SONICWALL

SonicWall Cloud Edge Secure Access

Installazione di Zero Trust Security in pochi minuti

SonicWall Cloud Edge Secure Access è un potente servizio cloud con semplici funzioni network-as-a-service per connettività site-to-site e cloud ibrido per AWS, Azure, Google Cloud etc., che abbina gli approcci alla sicurezza Zero-Trust e Least-Privilege in un'unica offerta integrata.

L'approccio basato sul privilegio minimo limita l'accesso dei singoli utenti alle funzioni strettamente necessarie, qualcosa di simile al principio dell'autorizzazione concessa a chi deve assolutamente conoscere determinate informazioni. Limitando l'esposizione ad altre aree sensibili della rete, le organizzazioni possono garantire la sicurezza delle loro risorse senza compromessi in termini di flessibilità operativa.

SonicWall Cloud Edge Secure Access applica la sicurezza Zero-Trust basata su quattro azioni di sicurezza principali:

- Verificare le credenziali dell'utente e del dispositivo, anche per il traffico interno
- Contestualizzare la richiesta per garantire autenticità e conformità alle linee guida aziendali
- Microsegmentare l'accesso alla rete per evitare che le minacce si spostino lateralmente
- Consentire l'accesso solo alle applicazioni necessarie

Al centro dell'infrastruttura Cloud Edge Secure Access c'è l'architettura moderna e intrinsecamente sicura Software-Defined Parameter (SDP).

SDP disaccoppia il controller che autentica utenti e dispositivi dai gateway che fungono da trust broker. Distribuendo i gateway vicino alle sedi degli utenti finali il servizio Cloud Edge Secure Access può essere rapidamente ampliato per mantenere prestazioni elevate e consentire la migliore esperienza nel cloud.

Inoltre, la separazione delle funzioni blocca efficacemente le comuni minacce informatiche, come DDos, dirottamento su Wifi pubblico, inondazione SYN e Slowloris, e consente a SonicWall di offrire una piattaforma di sicurezza Zero-Trust altamente integrata.

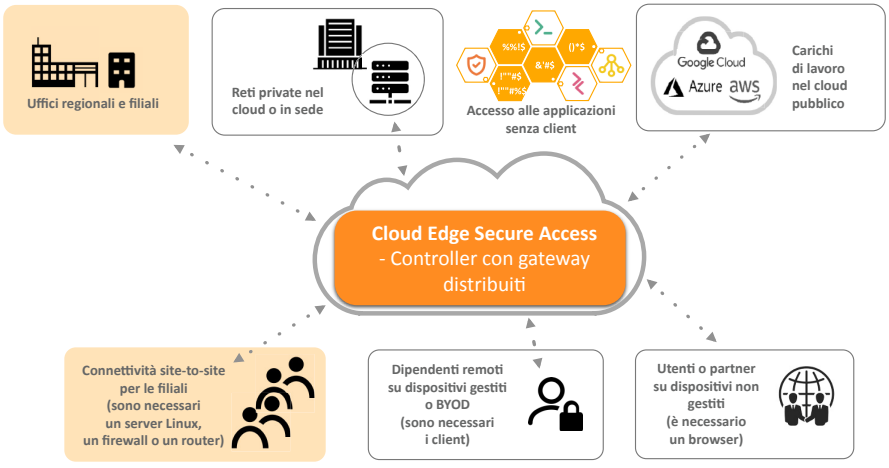

Figura 1 – SonicWall Cloud Edge Secure Access

Vantaggi:

- Garantisce la sicurezza delle imprese distribuite e della forza lavoro remota
- Accesso sicuro istantaneo a qualsiasi sito e a qualsiasi risorsa su cloud ibridi
- Politiche Zero-Trust in base alle reti, alle applicazioni, ai profili utente e ai dispositivi
- Microsegmentazione integrata per impedire i movimenti laterali non autorizzati
- Modulabile da centinaia a migliaia di utenti
- I responsabili informatici possono configurare il prodotto nel giro di 15 minuti
- L'utente finale può installare il prodotto in 5 minuti
- Nessun limite di utilizzo e di larghezza di banda
- Sicurezza del Wi-Fi pubblico
- Crittografia WireGuard di prestazioni elevate
- Integrazione Cloud Identity Provider
- Integrazione moderni servizi SSO e MFA
- Bloccaggio inondazioni DDoS, Slowloris e SYN
- Multi-tenancy per i MSSP
- Monitoraggio e reportistica completi per verifiche di conformità
- Gateway cloud dedicati e indirizzi IP per cliente
- Servizio disponibile negli USA, in Europa, Medio Oriente e Asia

L'evoluzione della VPN tradizionale alla sicurezza Zero-Trust

Nell'era della trasformazione digitale, in cui il personale può lavorare da qualsiasi luogo e le risorse sono nel cloud, le soluzioni VPN tradizionali sono troppo complesse da installare e presentano troppe limitazioni.

Per installare una VPN tradizionale ci possono volere diversi giorni se non settimane, ed occorre inoltre fare i conti con l'indisponibilità e la difficoltà di programmare i tempi morti.

La VPN tradizionale può anche aprire la backdoor a potenziali violazioni, perché qualsiasi accesso riuscito consente all'utente un ampio accesso alla rete e un movimento laterale all'interno della sottorete.

Infine, la VPN induce una latenza aggiuntiva, che peggiora l'esperienza degli utenti nel cloud perché il traffico passa attraverso il concentratore VPN installato in sede anziché andare direttamente nel cloud.

Gartner prevede che entro il 2023 il 60% delle imprese eliminerà gradualmente la maggior parte delle reti private virtuali (VPN) ad accesso remoto a tutto vantaggio delle ZTNA.

SonicWall Cloud Edge Secure Access risolve i problemi sopra descritti e propone ZTNA con queste tre funzioni fondamentali:

Accesso con privilegio minimo per proteggere le risorse aziendali

Installazione rapida e in autonomia

Accesso diretto e affidabile al cloud da qualsiasi luogo

Figura 2 – Funzioni di SonicWall Cloud Edge Secure Access

Casistiche d'uso principali

Installazione rapida e in autonomia

- **Installazione rapida:** in meno di 15 minuti un responsabile informatico può registrarsi, istanziare un gateway e configurare politiche granulari basate sulle reti e sul contesto utente.
- **Presa in carico rapida dell'utente:** l'utente finale può scegliere di connettersi tramite un'applicazione client per dispositivo mobile o per desktop o di bypassare del tutto l'installazione del client se utilizza un computer pubblico, a condizione che sia disponibile un browser. Con la modalità di installazione in autonomia un utente può essere attivo e funzionante in 5 minuti.
- **Accesso affidabile al cloud ibrido:** una volta completate le procedure preliminari gli utenti usufruiranno di un accesso rapido, facile e sicuro alle risorse interne e a quelle nel cloud pubblico da qualsiasi parte del mondo.

Protezione del lavoro da qualsiasi luogo nelle zone affidabili e negli hotspot pubblici

- **Sicurezza Wi-Fi automatica:** Le applicazioni degli agenti Cloud Edge Secure Access per i sistemi operativi Windows e Mac effettuano il monitoraggio previsionale dell'ambiente ed attivano automaticamente una connessione d'accesso sicura negli hotspot pubblici. In questo modo gli utenti vengono protetti dalle intercettazioni Wi-Fi fin troppo comuni, che possono provocare sottrazione di dati e violazioni della conformità.
- **Kill switch:** Per impedire eventuali violazioni informatiche, quando viene interrotta una connessione di accesso sicura, la connessione Internet del dispositivo viene sospesa immediatamente per impedire l'uscita dei dati dal dispositivo.
- **Reti Wi-Fi affidabili:** quando un SSID viene specificato come affidabile, la funzione di sicurezza Wi-Fi automatica non si attiva.
- **VPN/Applicazioni sempre attive:** questa pratica funzione ricollega automaticamente un utente o un dispositivo all'applicazione o a una serie di applicazioni senza dover rieffettuare l'accesso o l'autenticazione.

