SONICWALL

SONICWALL SECURE MOBILE ACCESS(SMA)

사용자, 장치 ID, 위치 및 신뢰를 기반으로 멀티 클라우드 환경에서 기업 자원에 언제 어디서나 안전한 액세스할 수 있습니다.

SonicWall SMA는 조직들이 언제 어디서나 어떤 장치를 통해서도 중요한 기업 자원에 액세스할 수 있게 해주는 통합형 보안 액세스 게이트웨이입니다. SMA의 세부적인 액세스 관리 정책 엔진, 상황 인식 장치 인증, 애플리케이션 레벨 VPN 및 싱글 사인온으로 강화된 인증 기능을 통해 조직들은 멀티 클라우드 환경에서 장소에 구애받지 않는 업무 방식과 개인 소유 장치의 업무 활용(BYOD)을 포괄적으로 수용할 수 있습니다.

이동성과 BYOD

BYOD, 유연 근무제 또는 제3자 액세스를 수용하고자 하는 조직에게 SMA는 조직 전반에서 대단히 중요한 실행 포인트가 되고 있습니다. SMA는 업계 최고의 보안 기능을 제공하여 위협 접촉 범위를 최소화하면서 최신의 암호화 알고리듬과 암호를 지원함으로써 조직의 보안성을 한층 강화시킵니다. SonicWall의 SMA를 통해 관리자들은 보안이 철저한 모바일 액세스와 ID 기반의 권한을 제공할 수 있어 최종 사용자가 업무용 애플리케이션과 필요한 데이터와 자원에 쉽고 간단히 접근할 수 있습니다. 동시에 조직들은 보안이 철저한 BYOD 정책을 수립하여 기업의 네트워크와 데이터를 무단 접근과 맬웨어로부터 지킬 수 있습니다.

클라우드로의 전환

클라우드 이전을 시작하는 조직들에게 SMA는 복합적인 IT 환경에서 사용자를 인증하기 위해 단일 웹 포털을 이용하는 싱글 사인온(SSO) 인프라를 제공합니다. 기업의 자원이 사내에 있든, 웹 상에 있든, 호스팅 클라우드에 있든 상관없이, 액세스 경험이 일관성 있고 원활합니다. SMA는 또한 보안 강화를 위해 업계 최고의 다중 인증 기술과 통합됩니다.

관리형 서비스 제공자

자체 인프라를 호스팅하는 조직이나 관리형 서비스 제공자들을 위해 SMA는 고도의 비즈니스 연속성과 확장성을 제공하는 턴키 솔루션을 제공합니다. SMA는 인텔리전트 클러스터링을 통해 수십만 명의 사용자들로 확대하는 능력과 함께 단일 장치에서 최대 20,000명이 동시에 연결할 수 있습니다. 데이터 센터는 액티브-액티브 클러스터링과 빌트인 다이내믹 로드 밸런서로 비용을 절감할 수 있으며, 사용자 수요에 따라 실시간으로 가장 최적화된 데이터 센터로 글로벌 트래픽을 재할당합니다. SMA 툴세트는 서비스 제공자들이 제로 다운타임으로 서비스를 제공할 수 있게 해주므로 매우 공격적인 SLA를 수행할 수 있습니다.

SMA를 통해 IT 부서는 사용자 시나리오에 따라 최상의 경험과 가장 안전한 액세스를 제공할 수 있습니다. 물리적 기기 또는 강력한 가상의 기기로 이용할 수 있는 SMA는 기존의 사내 및/또는 클라우드 인프라에 완벽히 적합합니다. 조직들은 개인 소유의 장치에서 제3자 또는 직원들을 위한 클라이언트가 없는 웹 기반의 다양한 보안 액세스나 모든 장치 종류에서 실무자들을 위한 더 전통적인 클라이언트 기반의 풀터널 VPN 액세스 중에서 선택할 수 있습니다. 조직들이 단일 위치에서 5명의 사용자들에게 신뢰할 수 있는 보안 액세스를 제공해야 하거나, 전 세계에 분산되어 있는 네트워크에서 수천 명의 사용자들로 확대해야 하든, SonicWall SMA는 솔루션을 가지고 있습니다.

SonicWall SMA는 조직들이 안심하고 이동성과 BYOD를 수용할 수 있고 손쉽게 클라우드로 전환할 수 있게 해줍니다. SMA는 직원들에게 권한을 주고 일관성 있는 액세스 경험을 제공합니다.

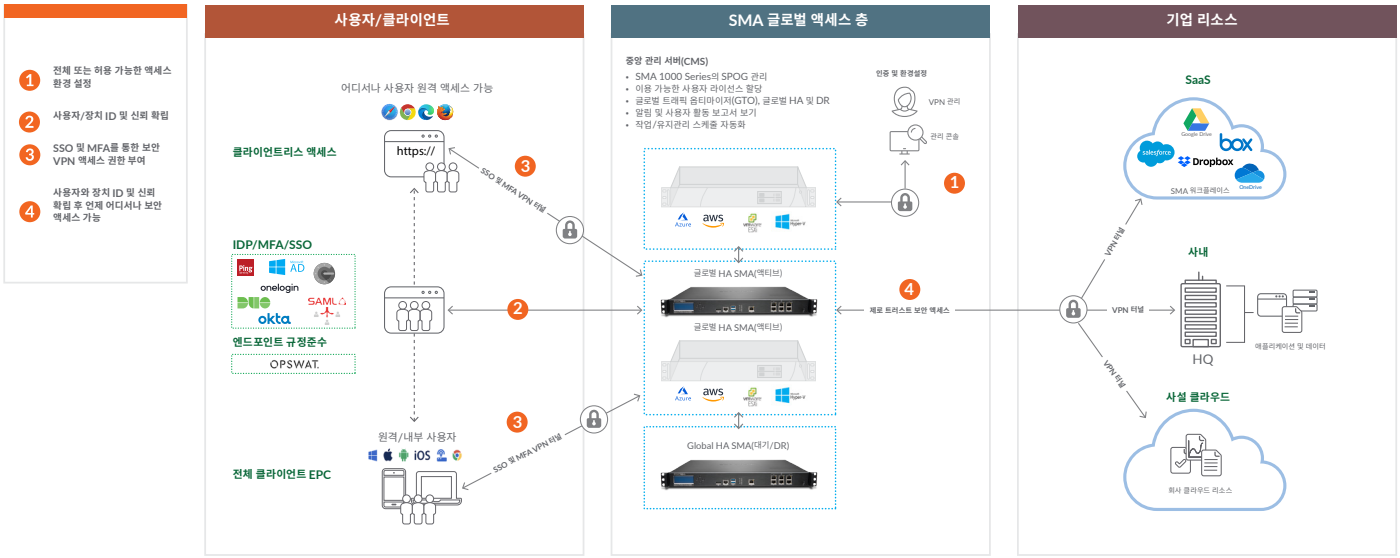
장점:

- "언제든지 모든 장치와 모든 애플리케이션"에 안전하게 액세스할 수 있게 모든 네트워크와 클라우드 리소스에 통합 액세스를 제공
- 강력한 액세스 컨트롤 엔진으로 세부적 정책을 정의함으로써 누가 무슨 리소스에 액세스할 수 있는지를 통제함
- 단일 URL로 모든 SaaS에 또는 로컬 호스팅 애플리케이션에 통합된 싱글 사인온을 제공함으로써 생산력 향상
- 인프라 구성요소를 복합 IT 환경에 통합하여 총 소유 비용(TCO)이 낮아지고, 액세스 관리의 복잡성이 감소
- 모든 연결 장치에 대한 가시성을 확보하여 정책과 엔드포인트의 건전성에 기반하여 액세스 권한 부여
- Capture ATP 샌드박스로 고객의 네트워크에 업로드되는 모든 파일을 스캔함으로써 맬웨어 침입 방지
- 웹 기반의 공격에 대비하고 웹 애플리케이션 방화벽(Web Application Firewall) 애드온을 통해 PCI 규정 준수
- Geo IP 감지 및 봇넷 보호로 디도스 공격과 좀비 공격을 차단
- 엔드포인트 장치에 에이전트를 설치, 관리하는 간접 비용 없이 웹 브라우저 기반의 클라이언트리스 HTML5를 이용하는 안전한 기본 에이전트 기능 사용
- 실시간 모니터링과 종합 보고로 적절한 결정을 내리는 데 필요한 실행 가능한 통찰 정보 확보
- ESXi 또는 Hyper-V의 사설 클라우드에서나 AWS 또는 Microsoft Azure 공용 클라우드 환경에서 물리적 어플라이언스 또는 가상 어플라이언스로서 구축
- 실시간 수요를 기반으로 하여 액세스 라이선스를 동적으로 발급할 수 있어 엔드포인트를 최고 성능과 최저 대기 연결로 자동으로 안내함
- 어플라이언스 대체 작동 기능에 악영향을 주지 않으면서도 추가 하드웨어나 서비스 없이 빌트인 로드 밸런싱으로 초기 비용 절감
- 즉각적으로 용량을 조정함으로써 비즈니스 중단이나 트래픽 급증에 대비함

SMA 구축

언제 어디서나 어떤 장치이든 안전한 액세스를 위한 강화된 에지 게이트웨이

SMA는 사내와 클라우드 및 하이브리드 데이터 센터에 호스팅되어 있는 기업 리소스에 종합적인 포괄적인 원격 보안 액세스를 가능하게 합니다. 또한 ID 기반, 정책 적용 액세스 제어, 상황 인식 장치 인증, 애플리케이션 레벨 VPN을 적용하여 사용자와 장치 ID, 위치 및 신뢰성을 규명한 후 데이터, 리소스 및 애플리케이션에 액세스 권한을 부여합니다. ESXi 또는 Hyper-V의 사설 클라우드에서나 AWS 또는 Microsoft Azure 공용 클라우드 환경에서 강화된 Linux 어플라이언스 또는 가상 어플라이언스로서 유연하게 구축됩니다.



SMA 클라우드/사내 구축

물리적 기기와 가상적 기기의 유연한 배치

SonicWall SMA는 강화된 고성능 기기로 또는 가상의 기기로 구축할 수 있고 공유 컴퓨팅 리소스를 활용하여 이용성을 최적화하고 전환을 용이하게 하며 자본 비용을 절감할 수 있습니다. 하드웨어 어플라이언스는 SSL 가속, VPN 처리량 및 강력한 프록시로 성능을 키워 확고한 보안 액세스를 제공하는 멀티코어 아키텍쳐를 기반으로 합니다. 규제기관과 연방 기관들을 위해 SMA는 FIPS 140-2 Level 2 인증으로도 이용할 수 있습니다. SMA 가상 어플라이언스는 Microsoft Hyper-V, VMware ESX 및 AWS를 비롯한 주요 가상 플랫폼 또는 클라우드 플랫폼에서 똑같이 강력한 보안 액세스 능력을 제공합니다.

어플라이언스간에 공유되는 사용자 라이선스

전 세계적으로 분산되어 있는 어플라이언스를 가진 조직들은 시차로 인한 사용자 라이선스 수요 변동으로 이득을 얻을 수 있습니다. 조직이 풀 VPN 라이선스를 구축하든, 기본적 ActiveSync 라이선스를 구축하든 상관없이, SMA의 중앙집중식 관리는 근무 외 시간/야간 시간 때문에 사용량이 감소한 다른 지리적 지역의 어플라이언스로부터 사용자 수요가 최고치에 이른 관리형 어플라이언스로 라이선스를 재할당합니다.

상황 인식 장치 프로파일링을 이용하는 네트워크 가시성

업계 최고의, 상황 인식 인증 기능은 오직 신뢰할 수 있는 장치와 권한을 가진 사용자에게만 액세스를 허용합니다. 랩탑과 데스크탑 PC에 대해서도 보안 소프트웨어, 클라이언트 인증서 및 장치 ID가 있는지 없는지 조사합니다. 모바일 장치에 대해서는 액세스 권한을 부여하기 전에 장치의 탈옥 여부나 루트 상태, 장치 ID, 인증서 상태 및 OS 버전과 같은 필수적인 보안 정보 조사를 합니다. 정책 요건에 부합하지 않는 장치들은 네트워크 액세스가 허용되지 않으며 해당 사용자에게 규정 미준수를 통보합니다.

단일 웹 포털에서 일관성 있는 경험

사용자들은 모든 개별 애플리케이션 URL을 기억하고 철저하게 북마크를 보관할 필요가 없습니다. SMA는 중앙집중식 액세스 포털을 제공하여 사용자들이 표준 웹 브라우저에서 모든 중요한 필수 애플리케이션에 액세스할 수 있도록 하나의 URL을 제공합니다. 사용자가 브라우저를 통해 로그온한 후, 브라우저 창에 주문형 웹 사용자 포털이 표시되고 모든 SaaS 또는 로컬 애플리케이션에 액세스할 수 있는 단일창 보기를 제공합니다. 이 포털은 특정한 엔드포인트 장치, 사용자 또는 그룹과 관련있는 링크와 개인 맞춤화된 북마크만 표시합니다. 이 포털은 관련 지식이 없어도 기능 수행을 할 수 있는 플랫폼이며 Windows, Mac OS, Linux, iOS 및 Android 장치를 비롯한 모든 주요 장치 플랫폼을 지원하고 이 모든 장치에서 광범위한 브라우저 지원을 제공합니다.

