Zscaler Zero Trust Firewall

Una protezione zero trust sicura e adattiva per il traffico web e non web, al 100% nativa del cloud.

SCHEDA TECNICA

Zscaler Zero Trust Firewall protegge il traffico Internet per ogni utente, applicazione e posizione con la piattaforma di sicurezza SSE (Security Service Edge) nativa del cloud più completa del settore.

Oggi, il mondo del lavoro è distribuito e mobile. Le applicazioni si spostano dai data center al cloud, mentre i nuovi workload digitali vengono sempre più spesso distribuiti in modo nativo sul cloud. Inoltre, gli utenti che lavorano da varie sedi, tra cui uffici domestici, ambienti di lavoro condivisi, filiali e da remoto, accedono alle applicazioni aziendali direttamente da Internet.

Gli utenti e le applicazioni cloud generano grandi volumi di traffico che vengono reindirizzati verso dispositivi di sicurezza tradizionali e incentrati sulla rete, influenzando la produttività, dando vita a colli di bottiglia nella connettività e intensificando i rischi per l'azienda. Se manca un'ispezione completa del traffico cifrato tramite SSL, gli aggressori se ne possono approfittare, utilizzando la crittografia e le porte non standard per eludere il rilevamento e sferrare attacchi celati. I firewall virtualizzati tentano di rispondere a questa sfida ma, dato che sono progettati per estendere la rete verso l'esterno alle risorse cloud, presentano le stesse limitazioni in termini di capacità.

Per garantire l'interconnettività e la sicurezza dei workload, sarà comunque necessario disporre di risorse dedicate per ottimizzare la gestione, altrimenti si rischiano errori di configurazione.

Zscaler Zero Trust Firewall

Zscaler Zero Trust Firewall offre una protezione cloud per il traffico web (HTTP/HTTPS) e non web (FTP, DNS, RDP, Telnet e altro) che copre tutti gli utenti e i dispositivi, indipendentemente dalla loro posizione. Inoltre, migliora la connettività e la disponibilità indirizzando in modo sicuro il traffico utilizzando punti di accesso a Internet locali, senza che sia necessario eseguire il backhauling tramite VPN e senza duplicare lo stack di dispositivi di sicurezza in ogni sede. Instradando le connessioni dirette a Internet e SaaS verso Zscaler, questa soluzione garantisce l'ispezione di tutto il traffico utente, incluso il traffico cifrato con SSL, grazie a una scalabilità elastica che consente di gestire volumi elevati di connessioni a lunga durata.

Zero Trust Firewall aiuta le organizzazioni a ottemperare agevolmente agli standard normativi, configurando, gestendo e applicando in modo universale una protezione dalle minacce sensibile agli utenti e alle applicazioni e policy basate sul rischio, per garantire la visibilità su rete e applicazioni tramite una console centralizzata per la gestione delle policy. In quanto soluzione firewall come servizio (Firewall as a Service, FWaaS), la responsabilità degli aggiornamenti, degli upgrade e delle patch, compresi i requisiti di scalabilità, ricade su Zscaler. Questo può fornire notevoli risparmi sui costi, con la sostituzione delle apparecchiature fisiche e l'eliminazione delle complesse matrici di configurazioni di rete e policy legate alle sedi fisiche.

Zscaler Zero Trust Firewall registra ogni sessione per garantire la massima visibilità su tutti gli utenti e le sedi, garantendoti l'accesso alle informazioni di cui hai bisogno, esattamente quando ne hai bisogno. Zscaler trasforma la connettività ibrida e delle filiali e fornisce una soluzione alle attuali esigenze in termini di sicurezza e prestazioni, garantendo la massima scalabilità per soddisfare le tue necessità di trasformazione e supportare il passaggio all'utilizzo di applicazioni native del cloud, come Microsoft 365.

I VANTAGGI DI ZSCALER ZERO TRUST FIREWALL:

- **Protezione completa per gli utenti che lavorano da qualsiasi luogo:** le policy di sicurezza dinamiche e basate sul rischio seguono i tuoi utenti ogni volta che si connettono, senza che si generi una matrice complessa di policy e configurazioni di rete.

- **Ispezione completa per individuare gli attacchi nascosti:** l'ispezione illimitata del traffico inline e la decifrazione SSL nativa prevengono le minacce elusive e interrompono le connessioni dannose.

- **Rilevamento del traffico web elusivo sulle porte non standard.** identificazione e intercettazione rapide delle minacce informatiche elusive e cifrate che sfruttano le porte non standard.

