Cloud Secure Edge

Accesso remoto, migliore sicurezza

SonicWall Cloud Secure Edge™, già noto come Banyan Security, è una soluzione Security Service Edge (SSE) altamente efficace e semplice da adottare che consente alla forza lavoro di accedere in sicurezza a qualsiasi risorsa da qualsiasi dispositivo. Offre un accesso Zero Trust semplice e sicuro a risorse private e internet per tutti i dipendenti e terze parti, indipendentemente dalla loro posizione di rete.

Combina le funzionalità di più appliance di rete tradizionali – VPN di accesso remoto, proxy web, firewall e altro ancora – in un'unica soluzione basata sul cloud, migliorando la postura di sicurezza e l'esperienza d'uso dell'intera forza lavoro.

Nota: i clienti che già utilizzano i firewall SonicWall Gen 7 possono collegarli direttamente a Cloud Secure Edge e gestire le policy di accesso tramite un dashboard unificato.

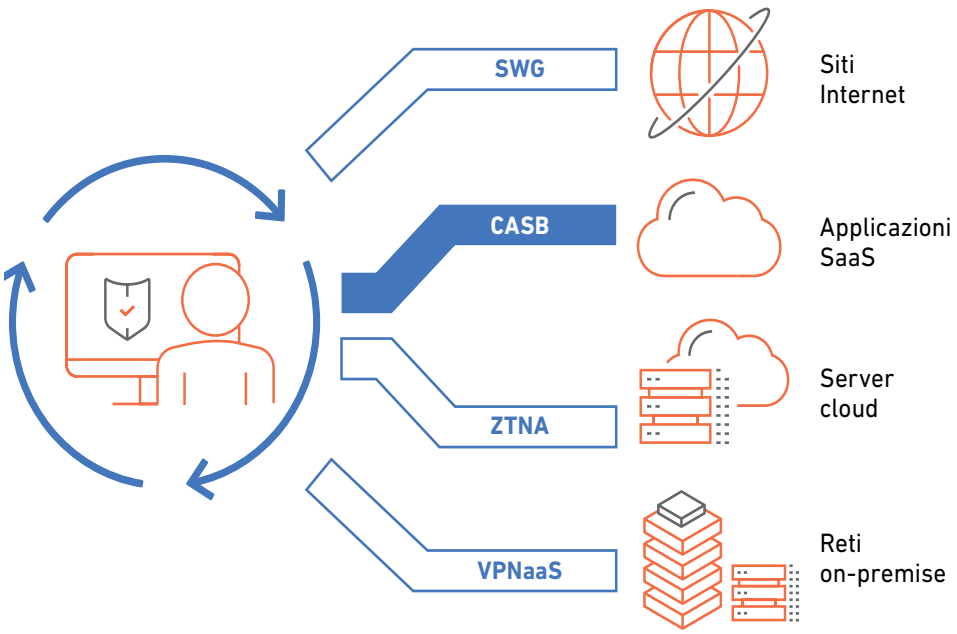

Figura 1: SonicWall Cloud Secure Edge protegge l'accesso a qualsiasi risorsa da qualsiasi dispositivo

SCHEDA TECNICA

Perché SonicWall Cloud Secure Edge?

FACILE DA IMPLEMENTARE E GESTIRE

Cloud Secure Edge può essere utilizzato come soluzione autonoma o aggiunto ai firewall SonicWall Gen 7 come abbonamento mensile. È ideale per gli MSP e per organizzazioni dotate di un team IT interno che dispongono di risorse limitate e sono alla ricerca di un basso TCO e di un rapido ritorno sull'investimento.

PROTEZIONE DALLE MINACCE ATTUALI

Cloud Secure Edge include i controlli di sicurezza Zero Trust necessari per consentire alla forza lavoro ibrida e remota di accedere alle risorse private e internet sensibili di cui ha bisogno per svolgere il proprio lavoro da qualsiasi luogo. Utilizza una tecnologia esclusiva basata su punteggi di attendibilità, incentrati sui dispositivi e sull'identità, e sulla crittografia a breve termine per garantire una protezione leader di settore combinata a un'esperienza d'uso eccellente.

PRESTAZIONI E PRIVACY

Cloud Secure Edge è stato creato appositamente per offrire prestazioni elevate garantendo al contempo la privacy. L'amministratore ha il pieno controllo dei dati e può fornire agli utenti la connessione più naturale ed efficiente possibile per garantire il massimo livello di produttività, protezione dei dati e privacy.

Casi d'uso comuni

Modernizzare le VPN e i firewall con ZTNA

Anziché affidarsi a strumenti generici come firewall e VPN legacy per proteggere le risorse aziendali, Cloud Secure Edge consente l'accesso con privilegi minimi ad applicazioni e server specifici in base a fattori contestuali combinati di attendibilità dell'utente e del dispositivo e alla sensibilità delle risorse, il tutto in tempo reale.

È basato sul cloud e può essere utilizzato in modalità autonoma o in combinazione con infrastrutture di sicurezza preesistenti.