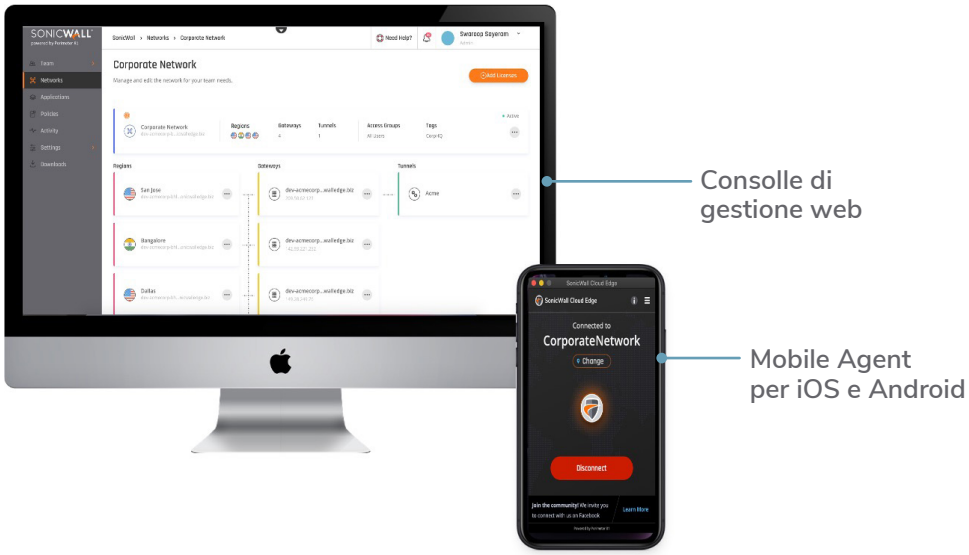

Figura 3 – Consolle di gestione di SonicWall Cloud Edge Secure Access e Mobile Agent Application per Apple IOS

Accesso applicazione Zero-Trust

Cloud Edge Secure Access mette a disposizione delle organizzazioni digitali uno strumento di cui si sentiva enorme bisogno per proteggere le risorse aziendali e nello stesso tempo consentire un ricorso efficace al telelavoro.

Grazie alle politiche Zero-Trust di Secure Access, gli utenti esterni opportunamente predisposti possono utilizzare tutta una serie di applicazioni desktop e web remote senza esporre la rete aziendale alle ciberminacce.

- **Il controllo dell'accesso basato sul privilegio minimo viene rigidamente attuato:** Le organizzazioni possono controllare le interazioni con le risorse sulla base di attributi pertinenti, comprese l'identità dell'utente e quella di gruppo e la sensibilità dei dati.
- **L'importanza del contesto:** La soluzione garantisce un accesso alle risorse interne e a quelle del cloud incentrato sull'utente e basato sulle politiche alle risorse.
- **Integrazione con i principali fornitori di gestione delle identità basati su cloud:** Le organizzazioni possono estendere la durata di funzionamento delle risorse interne convenzionali o passare ai moderni servizi di gestione delle identità basati su cloud forniti da società come Azure AD, Google Authenticator e Okta.
- **Microsegmentazione:** Segmentando con precisione tutto il traffico in arrivo, la microsegmentazione impedisce ai malware o agli utenti non autorizzati di muoversi lateralmente, riducendo la superficie d'attacco e l'esposizione complessiva alle ciberminacce.
- **Autenticazione federata SSO e multifattoriale:** Questa combinazione mette a disposizione un unico portale per autenticare gli utenti in un ambiente informatico ibrido con un'esperienza coerente e senza soluzione di continuità.
- **Funzione di verifica della conformità:** Tutte le attività di Zero-Trust Access sono completamente monitorate e registrate per le verifiche future.

