SONICWALL

SonicWall Cloud Edge Secure Access

Einbindung von Zero Trust Security in wenigen Minuten

SonicWall Cloud Edge Secure Access ist ein leistungsstarker Cloud-Dienst, der einfaches Network-as-a-Service für Site-to-Site- und Hybrid-Cloud-Konnektivität mit AWS, Azure, Google Cloud und mehr bietet. Dabei werden Zero-Trust und Least-Privilege Sicherheitsansätze in einem integrierten Angebot kombiniert.

Der Least-Privilege Access-Ansatz beschränkt den Zugriff eines bestimmten Benutzers ausschließlich auf das, was dieser unbedingt benötigt, ähnlich dem „Need-to-Know"-Prinzip. Durch die Einschränkung des Zugangs zu anderen sensiblen Bereichen des Netzwerks können Organisationen ihre Ressourcen sichern, ohne ihre betriebliche Flexibilität zu begrenzen.

SonicWall Cloud Edge Secure Access wendet Zero-Trust Security auf Basis von vier zentralen Sicherheitsmaßnahmen an:

- Überprüfung der Anmeldedaten des Benutzers und des Geräts, auch für den internen Datenverkehr
- Kontextualisierung der Anfrage, um die Authentizität und Einhaltung der Unternehmensrichtlinien sicherzustellen
- Mikrosegmentierung des Netzwerkzugriffs, um die laterale Bewegung von Bedrohungen zu verhindern
- Gewährung des Zugangs nur auf die beantragten Anwendungen und nicht mehr

Kern der Cloud Edge Secure Access-Infrastruktur ist die moderne, auf dem Security-by-Design-Konzept basierende Software-Defined Parameter (SDP)-Architektur.

SDP entkoppelt den Controller, der Benutzer und Geräte authentifiziert, von den als Trust-Broker fungierenden Gateways. Durch die Verteilung der Gateways nahe der Endbenutzer-Standorte kann der Cloud Edge Secure Access-Service schnell erweitert werden, um eine konstant hohe Leistung und das beste Cloud-Erlebnis zu bieten.

Darüber hinaus werden durch die Trennung der Funktionen häufige Cyber-Bedrohungen wie DDoS, Hijacking von öffentlichen WLANs, SYN-Floods und Slowloris effektiv gestoppt und SonicWall wird ermöglicht, eine hochintegrierte Zero-Trust Security-Plattform anzubieten.

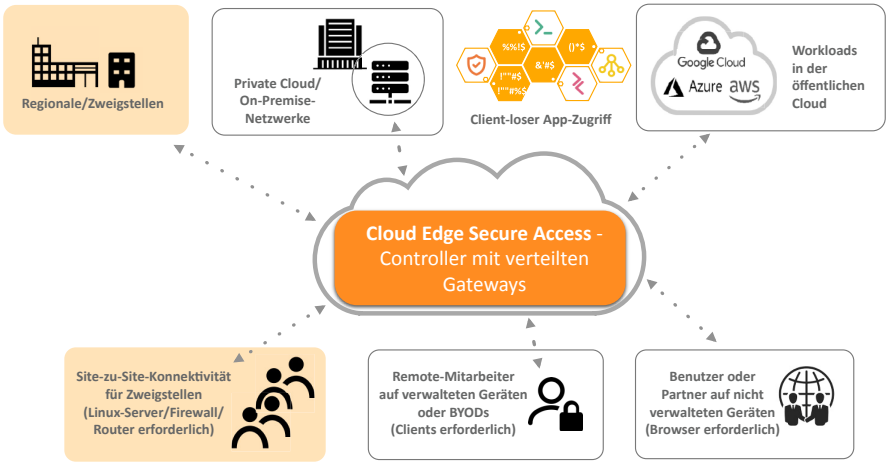

Abbildung 1 – SonicWall Cloud Edge Secure Access

Vorteile:

