SONICWALL

SonicWall Cloud Edge 보안 액세스

단시간에 제로 트러스트 보안 배치

SonicWall Cloud Edge 보안 액세스는 강력한 클라우드 서비스로서 AWS, Azure, Google Cloud 등을 위해 사이트간 및 하이브리드 클라우드 연결을 위한 간단한 서비스형 네트워크를 제공합니다. 그 과정에 제로 트러스트와 최소 권한 보안 접근방법을 하나의 통합 서비스로 통합합니다.

최소 권한 액세스 접근법은 "업무적 필요성" 개념과 유사하게, 필요한 경우로만 특정 사용자의 접근을 제한합니다. 기업은 네트워크의 다른 중요한 영역에 대한 노출을 제한함으로써 운영 융통성에 영향을 주지 않고 리소스를 보호할 수 있습니다.

SonicWall Cloud Edge 보안 액세스는 4가지의 핵심적 보안 조치를 바탕으로 제로 트러스트 보안을 적용합니다.

- 내부 트래픽에 대해서도 사용자 및 장치의 자격증명 확인
- 검증 및 기업지침 준수를 확인하기 위한 컨텍스트 파악
- 위협이 내부로 확산되지 않도록 네트워크 액세스를 극세분화
- 요청된 애플리케이션에 한 해 액세스 허용

Cloud Edge 보안 액세스 인프라의 핵심은 현대적이고 계획된 보안 소프트웨어 정의 경계 (SDP) 아키텍처입니다.

SDP는 사용자와 장치를 인증하는 컨트롤러를 트러스트 브로커의 역할을 하는 게이트웨이에서 분리합니다. Cloud Edge 보안 액세스 서비스는 게이트웨이를 최종 사용자 위치에 가까이 분산시킴으로써 신속하게 확장하여 고성능을 유지하고 최고의 클라우드 경험을 제공할 수 있습니다.

또한 기능을 분리하여 DDoS, 공용 WiFi 탈취, SYN 플러드, Slowloris 등과 같은 사이버 위협을 효과적으로 차단하고 SonicWall이 통합된 제로 트러스트 보안 플랫폼을 제공할 수 있도록 합니다.

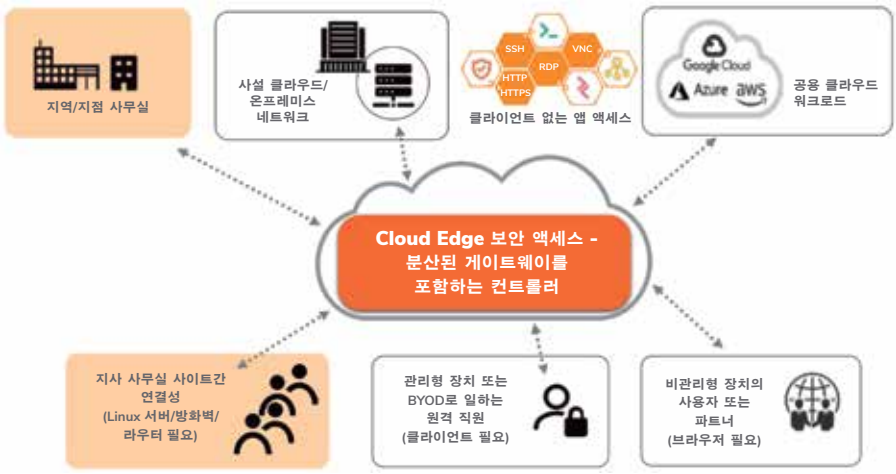

그림 1 – SonicWall Cloud Edge 보안 액세스

장점:

- 분산 엔터프라이즈 및 원격 직원을 위한 보안 솔루션
- 하이브리드 클라우드에서 모든 사이트 및 리소스에 즉시 보안 액세스
- 네트워크, 애플리케이션, 사용자 및 장치 프로필별 제로 트러스트 정책
- 무단 내부 확산 공격을 방지하기 위한 내장형 극세분화
- 사용자를 100명에서 수천명까지 확대
- IT 관리자가 15분만에 구성 가능
- 최종 사용자가 5분 만에 배치 가능
- 사용량 및 대역폭 제한 없음
- 공용 Wi-Fi 보안
- 고성능 WireGuard 암호화
- 클라우드 ID 제공자 통합
- 현대식 SSO 및 MFA 통합
- DDoS, Slowloris, SYN 플러드 차단
- MSSP를 위한 멀티 테넌시
- 준법 감사를 위한 완전한 모니터링 및 보고
- 고객마다 개별적인 전용 클라우드 게이트웨이 및 IP 주소
- 미국, 유럽, 중동, 아시아 지역에서 서비스 이용 가능

전통적인 VPN에서 제로 트러스트 보안으로의 진화

직원들이 어디에서나 일할 수 있고 리소스가 클라우드에 보관되는 디지털 전환 시대에 전통적인 VPN 솔루션은 배치하기에 너무 복잡하고 너무 많은 제약이 있습니다.

일반적인 VPN 배치는 며칠 또는 몇 주가 걸릴 수도 있어서 공급 가용성이 저하되고 다운타임 예약이 어렵습니다.

전통적인 VPN은 또한 성공적으로 로그인한 사용자에게 광범위한 네트워크 액세스를 제공하고 네트워크 서브넷에서 내부 확산 공격을 허용하기 때문에 잠재적인 침해를 위한 백도어를 열어줄 수도 있습니다.

마지막으로 사용자 트래픽이 클라우드로 직접 가는 것이 아니라 온프레미스 VPN 집중장치를 통해 순환하므로 VPN에는 사용자의 클라우드 경험에 부정적 영향을 주는 추가적인 지연이 포함되어 있습니다.

Gartner는 2023년까지 기업의 60%는 ZTNA를 위해 원격 액세스 가상 사설망(VPN)을 폐지할 것으로 예상하고 있습니다.

SonicWall Cloud Edge 보안 액세스는 위에 설명한 문제를 극복하고 다음 3가지의 필수 기능을 갖춘 ZTNA를 제공합니다.

그림 2 – SonicWall Cloud Edge 보안 액세스 기능

주요 사용 사례

신속한 셀프 서비스 배치

- **신속한 배치 –** IT 관리자는 15분만에 로그인하여, 게이트웨이를 인스턴스화하고, 네트워크 및 사용자 컨텍스트를 바탕으로 세부 정책을 구성할 수 있습니다.
- **신속한 사용자 온보딩 –** 최종 사용자는 브라우저를 사용할 수 있는 경우 공용 컴퓨터를 사용하는 동안 모바일 또는 데스크톱 클라이언트 앱을 통해 연결하거나, 클라이언트 설치를 우회하도록 선택할 수 있습니다. 셀프 서비스 배치 모델을 통해 사용자는 5분 이내에 전원을 켜고 실행할 수 있습니다.
- **하이브리드 클라우드에 신뢰성 있는 액세스 –** 배치가 완료되면 사용자는 전 세계 어디에서나 온프레미스 및 공용 클라우드 리소스에 신속하고 간편하며, 안전하게 액세스할 수 있습니다.

신뢰할 수 있는 지역 및 공용 핫스팟 지역에서는 어디에서나 업무 수행 가능

- **자동 Wi-Fi 보안 –** Windows 및 Mac Os용 Cloud Edge 보안 액세스 에이전트 애플리케이션은 공용 핫스팟에서 적극적으로 환경을 모니터링하고 보안 액세스 연결을 자동으로 활성화합니다. 그 결과 데이터 유출과 준법 위반으로 이어질 수 있는 일반적인 Wi-Fi 탈취로부터 사용자를 보호할 수 있습니다.
- **킬 스위치 –** 보안 액세스 연결이 차단되었을 때 잠재적 사이버 침해를 방지하기 위해 장치의 인터넷 연결이 즉시 해제되어 데이터 유출을 방지합니다.
- **신뢰할 수 있는 Wi-Fi 네트워크 –** SSID가 신뢰할 수 있는 것으로 지정되면 자동 Wi-Fi 보안 기능은 활성화되지 않습니다.
- **상시 작동 VPN/애플리케이션 –** 이 편리한 기능은 사용자 또는 장치를 재로그인하거나 재인증하지 않고도 애플리케이션이나 애플리케이션 집합에 자동으로 연결합니다.