SaaS와 로컬 애플리케이션에 통합된 싱글 사인온

비밀번호를 여러 개 사용해야 하는 필요성을 없애고 비밀번호 재사용과 같은 잘못된 보안 행태를 중단시켜 줍니다. SMA는 클라우드로 호스팅되는 SaaS 애플리케이션과 사내에 호스팅되는 애플리케이션 모두에 통합된 싱글 사인온을 제공합니다. SMA는 보안 강화를 위해 다수의 인증, 권한 부여 및 계정 서버를 최고의 다중 인증 기술과 통합합니다. 보안 SSO는 SMA가 엔드포인트 건전성과 규정 준수 여부를 확인한 후에 허가된 엔드포인트 장치에만 제공됩니다. 액세스 정책 엔진은 사용자들이 허가된 애플리케이션만 볼 수 있게 하고 인증이 성공된 후에 액세스를 허용합니다. 이 솔루션은 VPN 클라이언트를 이용할 때도 통합된 SSO를 지원하여 클라이언트 기반 액세스를 사용하든 클라이언트리스 보안 액세스를 사용하든 원활한 인증 경험을 제공합니다.

침해 및 지능형 위협 방지

SonicWall SMA는 액세스 보안 층을 추가하여 고객의 보안 상태를 개선하고 위협을 줄여줍니다.

- SMA는 SonicWall Capture ATP 클라우드 기반 멀티 엔진 샌드박스와 통합되어 엔드포인트가 관리되지 않는 사용자가 또는 기업 네트워크 외부인이 업로드하는 모든 파일을 스캔합니다. 이로써 사용자는 외출 중에도 사무실에 있을 때처럼 랜섬웨어나 제로데이 맬웨어 같은 지능형 위협으로부터 동일한 수준의 보호를 받을 수 있습니다[1].
- SonicWall Web Application Firewall 서비스는 기업들에게 사내 웹 기반 애플리케이션을 안전하게 지킬 수 있는 저렴하고 통합이 잘 된 솔루션을 제공합니다. 이 덕분에 고객들은 악의적이거나 확인되지 않은 사용자 액세스가 있는 경우 데이터 기밀을 지킬 수 있고 사내 웹 서비스도 피해를 입지 않습니다.
- Geo-IP 및 Botnet 감지 기능은 디도스 공격과 좀비 공격으로부터 조직을 보호하고 봇넷 기능을 하는 위험한 엔드포인트로부터도 조직을 보호합니다.

원활하고 보안이 철저한 브라우저 기반의 클라이언트리스 액세스

SonicWall SMA의 "클라이언트리스" 특징이란 관리자가 원격 액세스용으로 사용할 컴퓨터에 전체 클라이언트 컴포넌트를 직접 설치할 필요가 없다는 의미입니다. 이러한 특징으로 자바에 대한 의존성과 IT 간접비용이 없어지므로 원격 액세스의 개념을 크게 확대할 수 있습니다. 즉, 사전 설치나 사전 구성이 필요하지 않으므로, 권한을 가진 원격 사용자가 세계 어디서나 아무 컴퓨터에 앉아서도 그들의 기업 리소스에 안전하게 액세스 할 수 있다는 의미입니다. 가장 순수한 형태의 보안 액세스는 HTML5를 사용하는 엄격한 브라우저 방식으로서 사용자들에게 원활하고 통합된 경험을 제공합니다.

비즈니스 연속성 제공

원활한 사용자 경험을 위해 SMA는 관리형 윈도우 장치에 대해 상시 가동 VPN을 제공합니다. 관리자들은 허가된 엔드포인트 클라이언트가 공용 또는 신뢰할 수 없는 네트워크를 감지할 때마다 자동으로 VPN 연결을 만들도록 설정을 구성할 수 있습니다. 윈도우 장치에 한 번 로그인하는 것으로 사용자가 기업 리소스에 안전하게 연결될 수 있습니다. 사용자는 VPN 클라이언트에 로그인하거나 추가의 비밀번호를 관리할 필요가 없습니다. 이로써 모바일 사용자들이 마치 사무실에 있는 것처럼 중요한 필수 애플리케이션에 액세스할 수 있는 원활한 경험을 제공하고 IT 관리자들이 관리형 장치에 대한 통제권을 가지고 조직의 보안 상태를 개선할 수 있습니다.

직관적 관리 및 포괄적 보고

SonicWall은 직관적인 웹 기반 관리 플랫폼인 중앙집중식 관리 서버(CMS)를 제공하여, 어플라이언스 관리를 간소화하는 한편 광범위한 보고 기능을 제공합니다. 사용하기 쉬운 GUI는 개개의 또는 다수의 어플라이언스 정책 관리에 투명성을 제공합니다. 각 페이지는 관리되고 있는 모든 기계들간에 설정이 어떻게 구성되는지를 보여줍니다. 통합된 정책 관리는 액세스 정책과 환경설정을 만들고 모니터링하는 데 도움이 됩니다. 단일 정책은 사용자와 장치, 애플리케이션부터 데이터, 서버 및 네트워크까지 액세스를 통제할 수 있습니다. IT 팀은 정해진 작업과 예정된 활동을 자동화하여 보안 팀들을 반복 작업에서 자유롭게 하고 사고 대응과 같은 전략적 보안 작업에 집중할 수 있게 합니다. IT 팀은 사용하기 쉬운 보고 기능과 중앙에서 관리되는 로깅을 통해 사용자 액세스 동향과 시스템 차원의 건전성을 파악할 수 있게 됩니다.

운영 효율성 제공

조직들은 항상 중요한 필수 애플리케이션에 안전하게 액세스할 수 있도록 높은 신뢰수준으로 서비스를 유지하고 가동해야 합니다. SMA 어플라이언스는 하나의 데이터 센터를 가지고 있는 조직들에게는 전통적 액티브-패시브 고가용성(HA)을 지원하고, 현지의 또는 분산되어 있는 데이터 센터에는 액티브-액티브 또는 액티브-스탠바이 클러스터링의 글로벌 HA를 지원합니다. 그 두 가지 HA 모델 모두 시스템 대체 작동과 세션 지속성에 영향을 주지 않으면서 사용자들에게 마찰 없는 경험을 제공합니다.

고객의 니즈에 맞는 VPN 클라이언트 구축

랩탑, 스마트폰 및 태블릿을 비롯한 다양한 엔드포인트에 정책에 따른 보안 원격 액세스를 제공하기 위해 다양한 VPN 클라이언트 중에서 선택합니다.

VPN 클라이언트	지원되는 OS	지원되는 SMA 모델	주요 사항
모바일 연결	iOS, OS X, Android, Chrome OS, Windows 10	전체 모델	앱 VPN과 엔드포인트 제어 수행에 따라 생체 인증 제공
연결 터널(씬 클라이언트)	Windows, Mac OS 및 Linux	6200, 6210, 7200, 7210, 8200v, 9000	강력한 엔드포인트 컨트롤로 완벽한 "사무실 근무" 경험 제공
NetExtender(씬 클라이언트)	Windows 및 Linux	210, 410, 500v	세부적인 액세스 정책 시행과 기본 클라이언트를 통한 네트워크 액세스 확대

빌트인 로드 밸런서로 초기 비용 절감

SMA 어플라이언스에 내장된 로드 밸런싱 기능으로 중기업뿐만 아니라 대기업 모두 환경 구축시 예상되는 레벨 확장성을 가질 수 있습니다. SMA 어플라이언스의 엄선된 모델은 다이내믹 로드 밸런싱을 제공하여 세션 로드를 지능적으로 할당하고 수요에 기반하여 실시간으로 사용자 라이선스를 할당합니다. 조직들은 내부 로드 밸런스에 투자할 필요가 없으므로 초기 비용이 절감됩니다.

