DATENBLATT

Cloud Secure Edge

Remote-Zugriff bei höherer Sicherheit

Bei SonicWall Cloud Secure Edge™ handelt es sich um eine moderne cloudnative Security-Service-Edge(SSE)-Lösung, die ältere, eingeschränkte Netzwerk-Appliances ablöst und mit einem zentralisierten und skalierbaren Ansatz für einen sicheren Zugriff sorgt. Sie ermöglicht es Organisationen mit unterschiedlichsten Nutzern (Mitarbeitern, Auftragnehmern, Dritten etc.), von beliebigen Geräten und Standorten aus nahtlos und sicher interne und internetbasierte Ressourcen aufzurufen.

Weil zentrale Netzwerk- und Sicherheitsfunktionen wie Remote-Access-VPN, Web-Proxy und Firewalls in einer einzigen cloudbasierten Plattform zusammengefasst werden, stärkt Cloud Secure Edge Ihr Sicherheitskonzept und erlaubt eine proaktive Sicherheitsstrategie – ganz ohne Unterbrechungen für die Endanwender.

Hinweis: Kunden, die bereits Gen-7- oder neuere Firewalls von SonicWall nutzen, können diese out of the box mit Cloud Secure Edge verknüpfen und Zugriffsregeln ganz unkompliziert über ein einheitliches Dashboard verwalten.

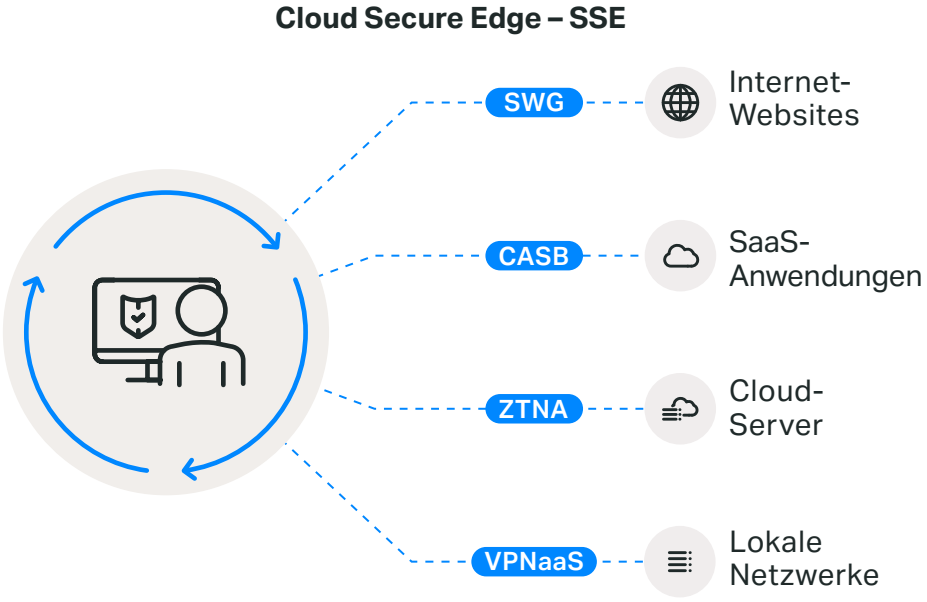

Abbildung 1: SonicWall Cloud Secure Edge bietet von jedem beliebigen Gerät aus einen sicheren Zugriff auf sämtliche Ressourcen.

Was spricht für SonicWall Cloud Secure Edge?

Leichte Verwaltung und Implementierung
Sie können Cloud Secure Edge als Stand-alone-Lösung nutzen oder im Rahmen eines Monatsabonnements zu Ihren bestehenden Gen-7- oder neueren Firewalls von SonicWall hinzufügen. Die Lösung ist ideal für MSPs und Organisationen mit eigenen IT-Teams, die nicht genügend Ressourcen haben und auf der Suche nach niedrigen Gesamtbetriebskosten und einem schnellen ROI sind. Nach dem erstmaligen Einloggen in Cloud Secure Edge können Administratoren in drei geführten Schritten ihren ersten sicheren VPNaaS-Tunnel einrichten und so die Time to Value verkürzen.

