

# Advanced Gateway Security Suite

하나의 통합 패키지로 네트워크 보안 완성

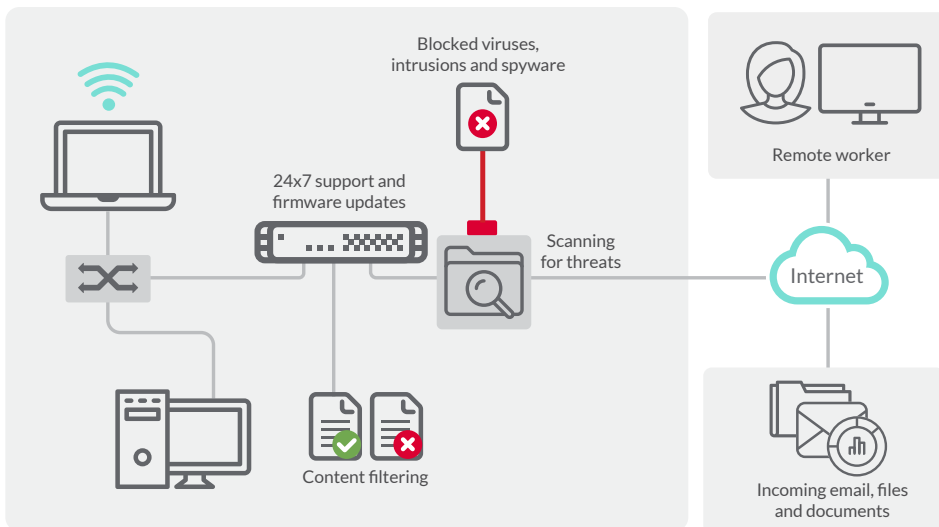
네트워크 보안을 이해하는 것은 복잡할 수 있지만, 알려진 악성 위협과 알려지지 않은 악성 위협으로부터 네트워크를 보호하는 일은 복잡해서는 안 됩니다. SonicWall AGSS(Advanced Gateway Security Suite)는 보호에 필요한 모든 네트워크 보안 서비스를 편리하고 경제적인 패키지로 묶어, 방대한 애드온 보안 서비스를 선택하는 복잡한 일을 할 필요가 없도록 했습니다.

NSsp, NSa, TZ, NSv 시리즈를 포함한 모든 물리적 방화벽과 가상 방화벽에 사용할 수 있는 SonicWall AGSS는 제로 데이 공격, 바이러스, 침입, 봇넷, 스파이웨어, 트로이 목마, 웜과 기타 악성 공격으로부터 네트워크를 안전하게 지킵니다. 클라우드 기반 다중 계층 샌드 박스의 게이트웨이에서 의심스러운 파일을 검사하여 알 수 없는 위협으로부터 네트워크를 안전하게 보호합니다. 새로운 위협이 파악되면

소프트웨어 공급 업체가 소프트웨어에 패치를 적용하기도 전에 SonicWall 방화벽과 캡처 클라우드 데이터베이스가 이러한 위협으로부터 보호하는 시그니처로 자동 업데이트됩니다. 모든 SonicWall 방화벽 내에는 특허 출원된 Reassembly-Free Deep Packet Inspection® 엔진이 있어 여러 애플리케이션 유형과 프로토콜의 트래픽을 검사, 네트워크가 항상 내부와 외부 공격에 안전하고 애플리케이션 취약성을 가지지 않도록 합니다. 또한 SonicWall 솔루션은 포괄적인 콘텐츠 필터링을 통해 인터넷 사용 정책을 시행하고, 내부에서 부적합하거나 비생산적이거나 불법일 수 있는 웹 콘텐츠에 액세스할 수 없도록 제어하는 도구를 제공합니다. 마지막으로 이 강력한 서비스 번들에는 24시간 기술 지원과 중요한 펌웨어 업데이트, 하드웨어 교체가 포함되어 있습니다.

