워크를 위협으로부터 보호하는 데 필요한 기본적인 보안 서비스가 포함된 가장 비용 효율적인 번들입니다. TZ270/370/470에서만 사용 가능한 이 번들은 게이트웨이 바이러스 백신, 침입 방지 및 애플리케이션 컨트롤, 콘텐츠 필터링 서비스, 네트워크 가용성 및 연중무휴 지원이 포함됩니다.

Essential Protection Services Suite는 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 Protection Services Suite는 지능형 네트워크 보안을 제공합니다. 이 번들에는 7일 동안의 클라우드 기반 보고 및 클라우드 관리와 함께 에센셜 번들 서비스가 포함되어 있습니다.

자세한 정보: *sonicwall.com*

고객에게 할 만한 질문

차세대 방화벽

- 어떻게 악성 웹사이트 액세스를 방지하고 부적절한 콘텐츠가 표시되지 않도록 할 생각이십니까?
- DNS 및 콘텐츠 필터링에 다른 솔루션을 두고 있습니까?
- 기가비트 또는 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 총 몇입니까?
- 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 딥 메모리 안에 숨겨진 위협을 탐지하고 차단할 수 있습니까?
- 귀하의 샌드박스에는 몇 개의 엔진이 포함되어 있습니까?
- 귀하의 샌드박스가 공개되기 전에 게이트웨이에서 파일을 계속 보유할 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 튼튼합니까?
- 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?

Capture Client

- 귀하의 엔드포인트를 랜섬웨어와 암호화된 위협으로부터 일관성 있게 보호하고 싶으십니까?
- 모든 엔드포인트에서 정책 준수와 라이선스 관리를 얼마나 쉽게 할 수 있습니까?
- 엔드포인트의 파악과 보안 태세 관리에 어려움을 겪고 있습니까?
- 귀사의 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 건전성을 모니터링합니까?
- 랜섬웨어로 인한 손상을 이전에 알던 무결 상태로 복원시킬 수 있습니까?
- 얼마나 신속하게 테넌트에 정책을 추가하거나 변경하고 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 위험한 상태에 있는지 어떻게 알 수 있습니까?
- 누가 언제 어디에서 데이터에 접근하고 있는지 파악할 수 있습니까? (BYOD)

심층 메모리 검사

특허받은 기술인 SonicWall Real-Time Deep Memory Inspection(RTDMI™) 엔진이 실시간으로 메모리를 심층 검사하여, 대중에 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.

SonicWave 시리즈

- 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?
- 802.11ax 무선 표준에 대해 얼마나 잘 알고 계십니까?
- 여러 위치의 액세스 포인트 관리에 유연성이 필요하십니까?
- Wi-Fi 네트워크를 효과적으로 계획하셨습니까?
- AP를 방화벽으로부터 분리해야 합니까?
- Wi-Fi 네트워크에 보안 기능을 강화하는 것에 대해 걱정이 있습니까?
- 귀하에게는 게스트 서비스가 중요합니까?
- 게스트 온보딩을 위한 게스트 로그인 포털을 맞춤화할 필요가 있습니까?

SonicWall 스위치

- PoE 지원 장비에 전원을 공급하려면 기가비트 지원 액세스 스위치가 필요합니까?
- 통합된 가시성과 관리 기능을 갖춘 통합 보안 태세가 중요합니까?
- SonicWall 에코시스템과 함께 작동하는 타사 스위치에 대한 솔루션 문제가 있습니까?
- 방화벽에 묶이지 않은 스위치가 필요하십니까?

보안 모바일 액세스

- 귀사의 현재 원거리 인력 접근 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

- 어떻게 펌웨어를 제때 업데이트하십니까?
- 어떻게 조직 전체에 보안 정책을 강제 적용하십니까?
- 귀사의 보안 솔루션을 단일창 경험을 가진 하나의 공동 관리 플랫폼으로 통합함으로써 어떤 문제를 해결할 수 있겠습니까?
- 클라우드 콘솔을 사용하여 모든 위치의 방화벽, AP, 스위치를 중앙에서 모두 관리했을 때 어떤 운영상의 이점이 있으십니까?
- PCI, HIPPA 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 있겠습니까?
- 대시보드 한 곳에서 무선 및 스위치를 통합 관리할 필요가 있으십니까?

Cloud Edge Secure Access

- 민감한 데이터가 많이 있습니까? 권한이 너무 많은 사용자에 대한 걱정이 있습니까?
- 데이터 보호 및 정보 보안에 대한 규제가 강화되는 것에 대한 걱정이 있습니까?
- 직원 간 상호작용, 외부 비즈니스 파트너, 민감한 리소스를 통제할 필요가 있습니까?
- 얼마나 많은 지사 사무실을 두고 계십니까? 신입 직원을 얼마나 효율적으로 온보딩하십니까?
- 재택 사용자를 안전하게 온보딩하는 데 얼마나 걸리십니까?