- Sichert verteilte Unternehmen und Remote-Mitarbeiter
- Sofortiger, sicherer Zugriff auf alle Websites und Ressourcen in Hybrid-Clouds
- Zero-Trust-Richtlinien nach Netzwerken, Anwendungen, Benutzer- und Geräteprofilen
- Integrierte Mikrosegmentierung zur Verhinderung unbefugter lateraler Bewegungen
- Größenordnung für 100 bis Tausende von Benutzern
- Kann in 15 Minuten vom IT-Manager konfiguriert werden
- Kann in 5 Minuten vom Endbenutzer implementiert werden
- Keine Einschränkung hinsichtlich der Nutzung und Bandbreite
- Sicherheit für öffentliches WLAN
- High-Performance WireGuard-Verschlüsselung
- Integration von Cloud Identity Provider
- Moderne SSO- und MFA-Integration
- Stoppt DDoS, Slowloris, SYN-Flood
- Multi-Tenancy für MSSPs
- Umfassende Überwachung und Berichterstattung für Compliance-Audits
- Dedizierte Cloud-Gateways und IP-Adressen für jeden Kunden
- Dieser Service ist in den USA, in Europa, im Nahen Osten und in Asien verfügbar

Evolution vom traditionellen VPN zum Zero-Trust-Sicherheitsmodell

Im Zeitalter der digitalen Transformation, in dem Mitarbeiter von überall aus arbeiten können und Ressourcen in die Cloud verlagert wurden, ist die traditionelle VPN-Lösung zu kompliziert und hat zu viele Einschränkungen.

Eine typische VPN-Einbindung kann Tage oder sogar Wochen in Anspruch nehmen und durch mangelnde Verfügbarkeit sowie die Planung für lange Ausfallzeiten behindert werden.

Das herkömmliche VPN kann auch Hintertüren für mögliche Einbrüche öffnen, da jede erfolgreiche Anmeldung einem Benutzer breiten Netzwerkzugriff gewährt und eine laterale Bewegung innerhalb des Subnetzes ermöglicht wird.

Des Weiteren bringt das VPN zusätzliche Latenz mit sich, die das Cloud-Erlebnis der Benutzer verschlechtert, da der Benutzerverkehr durch den On-Premise-VPN-Konzentrator anstatt direkt in die Cloud geleitet wird.

Gartner prognostiziert, dass bis 2023 60 % der Unternehmen die meisten ihrer Remote Access Virtual Private Networks (VPNs) zugunsten von ZTNA außer Betrieb setzen werden.

SonicWall Cloud Edge Secure Access löst die oben beschriebenen Probleme und bietet ZTNA mit diesen drei wichtigen Fähigkeiten:

Least-Privilege-Zugang zum Schutz der Vermögenswerte des Unternehmens

Schnelle Bereitstellung und Self-Service-Modell

Direkter und zuverlässiger Cloud-Zugang von überall

Abbildung 2 – SonicWall Cloud Edge Secure Access Fähigkeiten

Primäre Anwendungsfälle

Schnelle Bereitstellung und Self-Service-Modell

- **Schnelle Bereitstellung –** In weniger als 15 Minuten kann sich ein IT-Manager anmelden, ein Gateway installieren und granulare Richtlinien basierend auf den Netzwerken und dem Benutzerkontext konfigurieren.
- **Schnelles Onboarding neuer Benutzer –** Ein Endbenutzer hat die Wahl, sich über eine mobile oder Desktop-Client-App zu verbinden oder die Client-Installation komplett zu umgehen, wenn er einen öffentlichen Computer nutzt und ein Browser verfügbar ist. Mit dem Self-Service-Modell kann ein Benutzer in 5 Minuten einsatzbereit sein.
- **Zuverlässiger Zugriff auf die Hybrid-Cloud –** Nach der Implementierung haben Benutzer von überall auf der Welt schnellen, einfachen und sicheren Zugriff auf On-Prem- und Public-Cloud-Ressourcen.