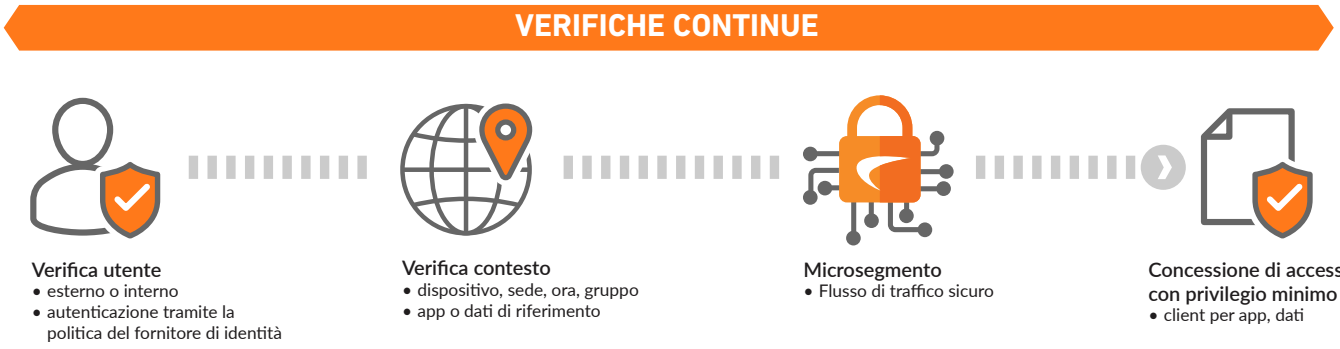

Figura 4 – Processo ZTNA di SonicWall Cloud Edge Secure Access

Interconnettività site-to-site o Network-as-a-Service (Naas)

Cloud Edge Secure Access mette a disposizione servizi di connettività site-to-site o Network-as-a-Service (Naas) per prendere rapidamente in carico le filiali dislocate in ampie zone geografiche.

Con il Naas, i responsabili informatici possono connettere in modo rapido e sicuro chioschi mobili, grande distribuzione e punti vendita alle risorse nel cloud senza dover ricorrere ai costosi MPLS.

- **Servizi di interconnessione site-to-site o site-to-cloud:** La soluzione consente una facile connessione agli ambienti cloud più diffusi, come AWS, Azure e Google Cloud, o di realizzare una connessione di comunicazione sicura tra due reti diverse in sedi diverse.
- **Installazione multiregionale:** Gli amministratori possono installare gateway Cloud Edge dedicati in diverse sedi per offrire alle filiali internazionali e ai dipendenti un servizio a velocità ottimale.
- **Backbone globale di prestazioni elevate:** Il servizio SonicWall Cloud Edge è disponibile a livello globale. L'infrastruttura garantisce una latenza minima distribuendo gateway vicino alle sedi dei clienti e bilanciando il traffico tra i server.
- **Tunnel WireGuard allo stato dell'arte:** I responsabili informatici possono sfruttare qualsiasi router o firewall di filiale con IPsec per collegarsi al gateway Cloud Edge più vicino.

  Per prestazioni ottimali SonicWall consiglia la funzione WireGuard Connector che richiede un server Linux di filiale per eseguire il servizio tunnel WireGuard sul gateway più vicino.
- **Verifica e monitoraggio di rete:** Consente di acquisire una maggiore conoscenza della situazione dell'attività e della sicurezza della rete, compresa la visibilità sulla creazione di gruppi e di server, sull'autenticazione dei membri dei gruppi, sulle variazioni delle password e altro ancora.