Schutz vor Bedrohungen
Cloud Secure Edge umfasst Zero-Trust-Sicherheitskontrollen. Diese sind wichtig für hybride und Remote-Teams, die einen Zugang zu sensiblen internen und internetbasierten Ressourcen brauchen, um von überall aus ihre Aufgaben erledigen zu können. Die Lösung nutzt eine einzigartige Technologie auf Basis von geräte- und identitätsbasiertem Trust-Scoring und kurzlebigen kryptografischen Schlüsseln und sorgt so für eine branchenführende Sicherheit bei exzellenter Benutzererfahrung.

Hohe Performance bei zuverlässigem Datenschutz
Cloud Secure Edge wurde von Grund auf mit besonderem Augenmerk auf eine hohe Performance und einen zuverlässigen Datenschutz konzipiert. Administratoren behalten die volle Kontrolle über ihre Daten, während User von einer möglichst intuitiven und effizienten Verbindung für ein Höchstmaß an Produktivität, Datenschutz und Privatsphäre profitieren.

Gängige Use-Cases

Modernisierung des VPN-/FW-Konzepts mit ZTNA
Anstatt sich beim Schutz von Unternehmensressourcen auf rudimentäre Tools wie Firewalls und veraltete VPNs zu verlassen, sorgt Cloud Secure Edge für einen Least-Privilege-Zugriff auf spezifische Anwendungen und Server. Dieser basiert einerseits auf echtzeit- und kontextbasierten Faktoren zur Vertrauenswürdigkeit von Benutzern und Geräten und andererseits auf der Empfindlichkeit der Ressourcen.

Die cloudbasierte Lösung kann entweder unabhängig oder in Kombination mit bestehenden Sicherheitsinfrastrukturen eingesetzt werden.

Schutz vor internen Bedrohungen und der Kompromittierung von Anmeldedaten
SonicWall hat weltweit leistungsstarke Edge-PoPs implementiert, um ein möglichst effizientes und direktes Routing sicherzustellen. Gleichzeitig schützen einheitliche Umsetzungskontrollen vor Angriffen und Risiken jeglicher Art. Das Ergebnis ist ein einfacher und effektiver Schutz vor Phishing-Angriffen und bösartigen Websites. Bei Bedarf wird auch Content-Filterung angewendet und die Gerätesicherheit wird im Vorfeld geprüft, bevor ein Zugriff gewährt wird – genauso, wie es sein sollte.

Schutz bei Usern mit hohem Risiko (Dritte/ BYOD/Auftragnehmer)
Sie können Dritten einen einfachen, sicheren Zugriff auf genau die Ressourcen bieten, die sie benötigen, ohne zu viele Daten bereitzustellen. Mit Cloud Secure Edge erfolgt der Zugriff nicht nur auf Basis des Sicherheitsstatus von Benutzer und Gerät; die Position und Befugnisse des Nutzers spielen ebenso eine Rolle. Auch die Verwaltung ist ein Kinderspiel: Gruppen und Rollen können vorab identifiziert und nach Bedarf von einer zentralen Konsole aus angewendet werden. Dabei ist es zu keinem Zeitpunkt nötig, Hardware zu patchen oder zu konfigurieren.

Lizenzierung

Cloud Secure Edge kann als Secure Private Access (sicherer privater Zugriff auf interne Netzwerke) und Secure Internet Access (sicherer Internetzugriff auf Ressourcen im öffentlichen Web) erworben werden.

1. **Secure Private Access bietet zwei Kernfunktionen:**
   - Tunnelbasiertes ZTNA (auch Cloud-VPN oder VPNaaS genannt): sicherer Netzwerkzugriff auf spezifische Netzwerksegmente.
     Proxybasiertes ZTNA: sicherer Zugriff auf private Ressourcen wie interne HTTP-Anwendungen und TCP-Services.

2. **Secure Internet Access bietet die folgenden Kernfunktionen:**
   - Cloud-Access-Security-Broker (CASB): Umsetzung von Device-Trust-Richtlinien für den Zugriff auf SaaS-Anwendungen.
   - Secure Web Gateway (SWG): Filterung von Webinhalten, um Malware und andere Bedrohungen im verschlüsselten Webverkehr zu blockieren.