Proteggersi dalle minacce di Internet e dalla compromissione delle credenziali

SonicWall ha distribuito punti di presenza (PoP) edge globali ad alte prestazioni per garantire un instradamento più efficiente e diretto, applicando controlli coerenti per proteggere da qualsiasi tipo di attacco o esposizione a rischi. Questo offre una protezione semplice ed efficace contro attacchi di phishing e siti web malevoli e consente di applicare il filtraggio dei contenuti desiderati e verificare la sicurezza dei dispositivi prima dell'accesso, così come dovrebbe essere.

Proteggere gli utenti ad alto rischio (terze parti / BYOD / nuove acquisizioni)

Consente di offrire a terze parti un accesso semplice e sicuro alle risorse specifiche di cui hanno bisogno senza il rischio di un provisioning eccessivo. Cloud Secure Edge garantisce l'accesso non solo in base alla postura di sicurezza dell'utente e del dispositivo, ma anche in base al suo ruolo e a quello che è autorizzato a visualizzare. La gestione è semplice grazie a gruppi e ruoli che possono essere preidentificati e applicati a seconda delle necessità da una console centrale. Non occorre applicare patch o configurare l'hardware.

Licenze

Cloud Secure Edge è disponibile per l'acquisto nelle varianti Secure Private Access (risorse sulle reti interne) e Secure Internet Access (risorse sull'Internet pubblico).

1. Secure Private Access offre due funzionalità principali:
   - ZTNA basato su tunnel (noto anche come Cloud VPN o VPNaaS): accesso sicuro a segmenti di rete specifici.
   - ZTNA basato su proxy: accesso sicuro a risorse private come applicazioni HTTP interne e servizi TCP.
2. Secure Internet Access offre tre funzionalità principali:
   - DNS-Layer Security (DNS): protezione dalle minacce a livello di dominio che blocca i domini dannosi e applica policy di utilizzo accettabili.
   - Cloud Access Security Broker (CASB): applicazione di policy di attendibilità dei dispositivi per l'accesso alle applicazioni SaaS.
   - Secure Web Gateway (SWG): filtraggio dei contenuti web per bloccare malware e altre minacce nascoste nel traffico web crittografato.

Le soluzioni Secure Private Access (SPA) e Secure Internet Access (SIA) sono disponibili in due livelli: Basic e Advanced. Le licenze vengono vendute per utente.

Funzionalità comuni

Piano di dati ad alte prestazioni

Architettura edge dinamica per connessioni rapide e affidabili con utenti in tutto il mondo

Supporto nativo per tutti i sistemi operativi client

Versione desktop (Windows, macOS, Linux) e mobile (iOS, Android, ChromeOS)

Interfaccia di gestione cloud

Consente agli amministratori IT e di sicurezza di configurare una connettività Zero Trust

Punteggi di attendibilità

Quantificano il livello di affidabilità e di rischio associato a utenti e dispositivi

Visibilità immediata

Vista completa del rischio di utenti/servizi e applicazioni/risorse

Applicazione continua delle policy

In base alla sensibilità delle risorse, a prescindere dalla posizione dell'utente

Integrazioni

Integrazione con gli strumenti esistenti (IDP, EDR, MDM, SIEM)

Connettore per firewall SonicWall

Integrazione immediata con i firewall Gen 7 in modalità Global per 7.1.2+.

Gestione multi-tenant

Policy basate sul cloud per la gestione multi-tenant

Utenti e dispositivi

Single Sign-On

Utilizzo dell'SSO aziendale con creazione di utenti "just-in-time" (JIT)

Gestione della postura

Analisi della postura di un dispositivo, come firewall, crittografia del disco, blocco dello schermo, versione del sistema operativo, ecc.

Correzione personalizzata

Configurazione di istruzioni per correggere la postura dei dispositivi, ad es. messaggistica e link, visualizzata agli utenti finali

Profili di attendibilità

Personalizzazione di fattori ed effetti delle policy in base a gruppi di utenti e dispositivi

Visibilità e conformità

Flusso di eventi in tempo reale

Monitoraggio del flusso di attività di utenti e dispositivi in tempo reale

Report sulla postura dei dispositivi

Tracciamento di tutti i dispositivi (gestiti e non gestiti) che accedono alle risorse aziendali e della loro postura di sicurezza

Report sull'attività degli amministratori

Registrazione di tutte le attività degli amministratori nel Cloud Command Center

Operazioni e automazione

API Restful

Endpoint RESTful per la configurazione di oggetti CSE nel piano di controllo

Client API – pybanyan, terraform

Libreria Python e Terraform per l'automazione e la gestione

Registrazione Zero Touch dei dispositivi

Distribuzione dell'app Banyan al parco dispositivi senza richiedere interazioni con gli utenti finali