- **Punti di accesso a internet locali forniti dal cloud:** connessioni dirette a Internet veloci e sicure, per tutto il traffico degli ambienti ibridi e delle filiali, che si adattano in modo elastico e migliorano l'esperienza utente.

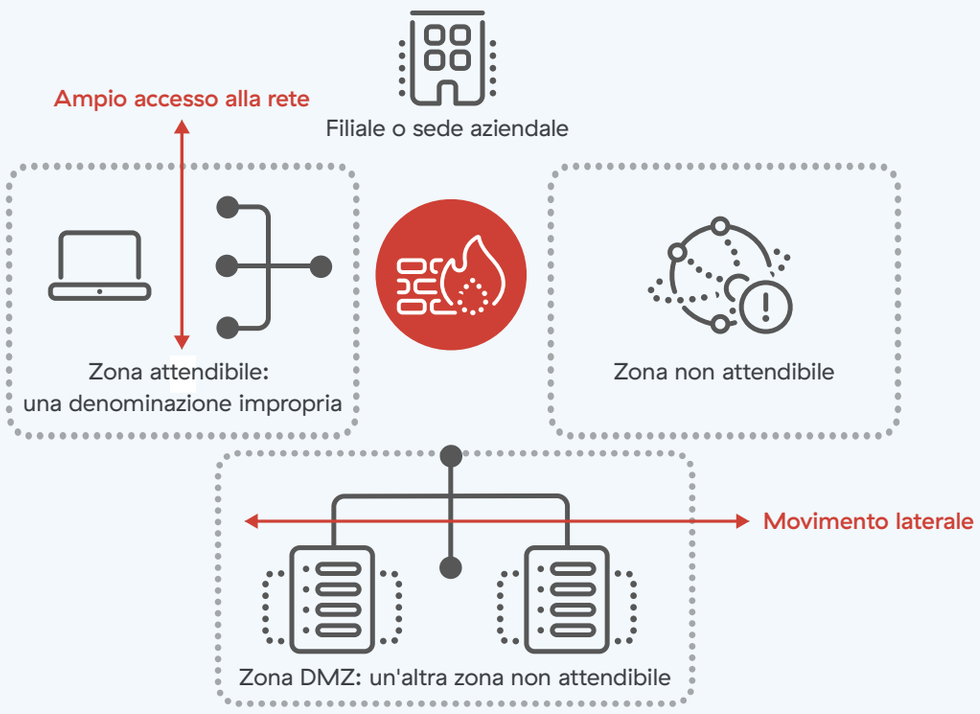
- **Sistema di prevenzione delle intrusioni (IPS) sul cloud sempre attivo:** le firme IPS comportamentali adattive, gestite da Zscaler ThreatLabz, operano in tempo reale per arricchire i flussi di lavoro di SecOps.

- **DNS sicuro senza compromissione delle prestazioni:** le risoluzioni localizzate garantiscono prestazioni superiori, mentre utenti ed endpoint rimangono al sicuro dai siti dannosi e dal tunneling DNS.

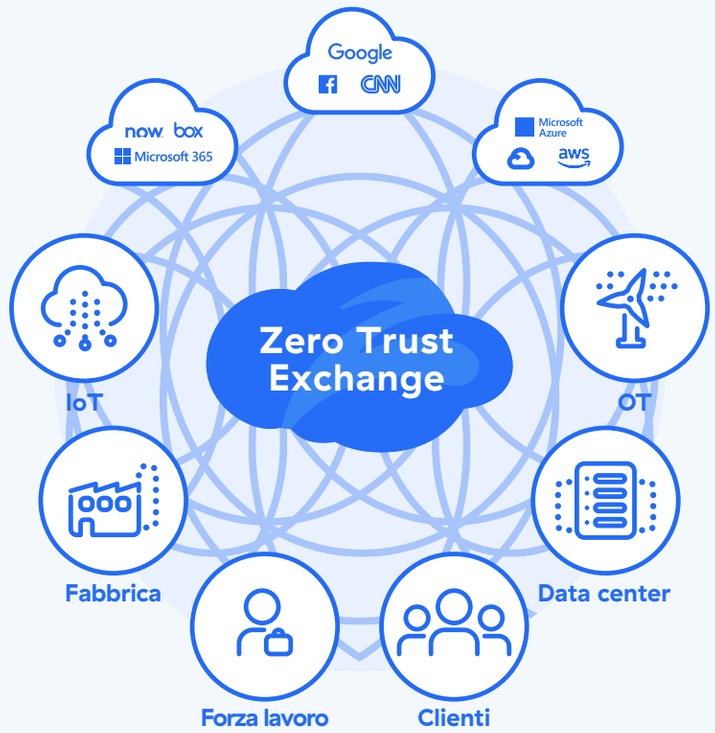
- **Protezione fornita dal cloud con una presenza all'edge a livello globale:** Zscaler Zero Trust Firewall offre una sicurezza e un'esperienza utente completamente integrate e senza pari tramite Zscaler Internet Access™ e nell'ambito della piattaforma Zscaler Zero Trust Exchange™.