Secure Private Access (SPA) und Secure Internet Access (SIA) sind je in zwei Ausführungen erhältlich: Basic und Advanced. Lizenzen werden pro Benutzer verkauft.

Allgemeine Funktionen

High-Performance-Data-Plane
Dynamische Edge-Architektur für schnelle und zuverlässige Verbindungen für Nutzer weltweit

Native Unterstützung für alle Client-Betriebssysteme
Desktop (Windows, macOS, Linux) und Mobilgeräte (iOS, Android, ChromeOS)

Cloud-Management-Schnittstelle
Zur Konfigurierung von Zero-Trust-Verbindungen durch IT- und Security-Admins

Trust-Scoring
Messung der Verlässlichkeits- und Risikostufen für Nutzer und Geräte

Aussagekräftige Einblicke
Umfassender Überblick über das Risiko von Benutzern/Geräten und Anwendungen/Ressourcen

Kontinuierliche Regeldurchsetzung
Basierend auf der Empfindlichkeit von Ressourcen, unabhängig vom Benutzerstandort

Integrationen
Integration mit bestehenden Tools (IDP, EDR, MDM, SIEM)

SonicWall-Firewall-Konnektor
Out-of-the-Box-Integration mit Gen-7- und neueren Firewalls im Global Mode bei 7.1.2+

Verwaltung mehrerer Nutzer
Cloudbasierte Richtlinien für die Verwaltung mehrerer Nutzer

Benutzer und Geräte

Single-Sign-on
Unternehmensinternes SSO mit Just-in-Time(JIT)-Benutzererstellung

Verwaltung des Status
Analyse des Gerätezustands, darunter Firewall, Festplattenverschlüsselung, Bildschirmsperre, OS-Version etc.

Vertrauensbasierte Profile
Anpassung von Faktoren und Regelauswirkungen basierend auf Benutzer- und Gerätegruppen

Benutzerdefinierte Problembehebung
Konfiguration von Anweisungen zur Problembehebung beim Gerätezustand, z. B. Nachrichten und Links für Endbenutzer

Transparenz und Compliance

Echtzeit-Event-Stream
Echtzeitüberwachung der Benutzer- und Geräteaktivität

Berichte zum Gerätezustand
Nachverfolgung aller (verwalteten und unverwalteten) Geräte, die auf Unternehmensressourcen zugreifen, inklusive deren Sicherheitsstatus

Berichte zu den Administratoraktivitäten
Protokollierung aller Administratoraktivitäten im Cloud-Command-Center

Prozesse und Automatisierung

RESTful-API
RESTful-Endpunkt zur Konfiguration von CSE-Objekten in der Kontrollebene

API-Clients – pybanyan, Terraform
Python-Bibliothek und Terraform für Automatisierung und Verwaltung

Vollautomatische Geräteregistrierung
Roll-out der CSE-App auf Ihre Geräteflotte, ohne dass eine Interaktion mit dem Endbenutzer nötig ist