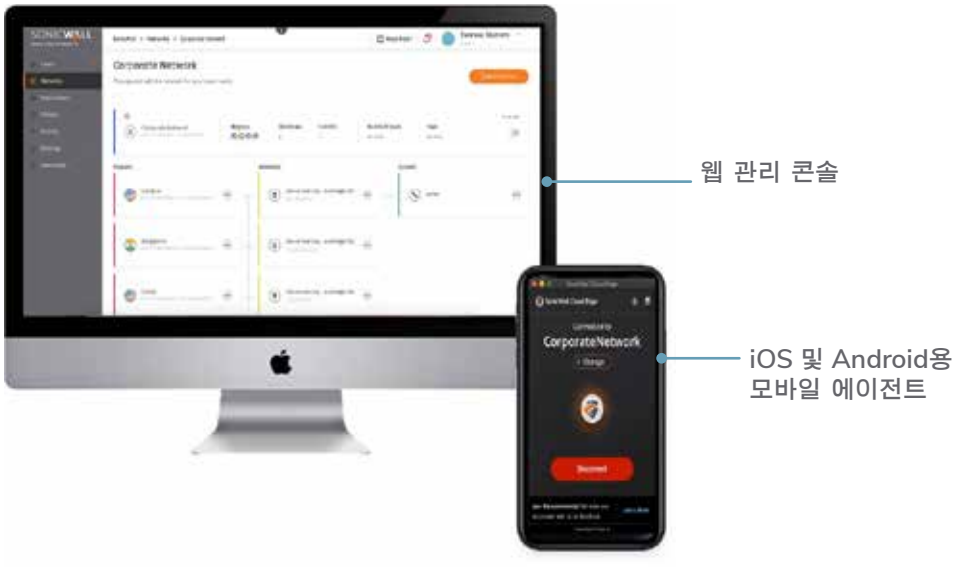

그림 3 – Apple iOS를 위한 SonicWall Cloud Edge 보안 액세스 관리 콘솔 및 모바일 에이전트 애플리케이션

제로 트러스트 애플리케이션 액세스

Cloud Edge 보안 액세스는 기업 리소스를 보호하는 동시에 원격 직원을 활성화하고 권한을 주기 위해 필요한 도구를 디지털 조직에게 제공합니다.

올바른 컨텍스트를 갖춘 외부 사용자는 기업 네트워크를 사이버 위협에 노출시키지 않고 보안 액세스의 제로 트러스트 정책을 통해 원격 데스크톱 및 웹 애플리케이션 호스트에 안전하게 액세스할 수 있습니다.

- **최소 권한 액세스 컨트롤을 철저하게 집행 –** 기업들은 사용자 및 그룹 ID, 액세스하는 데이터의 중요도와 같은 관련 속성을 바탕으로 한 리소스를 사용하여 인터랙션을 제어할 수 있습니다.
- **컨텍스트 중심 –** 이 솔루션은 온프레미스 및 클라우드 호스팅 리소스에 대한 사용자 중심의 정책 기반 액세스를 보장합니다.
- **주요 클라우드 기반 ID 관리 제공자와 통합 –** 기업들은 레거시 온프레미스 자산의 서비스 수명을 연장하거나, 현대적인 클라우드 기반 ID 관리 서비스를 Azure AD, Google Authenticator 및 Okta와 같은 제공업체로부터 마이그레이션할 수 있습니다.
- **극세분화 –** 극세분화는 각각의 유입 트래픽을 정확하게 세분화하여 맬웨어 또는 무단 사용자가 위협을 내부로 확산하지 못하게 함으로써 사이버 공격의 공격 대상과 전반적인 노출을 줄일 수 있습니다.
- **연합된 싱글 사인온 및 다중 인증 –** 이러한 조합은 일관성 있고 완전한 경험을 통해 하이브리드 IT 환경에 들어오는 사용자를 인증하기 위한 단일 포털을 제공합니다.
- **준법 감사 시설 –** 모든 제로 트러스트 액세스 활동은 미래의 감사를 위해 완전하게 모니터링되며 기록됩니다.