예상치 못한 사고에 대비한 보험

완벽한 기업 연속성과 DR 솔루션은 원격 액세스 트래픽에 있어서 중요한 스파이크 트래픽을 감당하면서도 보안과 비용 관리를 유지할 수 있어야 합니다. SMA를 위한 SonicWall 스파이크 라이선스 팩은 애드온 라이선스로서 분산되어 있는 기업이 사용자 수를 조정하고 즉시 최대 능력에 도달하여 기업 연속성을 순조롭게 달성할 수 있게 합니다. 스파이크 라이선스는 현재 사용자 수에서 향후 수십 또는 수백 명이 추가로 늘어날지 불확실한 상황에서 급증에 대비한 보험 같은 역할을 합니다.

기능

강화된 인증

통합된 싱글 사인온[2]	SMA는 SAML 2.0 인증을 사용하여 통합된 SSO로 단일 포털을 통한 사내 및 클라우드 리소스에 액세스할 수 있으며 보안 강화를 위한 다중 인증을 시행합니다.
다중 인증	X.509 디지털 인증서 서버 측과 클라이언트 측의 디지털 인증서 RSA SecurID, Dell Defender, Google OTP, Duo Security 및 기타 일회성 비밀번호/이중 인증 토큰 공통 액세스 카드(CAC) 듀얼 또는 다중 인증 캡차 지원, 사용자명/비밀번호
SAML 인증	SMA는 SAML ID 제공자(IdP), SAML 서비스 제공자(SP) 또는 기존의 사내 IdP로 설정하여 SAML 2.0 인증을 이용하는 통합 싱글 사인온(SSO)이 가능합니다.
인증 저장소	SMA는 사용자 계정과 비밀번호를 쉽게 관리할 수 있도록 업계 표준의 저장소와 간단히 통합된 저장소를 제공합니다. 중첩 그룹을 포함하여 RADIUS, LDAP 또는 Active Directory 인증 저장소를 기반으로 역동적으로 사용자 그룹을 이동시킬 수 있습니다. 특정한 권한 부여나 장치 등록 확인을 위해 공통 또는 사용자 정의 LDAP 속성을 조사할 수 있습니다.
Layer 3-7 애플리케이션 프록시	SMA는 유연성 있는 프록시 옵션을 제공합니다. 가령, 다이렉트 프록시를 통한 벤더 액세스, 리버스 프록시를 통한 계약자 액세스 및 ActiveSync를 통한 직원의 Exchange 액세스가 제공됩니다.
리버스 프록시	인증 기능이 있는 향상된 리버스 프록시 서비스를 통해 관리자는 애플리케이션 오프로딩 포털 및 북마크를 설정하여 사용자가 원격 애플리케이션과 RDP와 HTTP를 비롯한 리소스에 원활하게 연결될 수 있게 해줍니다. 이 기능은 IE, Chrome 및 Firefox를 포함한 모든 브라우저에서 지원됩니다.
Kerberos 제한 위임	SMA는 서비스를 위임하기 위해 프론트엔드 서비스를 신뢰할 필요가 없는 기존의 인증 인프라를 이용하는 인증 지원을 제공합니다.

액세스 관리

액세스 컨트롤 엔진(ACE)	관리자는 조직의 정책을 기준으로 액세스를 허용 또는 거부하며 세션을 격리할 때 복원 조치를 설정합니다. ACE 개체 기반의 정책은 네트워크, 리소스, ID, 장치, 애플리케이션, 데이터 및 시간 요소를 활용합니다.
엔드포인트 컨트롤(EPC)	EPC를 통해 관리자는 연결된 장치의 건전성 상태를 기반으로 세부적인 액세스 컨트롤 규칙을 시행할 수 있습니다. 심층적인 OS 통합으로 유형 분류와 위험 요소 평가를 위해 많은 요소들이 통합됩니다. EPC 조사는 서명 파일 업데이트의 버전 및 적용 가능성을 비롯하여 Windows, Mac 및 Linux 플랫폼을 위해 포괄적이고 사전 정의된 안티 바이러스 목록과 개인 방화벽과 안티 스파이웨어 솔루션을 사용하여 장치 프로필 설정을 간소하게 만듭니다.
앱 액세스 컨트롤(AAC)	관리자는 어떤 특정 모바일 애플리케이션이 개별 앱 터널을 통해 네트워크 상에서 어떤 리소스에 액세스 허용이 되는지를 정의할 수 있습니다. AAC 정책은 클라이언트와 서버 모두에서 시행되어 강력한 환경 보호를 제공합니다.

우수한 보안성

Layer 3 SSL VPN	SMA 시리즈는 모든 환경에서 가동되는 다양한 클라이언트 장치에 고성능의 layer-3 터널링 기능을 제공합니다.
암호화 기능 지원	구성 가능한 세션 길이 암호: AES 128 + 256비트, Triple DES, RC4 128비트 해시: SHA-256 타원 곡선 디지털 서명 알고리즘(ECDSA)
강화된 암호 지원	SMA 어플라이언스는 기본 설정 암호와 함께 규정 준수를 위한 격이 다른 강력한 암호 태세를 제공하므로 관리자는 성능, 보안 강도 또는 호환성을 추가로 개선할 수 있습니다.
보안 인증	FIPS 140-2 Level 2, ICSA SSL-TLS, 공동 평가 기준 진행, UC-APL에 대해 인증받음
보안 파일 공유	자동화된 복구로 게이트웨이에서 랜섬웨어와 같은 알 수 없는 제로데이 공격을 차단합니다. 보안 액세스를 통해 비관리 엔드포인트로 기업 네트워크에 업로드되는 파일들은 클라우드 기반의 다중 엔진 Capture ATP로 검사를 받습니다.
웹 애플리케이션 방화벽(WAF)	프로토콜과 웹 기반의 공격을 방지하여 금융, 의료, 전자상거래 및 다른 비즈니스가 OWASP Top 10 및 PCI 규정준수를 달성하도록 돕습니다.
Geo IP 탐지 및 봇넷 보호	Geo IP 탐지 및 봇넷 보호를 통해 메커니즘을 갖춘 고객들이 다양한 지리적 위치에서의 사용자 액세스를 허용하거나 제한할 수 있습니다.
TLS 1.3 지원	이전 모델의 복잡성은 줄이면서 보안과 성능 모두 개선.