Abbandona l’architettura legacy con Zscaler Zero Trust Firewall

Architettura zonale del firewall legacy



Piattaforma zero trust di Zscaler



I firewall legacy e quelli di nuova generazione non sono in grado di soddisfare i principi dello zero trust previsti dallo standard NIST 800-207.
L’architettura di sicurezza basata sul perimetro non è stata progettata per ispezionare il traffico cifrato su larga scala su reti e dispositivi non protetti.
La mancanza di un’autenticazione rigorosa degli utenti e di controlli continui delle policy a ogni passaggio potrebbe comportare la compromissione di un server o un dispositivo, offrendo agli aggressori un ampio accesso alla rete e l’opportunità di muoversi lateralmente. Inoltre, l’utilizzo di un firewall legacy come gateway per implementare una rete privata virtuale (VPN) espone le reti pubbliche e private.
Solo un firewall zero trust è in grado di garantire un accesso dinamico e a privilegi minimi per favorire la trasformazione della rete e della sicurezza.

I vantaggi di un firewall nativo del cloud

Realizzato appositamente per il mondo digitale di oggi, Zscaler Zero Trust Firewall ti fornisce un accesso sicuro a Internet e ti permette di gestire tutto il traffico web e non web, su tutte le porte e i protocolli, con una scalabilità elastica senza limiti e dalle prestazioni imbattibili. I tuoi utenti possono usufruire di una protezione coerente, indipendentemente dal dispositivo utilizzato o dalla loro posizione, che siano a casa, nelle sedi centrali, nelle filiali o in viaggio, senza i costi, la complessità e i limiti prestazionali dei tradizionali apparecchi firewall di nuova generazione.

ALIMENTATO DA UNA PIATTAFORMA ADATTIVA ZERO TRUST

Non accettare più le ispezioni statiche, i cali prestazionali e i limiti strutturali dei dispositivi firewall tradizionali. Costruito su una piattaforma nativa del cloud e completamente integrata, Zscaler Zero Trust Firewall si adatta in modo elastico per gestire il traffico delle applicazioni cloud che richiedono connessioni di lunga durata, intercettando e ispezionando in modo nativo il traffico SSL/TLS su larga scala per rilevare i malware nascosti nel traffico cifrato.

CONNESSIONI TRASFORMATIVE PER REALTÀ IBRIDE E FILIALI

Passa da infrastrutture costose e incentrate sulla rete a veri punti di accesso a Internet locali forniti dal cloud. Instrada il traffico Internet a livello locale per fornire connessioni dirette al cloud, offrendo così connessioni costantemente veloci e garantendo al contempo sicurezza e controlli degli accessi per tutte le porte e i protocolli. Inoltre, eliminando la necessità di dover installare o gestire apparecchiature fisiche, potrai ridurre i costi di backhauling tramite MPLS e azzerare le problematiche legate alla gestione delle patch, che risulta onerosa e dispendiosa in termini di tempo, al coordinamento delle finestre di interruzione e alla gestione delle policy.

SICUREZZA ONNIPRESENTE PER LA FORZA LAVORO MODERNA

Approfitta degli aggiornamenti di sicurezza in tempo reale basati su 300 bilioni di segnali giornalieri e condivisi ogni giorno sull'intero cloud per usufruire di una protezione identica su qualsiasi dispositivo, ovunque gli utenti si connettano. Avvicinando l'intero stack di soluzioni di sicurezza agli utenti, questi ultimi possono ottenere un'impareggiabile protezione dalle minacce sensibile a utenti e app, con policy dinamiche di tipo "follow-me" all'interno e all'esterno della rete aziendale.