## 장점:

- 완전한 네트워크 보안 솔루션
- ICSA 인증을 받은 게이트웨이 안티 바이러스, 안티 스파이웨어 보호
- 첨단 IPS 기술
- 애플리케이션 인텔리전스와 제어
- 콘텐츠 필터링
- 펌웨어 업데이트와 하드웨어 교체가 포함된 연중무휴 24시간 지원
- SonicWall RTDMI를 지원하는 다중 엔진 네트워크 샌드박스
- 클라우드 기반의 단일 창을 통한 관리



## Advanced Gateway Security Suite

NSsp 12800(1년)  
01-SSC-6591

NSsp 12400(1년)  
01-SSC-6588

NSa 9650(1년)  
01-SSC-2036

NSa 9450(1년)  
01-SSC-0414

NSa 9250(1년)  
01-SSC-0038

NSa 6650(1년)  
01-SSC-8761

NSa 5650(1년)  
01-SSC-3674

NSa 4650(1년)  
01-SSC-3493

NSa 3650(1년)  
01-SSC-3451

NSa 2650(1년)  
01-SSC-1783

TZ600 시리즈(1년)  
01-SSC-1460

TZ500 시리즈(1년)  
01-SSC-1450

TZ400 시리즈(1년)  
01-SSC-1440

TZ300 시리즈(1년)  
01-SSC-1430

NSv 1600(1년) 01-SSC-5787

NSv 800(1년) 01-SSC-5737

NSv 400(1년) 01-SSC-5681

NSv 300(1년) 01-SSC-5584

NSv 200(1년) 01-SSC-5306

NSv 100(1년) 01-SSC-5219

NSv 50(1년) 01-SSC-5194

NSv 25(1년) 01-SSC-5165

NSv 10(1년) 01-SSC-5008

다년 SKU도 이용할 수 있습니다.  
SonicWall 방화벽 제품군의  
전체 SKU를 보려면  
[www.sonicwall.com](http://www.sonicwall.com)을  
방문하세요.

SonicWALL Advanced Gateway Security Suite에는 다음이 포함됩니다.

- 게이트웨이 안티 바이러스, 안티 스파이웨어, 침입 방지 및 애플리케이션 인텔리전스, 제어 서비스 구독
- 콘텐츠 필터링 서비스 구독
- 연중무휴 24시간 지원 구독
- Capture ATP(Advanced Threat Protection) 서비스 구독
- Capture Security Center Lite 구독

### 기능과 장점

이 솔루션은 랜섬웨어, 바이러스, 스파이웨어, 웜, 트로이 목마, 애드웨어, 키로거, MMC(악성 모바일 코드)와 기타 위험한 애플리케이션, 웹 콘텐츠와 같은 위협으로부터 포괄적으로 보호하는 데 필요한 모든 것을 통합한 완전한 네트워크 보안 솔루션입니다.

Capture ATP(Advanced Threat Protection) 서비스는 게이트웨이에서 알려지지 않은 제로 데이 공격을 막고 자동화된 완화 조치를 하는 클라우드 기반의 다중 엔진 솔루션으로, 고급 위협 탐지와 샌드박싱을 혁신합니다.

Capture ATP는 SonicWall의 RTDMI(Real-Time Deep Memory Inspection) 기술을 통해 악의적인 행동을 하지 않거나 암호화를 통해 무기를 숨긴 맬웨어도 탐지하여 차단합니다. RTDMI 엔진은 맬웨어가 자신의 무기를 메모리에 노출하도록 함으로써 대량 판매, 제로 데이 위협, 알려지지 않은 맬웨어를 사전에 탐지하고 차단하며, 실시간 메모리 기반 검사 기술을 정확하게 활용합니다.

ICSA 인증을 받은 게이트웨이 안티 바이러스와 안티 스파이웨어 보호 기능은 네트워크 기반 안티 맬웨어 프로그램과 수천만 개의 맬웨어 시그니처가 포함된 클라우드 데이터베이스를 결합하여 교묘한 최신 위협에 대한 심층적인 보호 서비스를 제공합니다.

첨단 IPS 기술은 모든 네트워크 트래픽에서 악의적이거나 비정상적인 패턴을 검색하여

웜, 트로이 목마, 소프트웨어 취약성, 기타 침입으로부터 보호함으로써 네트워크 안정성과 성능을 향상시킵니다.

애플리케이션 인텔리전스와 제어 기능은 세부적인 애플리케이션별 정책의 세트와, 애플리케이션 분류와 정책 시행을 통해 관리자가 업무용 애플리케이션과 업무용이 아닌 관련 애플리케이션 모두를 제어하고 관리하는 데 유용합니다.

콘텐츠 필터링은 인터넷 사용 정책을 시행하고, 유해하거나 비생산적인 웹 콘텐츠에 액세스하지 못하도록 제어하여 안전, 보안, 생산성 문제를 해결합니다.

펌웨어 업데이트와 하드웨어 교체가 포함된 연중무휴 24시간 지원은 중요한 펌웨어 업데이트와 업그레이드, 최고의 기술 지원, 시기 적절한 하드웨어 교체와 전자 셀프 서비스 도구에 액세스할 수 있도록 하여 기업과 SonicWALL의 투자를 보호합니다.