직관적인 사용자 경험

상시 작동하는 VPN	보안을 개선하고 트래픽 가시성을 확보하고 규정을 준수하기 위해 회사가 지급한 Windows 장치에서 기업 네트워크에 보안 연결을 자동으로 설정합니다.
보안 네트워크 탐지(SND)	SMA의 네트워크 인식 VPN 클라이언트는 장치가 외부에 있을 때 이를 감지하고 VPN을 자동으로 재연결시키고 장치가 신뢰할 수 있는 네트워크로 돌아올 때 다시 중단시킵니다.
클라이언트리스 리소스 액세스	SMA는 HTML5 브라우저 에이전트를 통해 안전한 클라이언트리스 리소스 액세스를 제공하여 RDP, ICA, VNC, SSH 및 Telnet 프로토콜을 제공합니다.
싱글 사인온 포털	WorkPlace 포털은 복합적인 IT 환경에서 싱글 사인온(SSO)으로 어느 리소스에나 안전하고 쉽게 액세스할 수 있는 맞춤형 단일 보기창을 제공합니다. 추가적인 로그인이나 VPN이 필요없습니다.
Layer 3 터널링	관리자는 최대 성능을 위해 분할 터널을 선택하거나 SSL/TLS 터널링과 옵션형 ESP 대비책으로 Redirect-All 모드를 시행할 수 있습니다.
HTML5 파일 탐색기[1]	최신의 파일 브라우저를 사용하면 사용자들이 모든 웹 브라우저에서 파일 공유에 쉽게 액세스할 수 있습니다.
모바일 OS 통합	모든 OS 플랫폼에서 모바일 연결이 지원되어 사용자들은 완전히 자유롭게 모바일 장치를 선택할 수 있습니다.

복원력

글로벌 트래픽 옵티마이저(GTO)	SMA는 사용자에게 영향을 주지 않으면서 글로벌 트래픽 로드 밸런싱을 제공합니다. 트래픽은 가장 최적화되고 성능이 가장 우수한 데이터센터로 라우팅됩니다.
역동적인 고 가용성[2]	SMA는 액티브/패시브를 지원하고 단일 데이터센터에 구축하든 지리적으로 분산되어 있는 다수의 데이터센터에 구축하든, 고가용성을 위해 액티브/액티브 설정을 지원합니다.
일반적 세션 지속성[1]	시스템 대체 작동 기능에 악영향을 주지 않으면서 사용자들에게 마찰없는 경험을 제공합니다. 어플라이언스가 오프라인 상태인 경우에 SMA의 지능형 클러스터링이 재인증 필요 없이 세션 데이터에 따라 사용자를 재할당합니다.
확장 가능한 성능	SMA 어플라이언스는 다수의 어플라이언스를 구축함으로써 성능을 기하급수적으로 확장하여 단 하나의 장애 지점도 제거합니다. 수평적 클러스터링은 물리적 어플라이언스와 가상의 SMA 어플라이언스 혼합을 완전히 지원합니다.
효율적인 라이선스 정책	더 이상 개별 SMA 어플라이언스에 사용자 라이선스를 적용할 필요가 없습니다. 사용자 수요를 기반으로 관리형 어플라이언스 사이에서 사용자를 역동적으로 분산 및 재할당할 수 있습니다.

중앙 관리 및 모니터링

중앙 관리 시스템(CMS)	CMS는 모든 SMA 기능을 위해 중앙집중식, 웹 기반의 관리를 제공합니다.
맞춤형 알람	IT 인프라 네트워크 관리 시스템(NMS)에 의해 모니터링되는 SNMP 트랩을 생성할 수 있도록 알람을 설정할 수 있습니다. 관리자는 즉각적인 조치를 취하기 위한 Capture ATP 파일 스캔과 디스크 사용량에 대해 알람을 설정할 수도 있습니다.
실시간 대시보드	실시간, 맞춤형 대시보드를 이용하여 IT 관리자는 빠르고 쉽게 액세스 문제를 진단할 수 있어 문제해결을 위한 중요한 정보를 얻을 수 있습니다.
SIEM 통합	중앙의 SIEM 데이터 수집기로의 실시간 출력을 통해 보안 팀은 이벤트 중심의 활동을 서로 연관시켜 특정 사용자 또는 애플리케이션의 전체 워크 플로우를 이해할 수 있습니다. 이것은 보안 사고 관리와 포렌식 분석 시에 대단히 중요합니다.
스케줄러	수동으로 하지 않고 스케줄러를 사용하여 정책 배포, 환경 설정 복제 및 서비스 재시작과 같은 유지관리 작업을 예약할 수 있습니다.

확장성

관리 API	관리 API를 사용하여 단일 SMA 또는 글로벌 CMS 환경 내에서 모든 개체에 대한 완전한 프로그램 방식의 관리가 가능합니다.
최종 사용자 API	최종 사용자 API는 모든 로그온, 인증 및 엔드포인트 워크플로우에 대해 완전한 제어 기능을 제공합니다.
2중 인증(2FA)	SMA는 Google Authenticator, Microsoft Authenticator, Duo Security 등과 같은 일회용 만료 비밀번호(TOPT) 솔루션을 활용하여 이중 인증을 제공합니다.
MDM 통합	SMA는 Airwatch와 Mobile Iron과 같은 기업 모바일 관리(EMM) 제품과 통합되어 있습니다.
기타의 제3자 통합	SMA는 OPSWAT와 같은 업계 최고의 벤더와 통합하여 강화된 위협 방지 기능을 제공합니다.

[1]SMA OS 12.1 이상에서 사용 가능

[2] SMA 12.1에서 강화됨

기능 요약(모델 별 비교)