BLOCCO SEMPRE ATTIVO DEGLI ATTACCHI DANNOSI NOTI

Spingiti dove le soluzioni tradizionali non riescono ad arrivare e proteggiti dalle minacce con un sistema di prevenzione delle intrusioni (Intrusion Prevention System, IPS) sensibile al contesto e distribuito sul cloud, gestito da Zscaler ThreatLabz. Grazie all'ispezione illimitata del traffico inline, che copre anche il traffico cifrato e IoT/OT dentro e fuori dalla rete, le firme IPS comportamentali vengono applicate in tempo reale quando viene eseguito l'accesso a migliaia di applicazioni web e non web, indipendentemente dal tipo di connessione o dalla posizione.

OTTIMIZZA IL DNS PER POTENZIARE LE PRESTAZIONI E LA SICUREZZA

Ottieni una risoluzione più rapida raggruppando le app locali a livello geografico, migliorando così l'esperienza utente e le prestazioni delle app cloud e implementando al contempo policy di controllo e sicurezza del DNS. Con l'ispezione SSL su larga scala, puoi incrementare la visibilità e impedire agli aggressori di utilizzare impropriamente il DNS over HTTPS (DoH), proteggendo in modo ottimale utenti e dipendenti e impedendo loro di accedere a domini dannosi e aggirare le policy aziendali. Grazie all'approccio DNS come servizio (DNS as a Service), Zscaler riduce al minimo la latenza e protegge i punti di accesso a Internet locali utilizzando proxy completi per tutto il traffico DNS; inoltre, usa il machine learning per rilevare e bloccare l'attività dei tunnel di esfiltrazione dei dati.

GESTIONE DELLE POLICY DI FACILE COMPRENSIONE

Definisci, distribuisci e applica le policy istantaneamente e a livello globale a tutti gli utenti e le sedi da un'unica console. Invece di doverti districare tra complesse matrici di policy e configurazioni di rete e dover ricreare queste policy per ogni sede in cui sono implementati firewall tradizionali, con Zero Trust Firewall puoi semplificare la loro gestione creando una base centralizzata di regole granulari dei firewall definite per utente, applicazione, posizione, gruppo e reparto. Inoltre, gli amministratori possono inviare log completi di grado forense, arricchiti con dettagli su utenti, richieste, risposte, servizi utilizzati e altro agli strumenti di SIEM e XDR per migliorare le indagini sulla sicurezza e la risposta agli incidenti.

Gartner

Zscaler è stata nominata una leader nel MQ di Gartner per il Security Service Edge, posizionandosi al vertice per capacità di esecuzione (categoria Ability to Execute).

Scopri di più →

Le principali funzionalità di Zscaler Zero Trust Firewall

Gestione centralizzata delle policy	Definisci e applica istantaneamente le policy in tutte le sedi, senza doverle ricreare per ogni sede
Servizi di sicurezza completamente integrati	Le informazioni contestuali vengono condivise su DLP, APT, sandbox e altri servizi per fornire una protezione migliore e una maggiore visibilità
Controllo granulare, logging e visibilità in tempo reale	Log di grado forense ricchi di informazioni, unificati a livello globale e illimitati per sei mesi, per fornire una visibilità dettagliata e consentire l'analisi e la correlazione per scoprire tendenze, analizzare la produttività e facilitare la risoluzione dei problemi
Protezione dalle minacce sensibile all'utente	Gli utenti vengono definiti per gruppi, reparti o sedi, indicando anche se lavorano da casa o da remoto, e i dati estrapolati vengono integrati con i provider di identità e i database degli utenti locali per applicare policy uniformi indipendentemente dalla posizione fisica.

Le principali funzionalità di Zscaler Zero Trust Firewall (continua)

Protezione dalle minacce in base alle app	Identificazione e classificazione delle applicazioni al primo pacchetto per abilitare policy di filtraggio dei firewall e di inoltro e intraprendere azioni immediate e con maggiore priorità attraverso policy adattative sensibili al contesto Supporto di diversi tipi di applicazioni su tutti i servizi di rete: porte e protocolli, applicazioni di rete, SNI (hostname), DPI, UCaaS basato sull'identificazione del primo pacchetto, IP, gruppi FQDN e altri rilevamenti basati sull'euristica
Sicurezza e controllo IPS adattivi	Una protezione dalle minacce sempre attiva e distribuita sul cloud con firme IPS personalizzate e migliaia di firme IPS adattive e comportamentali su qualsiasi porta e protocollo, indipendentemente dal tipo di connessione o dalla posizione, con l'ispezione di tutto il traffico Internet degli utenti. Visualizza l'elenco di tutte le firme IPS gestite da ThreatLabZ.
Ispezione di sicurezza avanzata	L'ispezione avanzata dei pacchetti viene applicata sui protocolli non web, tra cui FTP, DNS, RDP, Telnet e altri, per identificare e prevenire il traffico elusivo sulle porte non standard.