Specifiche

Categoria	Funzione	Vantaggi
Dimensioni e prestazioni	Utenti	100-10000+
	Prestazioni	1 Gbps per gateway cliente; adeguamento orizzontale del cloud con più gateway
Piattaforma cloud	Piattaforma di gestione del cloud	Piattaforma di gestione del cloud per una facile definizione della rete dell'organizzazione, sia all'interno, sia nel cloud
	Installazione di rete rapida e semplice	Installazione automatica della rete in meno di 15 minuti
	Disponibilità e funzionamento senza interruzioni	Gestiti automaticamente dal servizio. Lo stato attuale di funzionamento di Cloud Edge è visualizzabile su https://status.sonicwall.com/
	Bilanciamento del carico	Effettuato da gateway condivisi/dedicati in più di 30 POP globali, mantenuti e gestiti da SonicWall
	Interconnettività site-to-site	Connettività tra due sedi (interne, esterne e nel cloud). Compatibilità IPsec e WireGuard
	DNS personalizzato	Per utilizzare i server DNS interni, una volta definito un tunnel, è anche possibile definire un server DNS personalizzato al posto di quello predefinito
	Accesso applicazioni senza client	Accesso applicazioni Zero Trust a HTTP, HTTPS, RDP, VNC, SSH
	Accesso tramite client	Disponibile per piattaforme Windows, Mac, IOS e Android
	Applicazioni e ambiente	Ideale per ambienti ibridi e carichi di lavoro nel cloud
Funzioni Zero Trust	Applicazioni Always-on	Le applicazioni Always-on consentono un accesso sicuro a Internet quando ci si collega a reti non affidabili, il che mette al riparo da minacce alla sicurezza
	Segmentazione basata sulle politiche	Applicazione delle politiche a utenti e applicazioni
	Politiche di controllo degli accessi granulari	Basate su utenti, applicazioni, Geo IP, geo-localizzazione (paese), tipo di browser, SO, data e ora
	Suddivisione tunneling	Consente di decidere a quale sottorete destinare il traffico
	Kill Switch	Per impedire violazioni informatiche, quando viene interrotta una connessione di accesso sicura, la connessione Internet del dispositivo viene sospesa immediatamente per impedire l'uscita dei dati dal dispositivo.
	Sicurezza Wi-Fi automatica	La nostra funzione brevettata protegge automaticamente i dispositivi dei dipendenti quando si collegano a Wi-Fi pubblici non sicuri
	Filtraggio DNS	Impedisce agli utenti della rete di accedere a determinati siti web, categorie di siti e indirizzi IP dai browser Internet
Autenticazione	Funzioni SSO	Possibilità di accesso unificato tramite fornitori SSO, come Okta, G Suite, Azure AD e Active Directory LDAP
	Autenticazione a due fattori	Impedisce gli attacchi remoti grazie all'integrazione predefinita con SMS, DUO Security e Google Authenticator 2FA
Monitoraggio, registrazione e supporto	Supporto 24X7	Soluzione completamente gestita nel cloud, compreso supporto
	Verifica e reportistica delle attività	Monitoraggio accessi, installazioni gateway e connessioni delle applicazioni
	Integrazione SIEM	Acquisizione, conservazione e invio di dati ed eventi di sicurezza in tempo reale a tutte le applicazioni SIEM, compresa una facile integrazione click-through con Splunk
	Stato servizi cloud	Verificare su https://www.sonicwall.com/support
Interfunzionalità	Firewall aziendale	SonicWall, Check Point, Fortinet, Palo Alto Networks, WatchGuard, Sophos, Xyxel, UniFi, pfSense, Cisco e Untangle
Integrazioni personalizzate	API disponibili	La nostra API completa basata su REST consente un'integrazione rapida e semplice con strumenti di gestione, automazione e orchestrazione di terzi, garantendo la protezione delle applicazioni virtualizzate rese disponibili ex novo o trasferite
Conformità	ISO 27001 & 27002, SOC-2 tipo 2	Infrastruttura cloud conforme a SOC 2 tipo 2
Ordinazione	Abbonamento	Per l'abbonamento a Cloud Edge Secure Access rivolgersi al MSSP o al rivenditore di fiducia o alla rete di distributori.

SonicWall

SonicWall fornisce soluzioni di cybersecurity illimitata per l'era iperdistribuita in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e della mancanza di sicurezza. Conoscendo l'ignoto, offrendo una visibilità in tempo reale e rendendo possibili economie innovative, SonicWall colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per ulteriori informazioni visitare www.sonicwall.com.

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

Datasheet-CloudEdge-US-VG-2807