카테고리	기능	210	410	500v	6210	7210	8200v
구축	운영 시스템	SMA 10.2	SMA 10.2	SMA 10.2	SMA 12.4	SMA 12.4	SMA 12.4
	지원되는 하이퍼바이저	–	–	VMware ESXi / Microsoft Hyper-V	–	–	VMware ESXi / Microsoft Hyper-V
	지원되는 공용 클라우드 플랫폼	–	–	AWS/Azure	–	–	AWS/Azure
처리량	최대 동시 사용자 세션	50	250	250	2,000	10,000	5,000
	최대 SSL/TLS 처리량	560 Mbps	844 Mbps	186 Mbps	800 Mbps	5.0 Gbps	1.58 Gbps
클라이언트 액세스	Layer 3 터널	•	•	•	•	•	•
	분할 터널과 redirect-all	•	•	•	•	•	•
	상시 작동 VPN	•	•	•	•	•	•
	자동 ESP 캡슐화	–	–	–	•	•	•
	HTML5(RDP, VNC, ICA, SSH, Telnet, 네트워크 탐색기)	•	•	•	•	•	•
	보안 네트워크 탐지	–	–	–	•	•	•
	파일 브라우저(CIFS/NFS)	•	•	•	•	•	•
	Citrix XenDesktop/XenApp	•	•	•	•	•	•
	VMware 보기	–	–	–	•	•	•
	주문형 터널	–	–	–	•	•	•
	Chrome/Firefox 확장 프로그램	–	–	–	•	•	•
	CLI 터널 지원	–	–	–	•	•	•
	Mobile Connect(iOS, Android, Chrome, Win 10, Mac OSX)	•	•	•	•	•	•
	Net Extender(Windows, Linux)	•	•	•	–	–	–
	Connect Tunnel(Windows, Mac OSX, Linux)	–	–	–	•	•	•
	Exchange ActiveSync	•	•	•	•	•	•
모바일 액세스	앱별 VPN	–	–	–	•	•	•
	앱 컨트롤 시행	–	–	–	•	•	•
	앱 ID 확인	–	–	–	•	•	•
사용자 포털	브랜딩	•	•	•	•	•	•
	커스터마이징	–	–	–	•	•	•
	로컬리제이션	•	•	•	•	•	•
	사용자 정의 북마크	•	•	•	•	•	•
	맞춤 URL 지원	•	•	•	•	•	•
	SaaS 애플리케이션 지원	–	–	–	•	•	•
보안	FIPS 140-2	–	–	–	•	•	–
	ICSA SSL-TLS	•	•	•	•	•	•
	Suite B 암호	–	–	–	•	•	•
	다이내믹 EPC 조사	•	•	•	•	•	•
	역할 기반의 액세스 컨트롤(RBAC)	–	–	–	•	•	•
	엔드포인트 등록	•	•	•	•	•	•
	안전한 파일 공유(Capture ATP)	•	•	•	•	•	•
	엔드포인트 격리	•	•	•	•	•	•
	OSCP CRL 확인	–	–	–	•	•	•
	암호 선택	–	–	–	•	•	•
	PKI 및 클라이언트 인증	•	•	•	•	•	•
	Geo IP 필터	•	•	•	–	–	–
	봇넷 필터	•	•	•	–	–	–
	포워드 프록시	•	•	•	•	•	•
	리버스 프록시	•	•	•	•	•	•
인증 및 신원확인 서비스	SAML 2.0	–	–	–	•	•	•
	LDAP, RADIUS	•	•	•	•	•	•
	Kerberos(KDC)	•	•	•	•	•	•
	NTLM	•	•	•	•	•	•
	SAML 신원 제공자(IdP)	•	•	•	•	•	•
	생체인식 장치 지원	•	•	•	•	•	•
	iOS의 페이스 ID 지원	•	•	•	•	•	•
	2중 인증(2FA)	•	•	•	•	•	•
	다중 인증(MFA)	–	–	–	•	•	•

기능 요약(모델 별 비교 계속)

카테고리	기능	210	410	500v	6210	7210	8200v
인증 및 신원확인 서비스 계속	연쇄 인증	–	–	–	•	•	•
	이메일 또는 SMS를 통한 일회용 패스코드	•	•	•	•	•	•
	공통 액세스 카드(CAC) 지원	–	–	–	•	•	•
	X.509 인증서 지원	•	•	•	•	•	•
	캡차 통합	–	–	–	•	•	•
	원격 비밀번호 변경	•	•	•	•	•	•
	양식 기반의 SSO	•	•	•	•	•	•
	통합된 SSO	–	–	–	•	•	•
	세션 지속성	–	–	–	•	•	•
	자동 로그온	•	•	•	•	•	•
액세스 컨트롤	그룹 AD	•	•	•	•	•	•
	LDAP 속성	•	•	•	•	•	•
	지리적 위치 정책	•	•	•	–	–	–
	지속적인 엔드포인트 모니터링	•	•	•	•	•	•
관리	관리 인터페이스(이더넷)	–	–	–	•	•	•
	관리 인터페이스(콘솔)	–	–	–	•	•	•
	HTTPS 관리	•	•	•	•	•	•
	SSH 관리	–	–	–	•	•	•
	SNMP MIBS	•	•	•	•	•	•
	Syslog 및 NTP	•	•	•	•	•	•
	사용량 모니터링	•	•	•	•	•	•
	환경 설정 롤백	•	•	•	•	•	•
	중앙집중식 관리	–	–	–	•	•	•
	중앙집중식 보고	–	–	–	•	•	•
	관리 REST API	–	–	–	•	•	•
	인증 REST API	–	–	–	•	•	•
	RADIUS 어카운팅	–	–	–	•	•	•
	예약된 작업	–	–	–	•	•	•
	중앙집중식 세션 라이센싱	–	–	–	•	•	•
	이벤트 중심의 감사	–	–	–	•	•	•
네트워킹	IPv6	•	•	•	•	•	•
	글로벌 로드 밸런싱	–	–	–	•	•	•
	서버 로드 밸런싱	•	•	•	–	–	–
	TCP 상태 복제	•	•	•	•	•	•
	클러스터 상태 장애 극복	–	–	–	•	•	•
	액티브/패시브 고 가용성	–	•	•	•	•	•
	액티브/액티브 고 가용성	–	–	–	•	•	•
	수평적 확장	–	–	–	•	•	•
	단일 또는 다중 FQDN	–	–	–	•	•	•
	L3-7 스마트 터널 프록시	•	•	•	•	•	•
	L7 애플리케이션 프록시	•	•	•	•	•	•
통합	2FA TOTP 지원	•	•	•	•	•	•
	EMM 및 MDM 제품 지원	–	–	–	•	•	•
	SIEM 제품 지원	–	–	–	•	•	•
	TPAM 비밀번호 저장소	–	–	–	•	•	•
	ESX 하이퍼바이저 지원	–	–	•	–	–	•
	Hyper-V 하이퍼바이저 지원	–	–	•	–	–	•
라이센싱 옵션	구독 기반 라이선스	–	–	–	•	•	•
	영구적 지원 라이선스	•	•	•	•	•	•
	웹 애플리케이션 방화벽(WAF)	•	•	•	–	–	–
	스파이크 라이센싱	•	•	•	•	•	•
	단계적 라이센싱	–	–	–	•	•	•
	가상 지원	•	•	•	–	–	–

** VPN 클라이언트에 대한 자세한 정보 알아보기: https://www.sonicwall.com/en-us/products/remote-access/vpn-client*

고급 어플라이언스로 업그레이드할 때의 이점

성능 강화 | 처리량 증가 | 기능 강화 | 확장성 개선

어플라이언스 사양

다양한 목적으로 특별히 만들어진 보안 모바일 액세스(SMA) 어플라이언스 중에서 선택하세요. 가상 어플라이언스와 물리적 어플라이언스로 유연한 구축 방법을 찾으세요.