Work-from-Anywhere-Schutz in vertrauten und öffentlichen Hotspot-Bereichen

- **Automatische WLAN-Sicherheit –** Cloud Edge Secure Access Agent-Anwendungen für Windows und Mac OS überwachen proaktiv die Umgebung und aktivieren automatisch eine sichere Zugangsverbindung in öffentlichen Hotspot-Bereichen. Dies schützt Benutzer vor allzu häufigen WLAN-Abhörvorgängen, die zu Datendiebstählen und Compliance-Verstößen führen können.
- **Not-Aus-Schalter –** Wenn eine sichere Verbindung unterbrochen wird und ein potenzieller Cybereinbruch verhindert werden muss, wird die Internetverbindung des Geräts sofort abgebrochen, um zu verhindern, dass Daten das Gerät verlassen.
- **Vertrauenswürdige WLAN-Netzwerke –** Wenn eine SSID als vertrauenswürdig gekennzeichnet ist, wird die automatische WLAN-Sicherheitsfunktion nicht aktiviert.
- **Always-on-VPN/Anwendungen –** Diese praktische Funktion verbindet einen Benutzer oder ein Gerät automatisch erneut mit der Anwendung oder einer Reihe von Anwendungen, ohne dass eine erneute Anmeldung oder eine erneute Authentifizierung erforderlich ist.

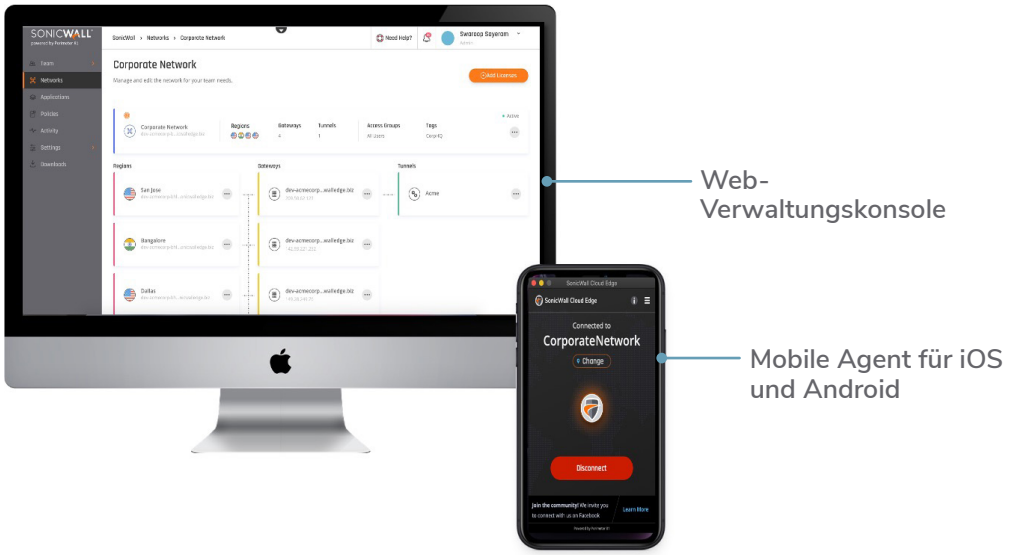

Abbildung 3 – SonicWall Cloud Edge Secure Access Managementkonsole und Mobile Agent-Anwendung für Apple iOS

Zero-Trust-Zugriff auf Anwendungen

Cloud Edge Secure Access bietet digitalen Unternehmen ein dringend benötigtes Tool für den Schutz der Unternehmensressourcen und die Aktivierung und Befähigung von Remote-Mitarbeitern.

Mit den Zero-Trust-Richtlinien von Secure Access können externe Benutzer mit dem entsprechenden Kontextbezug sicher auf eine Vielzahl von Remote-Desktop- und Webanwendungen zugreifen, ohne das Unternehmensnetzwerk an potenzielle Cyberbedrohungen auszusetzen.

- **Least-Privilege Access-Kontrolle wird strikt durchgesetzt –** Organisationen können Interaktionen mit Ressourcen anhand relevanter Attribute kontrollieren, einschließlich der Benutzer- und Gruppenidentität und der Sensibilität der abgerufenen Daten.
- **Kontextgesteuert –** Die Lösung gewährleistet benutzerorientierten und richtlinienbasierten Zugriff auf On-Premise- und Cloud-gehostete Ressourcen.
- **Integration mit führenden Cloud-basierten Identity-Management-Anbietern –** Unternehmen können das Dienstleben von bestehenden On-Premise-Assets verlängern oder auf moderne, Cloud-basierte Identity-Management-Dienste von Anbietern wie Azure AD, Google Authenticator und Okta umstellen.
- **Mikrosegmentierung –** Durch die präzise Segmentierung jedes eingehenden Datenverkehrs verhindert die Mikrosegmentierung, dass sich Malware oder unbefugte Benutzer lateral bewegen, wodurch die Angriffsfläche und die Aussetzung an Cyberbedrohungen insgesamt reduziert werden.
- **Föderiertes Single-Sign-On und Multifaktor-Authentifizierung –** Durch diese Kombination wird ein zentrales Portal für die Authentifizierung von Benutzern bei der Anmeldung in einer hybriden IT-Umgebung und eine einheitliche, nahtlose Benutzererfahrung bereitgestellt.
- **Compliance Audit-Einrichtung –** Jede Zero-Trust Access-Aktivität wird vollständig überwacht und für zukünftige Audits aufgezeichnet.