Capture Security Center Lite를 사용하면 클라우드에 있는 하나의 창으로 SonicWALL 배포 환경을 관리하고 방화벽 기본 설정을 백업/복원할 수 있습니다.

### AGSS 서비스 개요

다중 엔진 샌드박스, 게이트웨이 안티 바이러스, 안티 스파이웨어, 침입 방지, 애플리케이션 인텔리전스 및 제어 서비스

- 바이러스, 웜, 트로이 목마와 기타 인터넷 위협을 실시간으로 검사하는 실시간 게이트웨이 안티 바이러스 엔진입니다.
- 동적 스파이웨어 방지는 악성 스파이웨어 설치를 차단하고 기존 스파이웨어 통신을 중단시킵니다.
- 강력한 침입 방지 기능은 웜, 트로이 목마와 기타 악성 코드와 같은 다양한 네트워크 기반 위협으로부터 보호합니다.
- 애플리케이션 인텔리전스와 제어 기능은 애플리케이션 분류와 정책 적용 서비스를 제공합니다.

- 시그니처 데이터베이스는 지속적인 위협 방지를 위해 동적으로 업데이트됩니다.
- 다중 엔진 샌드박스의 특징은 RTDMI 기능으로, 제로 데이 공격, 랜섬웨어와 같은 위협을 방지합니다.

#### Capture ATP(Capture Advanced Threat Protection)

- 제로 데이 공격이 네트워크에 진입하기 전에 차단합니다.
- 다른 네트워크 보안 어플라이언스에 완화 시그니처를 신속하게 배포합니다.
- 변화하는 위협 환경에 대비하는 고급 보호 체계를 구축합니다.
- 다양한 파일 형식을 분석합니다.

#### CFS(콘텐츠 필터링 서비스)

- 포괄적인 콘텐츠 필터링으로 내부에서 부적합하거나 비생산적이거나 불법일 수 있는 웹 콘텐츠에 액세스할 수 없도록 제어하는 맞춤형 기능을 제공합니다.
- 웹 사이트 등급은 SonicWall 방화벽에 로컬로 캐시되어 자주 방문하는 사이트에 즉시 응답할 수 있도록 합니다.

- 동적으로 업데이트되는 등급 아키텍처는 수백만 개의 URL, IP 주소, 도메인이 포함된 클라우드의 데이터베이스와 요청된 모든 웹 사이트를 상호 참조한 다음 각 등급을 로컬 정책 설정과 비교합니다.

#### 콘텐츠 필터링 클라이언트

- RTDMI(Real-Time Deep Memory Inspection)를 사용하여 맬웨어를 신속하고 정확하게 차단합니다.
- SonicWALL 콘텐츠 필터링 클라이언트로 방화벽 경계 외부에 있는 엔드포인트 장치에 인터넷 사용 정책을 적용하여 보안을 강화하고 생산성을 늘립니다. Windows, Mac OS, Chrome 엔드포인트를 위한 별도의 구독 서비스로 이용할 수 있습니다.

#### 연중무휴 24시간 지원

- 소프트웨어, 펌웨어 업데이트와 업그레이드는 네트워크 보안을 유지하여 솔루션을 새로운 것처럼 만듭니다.
- 24시간 사용할 수 있는 전화와 웹 기반 지원으로 기본 구성과 문제 해결에 대한 도움을 받을 수 있습니다.
- 고장이 발생하면 하드웨어를 교체해 드립니다.

- 연간 구독하면 SonicWall 서비스 게시판과 전자 지원 도구, 관리되는 토론 그룹에 액세스할 수 있습니다.

#### Capture Security Center Lite\*

- 클라우드 기반 포털
- 관리를 위한 하나의 창
- 방화벽 기본 설정 백업과 복원

SonicWall Advanced Gateway Security Suite에 대한 자세한 내용을 보려면 [www.sonicwall.com](http://www.sonicwall.com)을 방문하세요.

#### 회사 소개

SonicWall은 전 세계 중소기업과 대기업을 보호하면서 27년 넘게 사이버 범죄와 싸우고 있습니다. 우리의 제품과 파트너 제품의 조합으로 215개 이상의 국가와 지역에서 50만 개 이상의 기업이 각자의 요구 사항에 맞는 실시간 사이버 방어 솔루션을 마련하여 안심하고 더 많은 업무를 하고 있습니다.

\*SuperMassive 9000 시리즈, NSa 9250/9450/9650, NSsp 12000 시리즈의 경우 해당 AGSS 구독을 활성화하면 자동으로 CSC 관리를 이용할 수 있게 됩니다.