SONICWALL

	Secure Private Access		Secure Internet Access	
FEATURE	BASIC	ADVANCED	BASIC	ADVANCED
Sicherer Netzwerkzugriff				
ZTNA-Tunnel (VPNaaS) für einen Zugriff auf spezifische Netzwerke	●	●		
ZTNA-Proxy für eine sichere Anbindung an interne HTTP-Anwendungen und TCP-Services		●		
Private Netzwerke (RFC-1918-Bereiche) und Domains (interne DNS-Server)	●	●		
Split Tunneling für spezifische Subnetze und Domains (privat oder öffentlich)	●	●		
Full Tunneling für den gesamten Traffic mittels Private Edge		●		
Netzwerk-/Layer-4-Richtlinien auf Basis von CIDRs und FQDNs	●	●		
Sicherer Zugriff auf private Ressourcen				
Zugriff auf interne Websites unter Nutzung von OpenID-Connect-Flows ausschließlich für Browser		●		
SSH für Linux-Server		●		
RDP für Windows-Geräte		●		
Native Clients für den Zugriff auf Datenbank-Server wie PostgreSQL und MySQL		●		
Kubernetes-Client für den Zugriff auf Cluster		●		
Authentifizierung über SSH-Zertifikate, Autorisierung von Principals und Audit-Logging		●		
Layer-7-Richtlinien für den Zugriff auf APIs, Webseiten		●		
Schutz vor Internetbedrohungen				
Sicherheit auf DNS-Ebene, wobei Domains mit Malware, Phishing-Aktivitäten, Botnets und anderen Risiken blockiert werden			●	●
Content-Kategorisierung			●	●
Benutzerdefiniertes Blockieren			●	●
SaaS-Anwendungssicherheit				
Cloud-Access-Security-Broker (CASB) zur Durchsetzung von Device-Trust-Richtlinien für SaaS-Anwendungen				●
Einblick in Cloud-Anwendungen/Schatten-IT				●
IP-Freigabelisten für Cloud-Anwendungen über SonicWall Edge	●	●		●
Device-Trust für Okta				●
Device-Trust für Azure AD				●
Device-Trust für andere IDPs wie OneLogin, JumpCloud				●
Web-Content-Filtering-Service				
Secure Web Gateway (SWG) | Content-Filterung über DNS			●	●
Secure Web Gateway (SWG) | Bedrohungsfilterung über DNS			●	●
Secure Web Gateway (SWG) | Risikobasierte URL-Filterung				●
Secure Web Gateway (SWG) | Geo-IP-Filterung				●
Benutzer und Geräte				
Passwortlose Authentifizierung über IDP-Federation		●		●
Regelbasierter Zugriff von nicht registrierten Geräten mit einem vertrauenswürdigen Gerätezertifikat		●		●
Clientloser Zugriff		●		●
Servicekonten (API-Token für programmatischen Zugriff wie Scripting und Automatisierung über die Datenebene)		●		
SCIM-Integration zur Verwaltung von Benutzerzuweisungen		●		●

SONICWALL

EDR-Integrationen (z. B. CrowdStrike, SentinelOne, Microsoft Defender)		●		●
MDM-/UEM-Integrationen (z. B. JAMF, Kandji, JumpCloud, Intune, Workspace One)		●		●
Transparenz und Compliance				
SIEM-Integration (z. B. Splunk, Elastic, Sumo Logic)	●			●
Erkennung privater Netzwerke (nicht genehmigte Anwendungen, die von Nutzern oder Geräten aufgerufen werden)	●			n/a
Erkennung von IaaS-Ressourcen	●			n/a
Erkennung von SaaS-Anwendungen	n/a			●
Prozesse und Automatisierung				
Private-Edge-Implementierung: Hosting eines identitätsbasierten SonicWall-Gateways in Ihrer eigenen Infrastruktur		●	n/a	n/a
Services und Support				
24/7-Support	●	●	●	●
Premier-Support		Add-on		Add-on
Remote-Implementierungsservices		Add-on		Add-on

Zusammenfassung

SonicWall Cloud Secure Edge ist eine bahnbrechende, über die Cloud bereitgestellte SSE-Lösung, die weitaus mehr kann, als veraltete Perimeter-Appliances abzulösen. Mit ihrem skalierbaren, modernen Ansatz sorgt sie für sichere Verbindungen zwischen Nutzern, dem Internet und internen Ressourcen. Sie prüft kontinuierlich User, Geräte, Anwendungen und Ressourcen und bietet so Mitarbeitern und Dritten einen echten, standortunabhängigen Zero-Trust-Zugriff.

Cloud Secure Edge wird einfach über die SonicWall-Firewalls implementiert und unterstützt Multi-Tenant-Management, das auf kleine wie große Unternehmen sowie deren MSPs zugeschnitten ist. Mit Cloud Secure Edge können Organisationen effektiv Sicherheitslücken schließen, eine überragende Benutzererfahrung bieten und einen proaktiven, risikominimierten Netzwerk- und Sicherheitsansatz umsetzen. Sind Sie bereit, den Zugriff über Ihre gesamte Organisation hinweg zu verbessern und sicherer zu gestalten? Sprechen Sie heute noch mit unserem Team oder fordern Sie eine Demo an.

Kontaktieren Sie Ihren Account-Manager, wenn Sie Cloud Secure Edge zu Ihren bestehenden SonicWall-Gen-7-Firewalls hinzufügen möchten.

SonicWall Inc.

1033 McCarthy Boulevard | Milpitas, Kalifornien 95035, USA | Weitere Informationen erhalten Sie auf unserer Website.