물리적 어플라이언스 사양

성능	SMA 210	SMA 410	SMA 6210	SMA 7210
동시 세션/사용자	최대 50	최대 250	최대 2,000	최대 10,000
SSL VPN 처리량* (최대 CCU)	560 Mbps	844 Mbps	최대 800 Mbps	최대 5.0 Gbps
폼 팩터	1U	1U	1U	1U
크기	16.92 x 10.23 x 1.75인치 (43x26x4.5cm)	16.92 x 10.23 x 1.75인치 (43x26x4.5cm)	17.0 x 16.5 x 1.75인치 (43 x 41.5x 4.5cm)	17.0 x 16.5 x 1.75인치 (43 x 41.5x 4.5cm)
어플라이언스 무게	11파운드(5kgs)	11파운드(5kgs)	17.7파운드(8kgs)	18.3파운드(8.3kgs)
암호화 데이터 가속(AES-NI)	없음	없음	있음	있음
전용 관리 포트	없음	없음	있음	있음
SSL 가속	없음	없음	있음	있음
하드디스크 용량	4GB(플래시 메모리)	4GB(플래시 메모리)	2 x 1TB SATA; RAID 1	2 x 1TB SATA; RAID 1
인터페이스	(2) GB 이더넷, (2) USB, (1) 콘솔	(4) GB 이더넷, (2) USB, (1) 콘솔	(6)포트 1GE, (2) USB, (1) 콘솔	(6)포트 1GE, (2)포트 10Gb SFP+, (2) USB, (1) 콘솔
메모리	4GB	8GB	8GB DDR4	16GB DDR4
TPM 칩	없음	없음	있음	있음
프로세서	4코어	8코어	4코어	4코어
MTBF(@ 25°C 또는 77°F) 단위: 시간	61,815	60,151	70,127	129,601
운영 및 규정준수	**SMA 210**	**SMA 410**	**SMA 6210**	**SMA 7210**
전원	고정형 전원 공급	고정형 전원 공급	고정형 전원 공급	듀얼 전원, 핫스왑 가능
정격 입력	100-240VAC, 50-60MHz	100-240VAC, 50-60MHz	100-240 VAC, 1.1 A	100-240 VAC, 1.79 A
전력 소비	26.9 W	31.9 W	77 W	114 W
총 열 전달	92 BTU	109 BTU	264 BTU	389 BTU
환경	WEEE, EU RoHS, China RoHS			
비 동작 충격	110 g, 2 msec			
배출가스	FCC, ICES, CE, C-Tick, VCCI; MIC			
안전성	TUV/GS, UL, CE PSB, CCC, BSMI, CB scheme			
작동 시 온도	0°C - 40°C(32°F - 104° F)			
FIPS 인증	없음	없음	조작 방지 기능이 있는 FIPS 140-2 Level 2	

** 처리 성능은 구축과 연결성에 따라 달라질 수 있습니다. 간행 번호는 사내 시험소 상태를 기준으로 한 것입니다.*

가상의 어플라이언스 사양

사양	SMA 500v(ESX/ESXi/Hyper-V)	SMA 8200v(ESX/ESXi/Hyper-V)
동시 세션	최대 250 사용자	최대 5000
SSL-VPN 처리량* (최대 CCU)	최대 186Mbps	최대 1.58Gbps
할당 메모리	2GB	8GB
프로세서	1코어	4코어
SSL 가속	없음	있음
적용된 디스크 크기	2GB	64GB(기본)
설치된 운영 체제	Linux	강화된 Linux
전용 관리 포트	없음	있음

** 처리 성능은 구축과 연결성에 따라 달라질 수 있습니다. 간행 번호는 사내 시험소 상태를 기준으로 한 것입니다. Hyper-V의 SMA 8200v는 최대 5000 동시 세션으로 확장되고 Windows Server 2016으로 SMA OS 12.1을 실행할 때 최대 1.58Gbps SSL-VPN 처리량을 제공합니다.*

주문 정보

SKU	SONICWALL 보안 모바일 액세스(SMA) 어플라이언스
02-SSC-2800	SMA 210, 사용자 라이선스 5개
02-SSC-2801	SMA 410, 사용자 라이선스 25개
01-SSC-8469	SMA 500v, 사용자 라이선스 5개
02-SSC-0978	SMA 7210, 관리자 테스트 라이선스
02-SSC-0976	SMA 6210, 관리자 테스트 라이선스
01-SSC-8468	SMA 8200v(가상 어플라이언스)
SKU	**SONICWALL SMA 사용자 라이선스**
01-SSC-9182	SMA 500V 추가 5 사용자(SMA 210에도 사용 가능)
01-SSC-2414	SMA 500V 추가 100 사용자(SMA 410에도 사용 가능)
01-SSC-7856	SMA 5 사용자 라이선스 - 6210, 7210, 8200v에 스태킹 가능
01-SSC-7860	SMA 100 사용자 라이선스 - 6210, 7210, 8200v에 스태킹 가능
01-SSC-7865	SMA 5000 사용자 라이선스 - 7210, 8200v에 스태킹 가능
SKU	**SONICWALL SMA 지원 계약**
01-SSC-9191	SMA 500V 최대 25 사용자 1년 24X7 지원(SMA 210 및 410에도 사용 가능)
01-SSC-2326	SMA 6210 100 사용자 1년 24X7 지원 - 스태킹 가능
01-SSC-2350	SMA 7210 500 사용자 1년 24X7 지원 - 스태킹 가능
01-SSC-8434	SMA 8200V 5 사용자 1년 24X7 지원 - 스태킹 가능(SMA 6210, 7210에도 사용 가능)
01-SSC-8446	SMA 8200V 100 사용자 1년 24X7 지원 - 스태킹 가능(SMA 6210, 7210에도 사용 가능)
01-SSC-7913	SMA 8200V 5000 사용자 1년 24X7 지원 - 스태킹 가능(SMA 6210, 7210에도 사용 가능)
SKU	**6210, 7210, 8200V에 대한 중앙 관리**
CMS 어플라이언스 라이선스	
01-SSC-8535	CMS base + 3 어플라이언스 라이선스(무료 - 체험용 및 유료가입 사용자 라이선스로 이용)
01-SSC-8536	CMS 100 어플라이언스 라이선스 1년(유료가입 사용자 라이선스로 이용)
01-SSC-3369	CMS base + 3 어플라이언스(무료 - 영구적 사용자 라이선스로 이용)
01-SSC-3402	CMS 100 어플라이언스 라이선스 1년(영구적 사용자 라이선스로 이용)
중앙의 사용자 라이선스(유료가입)	
01-SSC-2298	CMS 라이선스풀 10 사용자 1년
01-SSC-8539	CMS 라이선스풀 1000 사용자 1년
01-SSC-5339	CMS 라이선스풀 50000 사용자 1년
중앙 사용자 라이선스(영구)	
01-SSC-2053	CMS 영구 라이선스 10명 사용자
01-SSC-2058	CMS 영구 라이선스 1000명 사용자
01-SSC-2063	CMS 영구 라이선스 50000명 사용자
중앙 사용자 라이선스(영구)에 대한 지원	
01-SSC-2065	CMS 24x7 지원 1년 10명 사용자
01-SSC-2070	CMS 24x7 지원 1년 1000명 사용자
01-SSC-2075	CMS 24x7 지원 1년 50000명 사용자
중앙 ActiveSync 라이선스(유료가입)	
01-SSC-2088	CMS 이메일 라이선스풀 10명 사용자 1년
01-SSC-2093	CMS 이메일 라이선스풀 1000명 사용자 1년
01-SSC-2087	CMS 이메일 라이선스풀 50000명 사용자 1년