그림 4 – SonicWall Cloud Edge 보안 액세스 ZTNA 프로세스

사이트간 상호연결 또는 서비스형 네트워크(NaaS)

Cloud Edge 보안 액세스는 지리적으로 분산된 지사 사무실을 신속하게 온보딩하기 위해 사이트간 연결 서비스 또는 서비스형 네트워크(NaaS)를 제공합니다.

NaaS를 통해 IT 관리자는 비싼 MPLS에 의존하지 않고 모바일 키오스크, 소매 매장, 판매 지점을 클라우드 호스팅 리소스에 신속하고 안전하게 연결할 수 있습니다.

- **사이트간 또는 사이트-클라우드간 상호연결 서비스 –** 이 솔루션은 AWS, Azure, Google Cloud와 같은 유명한 클라우드 환경에 쉽게 연결하거나 다른 장소에 있는 두 네트워크 사이에 안전한 통신 링크를 생성합니다.
- **다지역 배치 –** 관리자들은 해외 지사와 직원을 최적의 속도로 관리하기 위해 다른 장소에 있는 전용 Cloud Edge 게이트웨이를 배치할 수 있습니다.
- **고성능 글로벌 백본 –** SonicWall Cloud Edge 서비스는 전 세계에서 이용할 수 있습니다. 이 인프라는 게이트웨이를 고객의 위치 및 서버 전체의 로드 밸런싱 트래픽 가까이에 배치하여 지연 시간을 최소화합니다.
- **첨단 WireGuard 터널 –** IT 관리자는 IPsec을 사용하는 지사 라우터 또는 방화벽을 사용하여 가장 가까운 Cloud Edge 게이트웨이에 연결할 수 있습니다.

  SonicWall은 최고의 성능을 위해 지사의 Linux 서버가 가까운 게이트웨이로 WireGuard 터널 서비스를 실행하도록 하는 WireGuard 커넥터 기능을 권장합니다.
- **네트워크 감사 및 모니터링 –** 그룹에 대한 가시성과 서버 생성, 팀원 인증, 암호 변경 등을 비롯한 네트워크의 상태, 활동 및 보안에 대한 통찰력을 얻으십시오.