Le principali funzionalità di Zscaler Zero Trust Firewall (continua)

Sicurezza e controllo dei DNS	Inoltrando tutto il traffico DNS tramite Zscaler, le prestazioni delle applicazioni cloud vengono ottimizzate e si riduce al minimo la latenza, garantendo una sicurezza senza compromessi. Abilitando le policy in base all'utente, all'app, alla posizione e all'IP del Paese, è possibile bloccare automaticamente gli utenti di domini dannosi e rilevare e prevenire il tunneling DNS. • **Risoluzione:** il DNS as a Service fornisce una risoluzione ottimale con localizzazione, tenancy e latenza minima • **Filtraggio DNS:** creazione di regole di filtraggio DNS personalizzate per bloccare, consentire o reindirizzare diversi tipi di richieste DNS da destinazioni note e dannose • **Sicurezza ed esfiltrazione dei dati:** il machine learning rileva malware, phishing, tunnelling DNS ed esfiltrazione dei dati • **DNS over HTTPS (DoH):** i punti ciechi generati dal DoH vengono eliminati, così come l'aggiramento delle misure di controllo interne quando le connessioni DNS vengono cifrate nel traffico HTTPS comune
Policy per il nome di dominio completo (FQDN)	Configurazione e gestione semplificate delle policy di accesso per le applicazioni ospitate su più IP
Controllo del protocollo di trasferimento file (FTP) e supporto della traduzione degli indirizzi di rete (NAT)	Supporto per il controllo degli accessi tramite FTP e FTP over HTTP e supporto per proxy di destinazione NAT e inoltro NAT
Certificazioni di privacy e conformità	Ottemperanza a rigorosi standard globali commerciali e governativi relativi a rischio, privacy e conformità
Normative di settore e sulla privacy dei dati	Conformità alle normative sulla privacy dei dati specifiche per settore e singoli Paesi
Protezione condivisa a livello globale	Grazie all'effetto cloud, ogni volta che una nuova minaccia viene identificata in una qualsiasi delle decine di miliardi di richieste elaborate quotidianamente dal cloud Zscaler, la minaccia viene bloccata per tutti gli utenti Zscaler, ovunque

Zscaler Zero Trust Firewall è parte integrante di Zscaler Internet Access ed è incluso nelle edizioni ZIA e Zscaler for Users Essentials e Business. Le funzionalità avanzate di Zscaler Zero Trust Firewall sono incluse nelle edizioni ZIA e Zscaler for Users Transformation e Unlimited, nonché come modulo aggiuntivo per le edizioni Essentials e Business.

	Standard	Advanced
CRITERI DELLE POLICY DI ZERO TRUST FIREWALL		
Servizi di rete e applicazioni	✓ Fino a 10 regole	✓
Controllo del filtraggio FQDN		✓
Sensibilità alla posizione		✓
Sensibilità all'utente – incluso	–	✓
Applicazione di rete (DPI)	–	✓
Policy dinamiche basate sul rischio	–	✓
Regole del firewall	✓ Fino a 10 regole	✓ Oltre 1.000 regole
DNS CONTROL		
Resolver DNS attendibile	✓	✓
Filtraggio e sicurezza DNS	✓ fino a 64 regole	✓
Rilevamento di tunnel DNS e app	–	✓
CONTROLLO IPS	–	✓
CONTROLLO FTP	✓	✓
CONTROLLO NAT	✓	✓

FUNZIONALITÀ DELLA PIATTAFORMA		
Ispezione SSL completa	✓	✓
Logging in tempo reale	✓ Dettagli di logging aggregati per le azioni “allow” (consenti) del firewall e dettagliati per le azioni “block” (blocco) con log DNS completi	✓ Tutti i log per tutte le azioni e tutte le funzioni, inclusi ID utente, ID app, IPS e altro
	Incluso con Essentials e la licenza della piattaforma	È richiesta una licenza specifica per il componente aggiuntivo

Informazioni su Zscaler
Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. La piattaforma Zscaler Zero Trust Exchange™ protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati, collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 150 data center a livello globale, Zero Trust Exchange™, basata sul framework SSE, è la più grande piattaforma di cloud security inline del mondo. Per saperne di più, visita **zscaler.com/it** oppure seguici su X (precedentemente Twitter) **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/it**

zscaler™

Zero Trust Everywhere