주문 정보 계속

SKU	6210, 7210, 8200V에 대한 중앙 관리
중앙 스파이크 라이선스	
01-SSC-2111	CMS 스파이크 1000명 사용자 5일
01-SSC-2115	CMS 스파이크 50000명 사용자 5일
Capture 애드온(구독)	
해당 대리점에 문의 ** 구독 라이선스에는 24X7 지원이 포함되어 있습니다*	
SKU	**SONICWALL SMA 애드온**
01-SSC-2406	SMA 7210 FIPS 애드온
01-SSC-2405	SMA 6210 FIPS 애드온
01-SSC-9185	SMA 500V Web Application Firewall 1년(SMA 210 및 410에도 이용 가능)
SKU	**SONICWALL SMA 보안 업그레이드**
02-SSC-2794	SMA 210 보안 업그레이드, 5 사용자 번들 최대 25명 사용자 1년 24X7 지원
02-SSC-2795	SMA 210 보안 업그레이드, 5 사용자 번들 최대 25명 사용자 3년 24X7 지원
02-SSC-2798	SMA 410 보안 업그레이드, 25 사용자 번들 최대 100명 사용자 1년 24X7 지원
02-SSC-2799	SMA 410 보안 업그레이드, 25 사용자 번들 최대 100명 사용자 3년 24X7 지원
02-SSC-2893	SMA 6210 보안 업그레이드, 최대 100명 사용자 1년 24X7 지원
02-SSC-2894	SMA 6210 보안 업그레이드, 최대 100명 사용자 3년 24X7 지원
02-SSC-2895	SMA 7210 보안 업그레이드, 최대 250명 사용자 1년 24X7 지원
02-SSC-2896	SMA 7210 보안 업그레이드, 최대 250명 사용자 3년 24X7 지원
02-SSC-0860	SMA 8200V 보안 업그레이드, 최대 100명 사용자 1년 24X7 지원
02-SSC-0862	SMA 8200V 보안 업그레이드, 최대 100명 사용자 3년 24X7 지원
02-SSC-2807	SMA 500V 보안 업그레이드, 최대 100명 사용자 1년 24X7 지원
02-SSC-2808	SMA 500V 보안 업그레이드, 최대 100명 사용자 3년 24X7 지원
SKU	**SMA 스파이크 라이선스(용량 도달에 필요한 증분)**
01-SSC-2240	SMA 210 10일 50 사용자 스파이크 라이선스(SMA 410 및 500v에도 이용 가능)
01-SSC-7873	SMA 8200v 10일 5-2500 사용자 스파이크 라이선스(SMA 6210, 7210에도 사용 가능)
02-SSC-4490	SMA 500V 30일 250 사용자 스파이크 라이선스
02-SSC-4489	SMA 500V 60일 250 사용자 스파이크 라이선스
02-SSC-4488	SMA 200/210 30일 50 사용자 스파이크 라이선스
02-SSC-4487	SMA 200/210 60일 50 사용자 스파이크 라이선스
02-SSC-4486	SMA 400/410 30일 250 사용자 스파이크 라이선스
02-SSC-4485	SMA 400/410 60일 250 사용자 스파이크 라이선스
02-SSC-4471	SMA CMS 스파이크 애드온 라이선스 100 사용자 30일
02-SSC-4473	SMA CMS 스파이크 애드온 라이선스 500 사용자 30일
02-SSC-4475	MA CMS 스파이크 애드온 라이선스 1,000 사용자 30일
02-SSC-4477	SMA CMS 스파이크 애드온 라이선스 5,000 사용자 30일
02-SSC-4479	SMA CMS 스파이크 애드온 라이선스 10,000 사용자 30일
02-SSC-4481	MA CMS 스파이크 애드온 라이선스 25,000 사용자 30일
02-SSC-4483	SMA CMS 스파이크 애드온 라이선스 50,000 사용자 30일
02-SSC-4472	SMA CMS 스파이크 애드온 라이선스 100 사용자 60일
02-SSC-4474	SMA CMS 스파이크 애드온 라이선스 500 사용자 60일
02-SSC-4476	SMA CMS 스파이크 애드온 라이선스 1,000 사용자 60일

주문 정보 계속

SKU	SMA 스파이크 라이선스(용량 도달에 필요한 증분)
02-SSC-4478	SMA CMS 스파이크 애드온 라이선스 5,000 사용자 60일
02-SSC-4480	SMA CMS 스파이크 애드온 라이선스 10,000 사용자 60일
02-SSC-4482	SMA CMS 스파이크 애드온 라이선스 25,000 사용자 60일
02-SSC-4484	SMA CMS 스파이크 애드온 라이선스 50,000 사용자 60일

** 다년간의 SKU 및 지원 계약도 가능합니다. SKU의 전체 리스트는 해당 대리점으로 문의하십시오.*

파트너 지원 서비스

SonicWall 솔루션의 계획, 구축 또는 최적화에 도움이 필요하십니까? SonicWall 고급 서비스 파트너는 세계 최고 수준의 전문 서비스를 제공하기 위한 교육을 받았습니다. 자세히 알아보기: www.sonicwall.com/PES.

SonicWall 소개

SonicWall은 전 세계 중소기업, 대기업, 정부 기관을 보호하기 위해 27여 년을 사이버 범죄에 맞서 싸워왔습니다. 수상 경력에 빛나는 실시간 침입 탐지, 방지 솔루션은 SonicWall Capture Labs 연구의 지원을 받아 215개 이상의 국가와 지역에서 100만 개 이상의 네트워크와 이메일, 애플리케이션 및 데이터를 보호합니다. 당사의 솔루션을 채택한 조직들은 보다 효과적으로 운영되고 보안에 대한 두려움이 적습니다. 자세한 정보를 원하시면 www.sonicwall.com을 방문하시거나 트위터, 링크드인, 페이스북 및 인스타그램에서 저희 사이트를 팔로우해주시기 바랍니다.

SonicWall Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
저희 웹사이트에서 더 많은 정보를 보실 수 있습니다.
www.sonicwall.com
© 2020 SonicWall Inc. 모든 권한 보유. SonicWall은 미국 및/또는 기타 국가에서 SonicWall Inc. 및/또는 그 계열사의 상표 또는 등록상표입니다. 그 밖의 모든 상표와 등록상표는 각 소유권자의 재산입니다.
Datasheet-SecureMobileAccess-US-VG-1834