사양

카테고리	기능	장점
확장 및 성능	사용자	100-10000+
	성능	고객 게이트웨이당 1Gbps; 더 많은 게이트웨이로 수평 클라우드 확장
클라우드 플랫폼	클라우드 관리 플랫폼	조직의 네트워크를 간편하게 생성하기 위한 클라우드 관리 플랫폼. 온프레미스 및 클라우드 포함
	신속하고 간편한 네트워크 배치	15분만에 네트워크를 자동으로 배치
	가용성 및 가동 시간	서비스가 자동으로 관리. 현재 Cloud Edge 서비스는 https://status.sonicwall.com/에서 제공합니다.
	로드 밸런싱	SonicWall이 호스팅하고 관리하는 30여 개 글로벌 POP에서 공용/전용 게이트웨이가 제공.
	사이트간 상호연결	두 사이트(온사이트, 오프사이트 또는 클라우드 기반) 사이의 연결성 IPsec 및 WireGuard 지원
	사용자 지정 DNS	터널을 정의하고 내부 DNS 서버를 사용하려면 기본 DNS 대신 사용자 지정 DNS 서버를 정의할 수 있습니다.
	클라이언트 없는 애플리케이션 액세스	HTTP, HTTPS, RDP, VNC, SSH에 제로 트러스트 애플리케이션 액세스
	클라이언트 기반 액세스	Windows, Mac, iOS 및 Android 플랫폼에 사용 가능
	앱 및 환경	하이브리드 환경 및 클라우드 워크로드에 가장 적합
제로 트러스트 기능	상시 작동 애플리케이션	상시 작동 애플리케이션은 신뢰할 수 없는 네트워크에 연결할 때 보안 위협으로부터 보호해주는 안전한 인터넷 액세스를 제공합니다.
	정책 기반 세분화	각 사용자와 애플리케이션에 적용되는 정책
	세분형 액세스 제어 정책	사용자, 애플리케이션, Geo IP, 지리적 위치, 브라우저 유형, OS, 날짜 및 시간 기준
	분할 터널	통과할 사용자 트래픽 서브넷을 결정 가능
	킬 스위치	보안 액세스 연결이 차단되었을 때 잠재적 사이버 침해를 방지하기 위해 장치 인터넷 연결이 즉시 해제되어 데이터 유출을 방지합니다.
	자동 Wi-Fi 보안	특허를 획득한 당사의 기능은 직원이 안전하지 않은 공용 Wi-Fi에 연결할 때 직원의 장치를 자동으로 보호합니다.
	DNS 필터링	네트워크에서 사용자가 인터넷 브라우저를 통해 특정 웹 사이트, 사이트 카테고리, IP 주소 등에 액세스하지 못하도록 차단
인증	싱글 사인온 기능	Okta, G Suite, Azure AD 및 Active Directory LDAP와 같은 싱글 사인온 제공업체를 통해 통일된 로그인을 실행
	2중 인증	내장형 SMS DUO 보안 및 Google Authenticator 2FA 통합으로 원격 공격을 차단
모니터링, 로깅 및 지원	매일 24시간 지원	지원 서비스를 포함한 완전한 관리형 클라우드 솔루션
	행동 감사 및 보고서	로그인, 게이트웨이 배치 및 앱 연결을 모니터링
	SIEM 통합	Splunk와의 간편한 클릭스루 통합을 포함하여 모든 SIEM 애플리케이션에 실시간으로 보안 정보 및 이벤트를 캡처하고, 보관, 전달.
	클라우드 서비스 상태	https://www.sonicwall.com/support를 확인하십시오.
상호운용성	엔터프라이즈 방화벽	SonicWall, Check Point, Fortinet, Palo Alto Networks, WatchGuard, Sophos, Xyxel, UniFi, pfSense, Cisco 및 Untangle
사용자 지정 통합	API 사용 가능	당사의 종합적인 REST 기반 API는 제3자 관리, 자동화, 조율 도구와 신속하고 간편하게 통합할 수 있어서 새로 프로비져닝하거나 재배치한 가상화된 애플리케이션을 보호할 수 있습니다.
규정 준수	ISO 27001 & 27002, SOC-2 타입 2	SOC 2 타입 2 준법 클라우드 인프라
주문	구독	Cloud Edge 보안 액세스 구독에 대한 정보는 해당 MSSP, 리셀러 및 판매자에게 문의해 주십시오.

SonicWall 소개

SonicWall은 초분산 시대와 모든 사람이 원격, 모바일 및 비보안 상태인 업무 현실을 위한 Boundless Cybersecurity를 제공합니다. SonicWall은 알려지지 않은 정보를 파악하고 실시간 가시성을 제공하며 혁신적인 경제성을 제공함으로써 전 세계 기업, 정부 및 중소기업의 사이버 보안 비즈니스 격차를 해소합니다. 자세한 정보는 www.sonicwall.com에서 확인할 수 있습니다.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
기타 정보는 당사의 웹 사이트를 참조하십시오.
www.sonicwall.com

Datasheet-CloudEdge-US-VG-2807