	Secure Private Access		Secure Internet Access	
Funzionalità	**Basic**	**Advanced**	**Basic**	**Advanced**
Capacità essenziali				
Tunnel ZTNA (VPNaaS) per consentire l'accesso a reti specifiche	✓	✓		
Proxy ZTNA per connettersi in sicurezza ad applicazioni HTTP interne e servizi TCP		✓		
Sicurezza a livello DNS per proteggere dalle minacce provenienti da Internet			✓	✓
Cloud Access Security Broker (CASB) per applicare policy di attendibilità dei dispositivi per le applicazioni SaaS				✓
Advanced Secure Web Gateway (SWG) per filtrare malware e altre minacce nascoste nel traffico web crittografato				✓
Accesso sicuro alla rete				
Reti (intervallo RFC-1918) e domini (server DNS interni) privati	✓	✓		
Split-tunneling in sottoreti e domini specifici (privati o pubblici)	✓	✓		
Tunneling completo per tutto il traffico	✓	✓		
Policy di rete/layer 4 basate su CIDR e FQDN	✓	✓		
Accesso sicuro a risorse private				
Accesso ai siti web interni tramite flussi OpenID Connect solo per browser		✓		
SSH ai server Linux		✓		
RDP alle macchine Windows		✓		
Client nativi per accedere a server di database come PostgreSQL e MySQL		✓		
Client Kubernetes per accedere al cluster		✓		
Autenticazione con certificato SSH, autorizzazione dei principali e log degli audit		✓		
Policy al layer 7 per accedere ad API, pagine web		✓		
Protezione da minacce Internet				
Sicurezza a livello DNS per bloccare i domini con malware, phishing, botnet e altri rischi			✓	✓
Categorizzazione dei contenuti			✓	✓
Blocco personalizzabile			✓	✓
Sicurezza delle applicazioni SaaS				
Visibilità nelle applicazioni cloud / shadow IT				✓
Lista di autorizzazione IP per applicazioni cloud tramite SonicWall Edge				✓
Attendibilità dei dispositivi per Okta				✓
Attendibilità dei dispositivi per Azure AD				✓
Attendibilità dei dispositivi per altri IDP come OneLogin, Jumpcloud				✓
Servizio di filtraggio dei contenuti web				
Filtraggio degli URL				✓
Protezione anti-malware				✓
Utenti e dispositivi				
Autenticazione senza password tramite federazione IDP		✓		✓
Accesso basato su policy da dispositivi non registrati con un certificato di attendibilità del dispositivo		✓		✓
Accesso clientless		✓		✓
Account di servizio (token API per l'accesso programmatico come script e automazione tramite il piano dati)		✓		✓

SONICWALL

Utenti e dispositivi (continuazione)				
Integrazione SCIM per gestire le assegnazioni degli utenti		✓		✓
Integrazioni EDR (ad es. CrowdStrike, SentinelOne, Microsoft Defender)		✓		✓
Integrazioni MDM/UEM (ad es. JAMF, Kandji, Jumpcloud, Intune, Workspace One)		✓		✓
Visibilità e conformità				
Integrazione SIEM (ad es. Splunk, Elastic, Sumo Logic)		✓		✓
Rilevamento di reti private (accesso ad applicazioni non approvate da parte di utenti o dispositivi)		✓		n/d
Rilevamento di risorse IaaS		✓		n/d
Rilevamento di applicazioni SaaS		n/d		✓
Operazioni e automazione				
Implementazione di Private Edge: consente di ospitare il gateway SonicWall sensibile alle identità nella propria infrastruttura		✗	n/d	n/d
Servizi e supporto				
Supporto 24x7	✓	✓	✓	✓
Supporto Premier		add-on		add-on
Servizi di implementazione remota		add-on		add-on

Riepilogo

Cloud Secure Edge di SonicWall è una soluzione Security Service Edge che combina un TCO leader del settore a una sicurezza Zero Trust di livello aziendale. Offre un accesso Zero Trust semplice e sicuro a risorse private e internet per dipendenti e terze parti, indipendentemente dalla loro posizione fisica e dal loro dispositivo. Cloud Secure Edge combina le funzionalità di diverse appliance di rete tradizionali – VPN di accesso remoto, proxy web, firewall, ecc. – in una soluzione multi-tenant unificata, basata sul cloud e semplice da implementare e gestire per aziende di tutte le dimensioni, che ottimizza il ROI delle aziende e dei clienti.

Vuoi saperne di più su SonicWall Cloud Secure Edge? Inizia qui.

Se desideri aggiungere Cloud Secure Edge ai tuoi firewall SonicWall Gen 7 esistenti, contatta il tuo responsabile commerciale.

SonicWall

SonicWall è un precursore della sicurezza informatica con oltre 30 anni di esperienza e di impegno continuo verso i propri partner. Grazie alla capacità di creare, scalare e gestire la sicurezza informatica in ambienti cloud, ibridi e tradizionali in tempo reale, SonicWall può fornire in modo rapido ed economico soluzioni di sicurezza dedicate a qualsiasi tipo di organizzazione in tutto il mondo. Mediante i dati del proprio centro di ricerca sulle minacce, SonicWall garantisce una protezione completa contro gli attacchi informatici più elusivi e fornisce informazioni pratiche sulle minacce ai partner, ai clienti e alla comunità di cybersecurity.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com