Abbildung 4 – SonicWall Cloud Edge Secure Access ZTNA-Prozess

Site-to-Site-Konnektivität oder Network-as-a-Service (NaaS)

Cloud Edge Secure Access bietet Site-to-Site-Konnektivitätsdienste oder Network-as-a-Service (NaaS) für ein schnelles Onboarding von Zweigstellen an geografisch weit verteilten Standorten.

Mit NaaS kann ein IT-Manager mobile Kioske, Einzelhandelsgeschäfte und Verkaufsstellen schnell und sicher mit Cloud-gehosteten Ressourcen verbinden, ohne sich auf teure MPLS verlassen zu müssen.

- **Site-to-Site- oder Site-to-Cloud-Konnektivitätsdienst –** Die Lösung ermöglicht eine einfache Verbindung zu beliebten Cloud-Umgebungen wie AWS, Azure und Google Cloud oder stellt eine sichere Kommunikationsverbindung zwischen zwei verschiedenen Netzwerken an verschiedenen Standorten her.
- **Multiregionale Bereitstellung –** Administratoren können dedizierte Cloud Edge-Gateways an verschiedenen Standorten einsetzen, um internationale Niederlassungen und Mitarbeiter mit optimaler Geschwindigkeit zu versorgen.
- **Leistungsstarkes globales Backbone –** Der SonicWall Cloud Edge-Service ist weltweit verfügbar. Die Infrastruktur zeichnet sich durch eine minimale Latenz aus, da Gateways nahe den Kundenstandorten verteilt sind und der lastverteilte Verkehr über Server geleitet wird.
- **Moderner WireGuard-Tunnel –** Ein IT-Manager kann alle Zweigrouter oder Firewalls mittels IPsec einsetzen, um die Verbindung mit dem nächstgelegenen Cloud Edge Gateway herzustellen.

  Für höchste Leistung empfiehlt SonicWall die WireGuard Connector-Funktion, für die ein Linux-Zweigstellenserver benötigt wird, um den WireGuard-Tunneldienst mit dem nächstgelegene Gateway zu verbinden.
- **Netzwerk-Audit und -Überwachung –** Gewinnen Sie mehr Einblick in Zustand, Aktivität und Sicherheit Ihres Netzwerks sowie Einsicht in die Gruppen- und Servererstellung, die Authentifizierung von Teammitgliedern, Kennwortänderungen und mehr.

Technische Daten

Kategorie	Funktion	Vorteile
Skalierung und Leistung	Benutzer	100 - 10.000+
	Leistung	1 Gbit/s pro Kunden-Gateway; horizontale Cloud-Skalierung mit mehr Gateways
Cloud-Plattform	Cloud-Managementplattform	Cloud-Managementplattform zur einfachen Erstellung des Netzwerks Ihrer Organisation On-Premise und On-Cloud sind enthalten
	Schnelle und einfache Netzwerkbereitstellung	Automatische Bereitstellung Ihres Netzwerks in weniger als 15 Minuten
	Verfügbarkeit und Betriebszeit	Automatische Verwaltung durch den Dienst Aktueller Cloud Edge-Servicestatus auf https://status.sonicwall.com/
	Lastverteilung	Bereitstellung durch gemeinsame/dedizierte Gateways über 30 globale POPs, die von SonicWall gehostet und verwaltet werden
	Site-to-Site-Konnektivität	Konnektivität zwischen zwei Standorten (vor Ort, außerhalb oder Cloud-basiert). Unterstützt IPsec und WireGuard
	Benutzerdefinierter DNS-Server	Bei Verwendung Ihrer internen DNS-Server können Sie nach der Definition eines Tunnels auch einen benutzerdefinierten DNS-Server bestimmen, anstatt den Standard-DNS zu verwenden
	Client-loser Zugriff auf Anwendungen	Zero Trust-Zugriff auf Anwendungen auf HTTP, HTTPS, RDP, VNC, SSH
	Client-basierter Zugriff	Verfügbar für Windows-, Mac-, iOS- und Android-Plattformen
	Apps und Umgebung	Bestens geeignet für hybride Umgebungen und Cloud-Workloads
Zero-Trust-Fähigkeiten	Always-on-Anwendungen	Always-on-Anwendungen bieten sicheren Zugriff auf das Internet, wenn über ein nicht vertrautes Netzwerk verbunden wird, und sie bieten Schutz vor Sicherheitsbedrohungen
	Richtlinienbasierte Segmentierung	Pro Benutzer und pro Anwendung angewendete Richtlinien
	Richtlinien für die granulare Zugangskontrolle	Basierend auf Benutzer, Anwendung, Geo-IP, Standort (Land), Browsertyp, Betriebssystem, Datum und Uhrzeit
	Split-Tunneling	Ermöglicht die Wahl des Subnetzes, durch das der Verkehr geleitet werden soll
	Not-Aus-Schalter	Wenn eine sichere Verbindung unterbrochen wird und ein potenzieller Cybereinbruch verhindert werden muss, wird die Internetverbindung des Geräts sofort abgebrochen, um zu verhindern, dass Daten das Gerät verlassen.
	Automatische WLAN-Sicherheit	Unsere patentierte Funktion schützt die Geräte der Mitarbeiter automatisch, wenn sie sich mit einem ungesicherten öffentlichen WLAN verbinden
	DNS-Filterung	Blockiert den Zugriff der Benutzer auf bestimmte Websites, Website-Kategorien und IP-Adressen mittels Internetbrowser
Authentifizierung	Single-Sign-On-Fähigkeit	Implementierung eines einheitlichen Logins über Single Sign-On-Anbieter wie Okta, G Suite, Azure AD und Active Directory LDAP
	Zwei-Faktor-Authentifizierung	Verhindert Remote-Angriffe durch integrierte SMS, DUO Security und Google Authenticator 2FA-Integration
Überwachung, Protokollierung und Support	24/7 Support	Vollständig verwaltete Cloud-Lösung inklusive Support
	Aktivitäts-Audits und Berichte	Überwachung von Anmeldungen, Gateway-Bereitstellungen und App-Verbindungen
	SIEM-Integration	Erfassung, Speicherung, Bereitstellung von Sicherheitsinformationen und -ereignissen in Echtzeit für alle SIEM-Anwendungen sowie Click-through-Integration mit Splunk
	Cloud-Service-Status	Weitere Informationen auf https://www.sonicwall.com/support
Interoperabilität	Enterprise Firewall	SonicWall, Check Point, Fortinet, Palo Alto Networks, WatchGuard, Sophos, Xyxel, UniFi, pfSense, Cisco und Untangle
Bedarfsgerechte Integrationen	API verfügbar	Unsere umfassende REST-basierte API ermöglicht eine schnelle und einfache Integration mit Management-, Automatisierungs- und Orchestrierungswerkzeugen von Drittanbietern und gewährleistet Schutz für neu bereitgestellte oder verlagerte virtualisierte Anwendungen
Konformität	ISO 27001 und 27002, SOC-2 Typ 2	SOC 2 Typ 2-konforme Cloud-Infrastruktur
Bestellung	Aboservice	Kontaktieren Sie Ihren MSSP, Wiederverkäufer und Distributor, um das Cloud Edge Secure Access-Abonnement zu bestellen

Über SonicWall

SonicWall bietet Boundless Cybersecurity für das hyperverteilte Umfeld einer neuen Arbeitsrealität, in der jeder remote, mobil und ungeschützt ist. Indem SonicWall das Unbekannte kennt, Echtzeit-Transparenz und skalierbare Ökonomien ermöglicht, werden Cybersicherheitslücken bei Unternehmen, Regierungen und KMU weltweit geschlossen. Weitere Informationen finden Sie auf www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com

Datasheet-CloudEdge-US-VG-2807

SONICWALL®