Accesso alla rete Zero Trust con routing privato

Previeni il movimento laterale e riduci la dipendenza dalle VPN

Affidarsi ai controlli basati sulla rete (come VPN e limitazione delle posizioni IP) per l'accesso alle applicazioni può aumentare la superficie di attacco, limitare la visibilità e frustrare gli utenti finali. Zero Trust Network Access di Cloudflare funziona con i provider di identità e le piattaforme di protezione degli endpoint per applicare regole Zero Trust di negazione predefinita che limitano l'accesso alle applicazioni aziendali, agli spazi IP interni e ai nomi host. Alimentato dalla vasta e performante rete Anycast di Cloudflare, rende le connessioni degli utenti più veloci di una VPN.

Sin dall'implementazione interna di Zero Trust Network Access, Cloudflare ha riscontrato i seguenti vantaggi:

- Riduzione del 91% della superficie d'attacco[1]
- Risparmi raddoppiati grazie alla riduzione degli sforzi IT
- Riduzione dell'80% del tempo dedicato alla gestione dei ticket correlati alla VPN
- Riduzione del 70% del volume dei ticket
- Più di 300 ore all'anno di produttività sbloccate durante l'onboarding dei nuovi dipendenti

Cosa è possibile fare con Access

Proteggi tutte le applicazioni

Cloudflare è indipendente dall'identità e dall'applicazione, consentendoti di proteggere qualsiasi applicazione, SaaS, cloud o locale con il tuo provider di identità preferito.

Connetti gli utenti in modo flessibile, con o senza client

Facilitate le applicazioni Web e le connessioni SSH senza bisogno di software client o configurazione dell'utente finale. - Per applicazioni non Web, connessioni RDP e routing privato, utilizza un client completo su Internet e casi d'uso di accesso alle applicazioni.

Abilita la federazione delle identità tra più provider di identità

Integra tutti i tuoi provider di identità aziendale (Okta, Azure AD e altri) per migrazioni, acquisizioni e accesso utenti di terze parti più sicure. Abilita pin una tantum per l'accesso temporaneo o incorpora fonti di identità social come LinkedIn e GitHub.

Limita gli spostamenti laterali tra risorse aziendali

Applica metodi di autenticazione forti e coerenti anche alle applicazioni legacy con firewall IP e regole Zero Trust.

Applica un accesso in grado di riconoscere i dispositivi

Prima di concedere l'accesso, valuta i segnali di posizione del dispositivo, inclusa la presenza del client Gateway, il numero di serie e il certificato mTLS, assicurandoti che solo i dispositivi sicuri e conosciuti possano connettersi alle tue risorse. Integra lo stato del dispositivo dai fornitori di Endpoint Protection Platform (EPP), tra cui Crowdstrike, Carbon Black, Sentinel One e Tanium.

Registra l'attività dell'utente su qualsiasi app

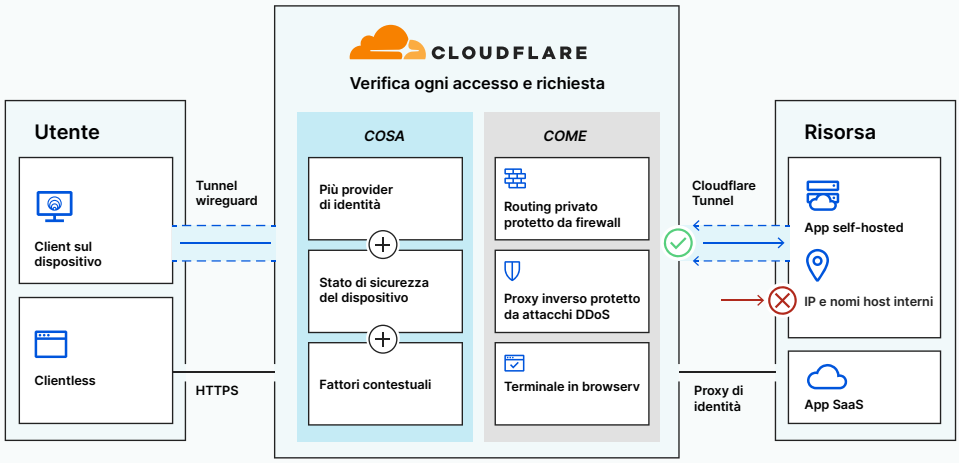
Registra qualsiasi richiesta fatta nelle tue applicazioni protette, non solo di login e logout. Aggrega i log delle attività in Cloudflare oppure esportali sul provider SIEM.

[1]Quando Zero Trust Network Access è combinato con la navigazione su Internet

Cloudflare fa la differenza

- Le **prestazioni senza eguali** instradano le richieste più velocemente con un routing ottimizzato e basato sull'intelligence attraverso la rete Anycast di Cloudflare. In media, l'accesso alle app Web è più rapido del 30% e le connessioni TCP registrano una riduzione del 17% del tempo di andata e ritorno. La nostra intelligence si basa sull'analisi dei dati di rete da 25 milioni di richieste HTTP/secondo e 39.000 nuove connessioni TCP/secondo.
- La **gestione semplificata** combina Zero Trust Network Access, Secure Web Gateway, Remote Browser Isolation e altro ancora in un unico piano di controllo con un'esperienza di amministrazione costruita da zero, non acquisita e combinata da più fornitori.
- L'**ispezione a passaggio singolo** verifica, filtra, isola e analizza il traffico in modo rapido e coerente in tutto il mondo, perché ogni servizio Cloudflare è distribuito su ogni datacenter nelle nostre oltre 250 sedi in tutto il mondo.

Come funziona



Invece di una VPN, gli utenti si connettono alle risorse aziendali tramite un client o un browser Web. Man mano che le richieste vengono instradate e accelerate attraverso l'edge di Cloudflare, vengono valutate rispetto alle regole Zero Trust che incorporano i segnali dei provider di identità, dei dispositivi e di altri contesti. Laddove il software RDP, i visualizzatori di file SMB e altri programmi thick client richiedevano una VPN per la connettività di rete privata, i team possono ora instradare privatamente qualsiasi traffico TCP o UDP attraverso la rete di Cloudflare dove viene accelerato, verificato e filtrato in un unico passaggio, facilitando il miglioramento delle prestazioni e sicurezza.

"Cloudflare Access ci ha salvato dalla necessità di sviluppare un nostro proprio sistema IAM (Identity and Access Management). Non dobbiamo creare funzioni di autorizzazione utente nelle app protette da Access. Siamo entrati tutti, ognuno in azienda ha il suo posto."

Jim Tyrell
Head of Infrastructure, Canva

"Noi di Delivery Hero ci impegniamo molto per offrire ai nostri clienti un'esperienza straordinaria. Cloudflare Access ci aiuta a fare lo stesso per i nostri team interni offrendo loro un ambiente di lavoro sicuro ed eliminando la necessità di una VPN per accedere alle nostre applicazioni in tutto il mondo."

William Carminato
Senior Director, Engineering, Delivery Hero

Integrazioni con Identity and Access Management (IAM)

Active Directory · okta · Google Workspace · PingIdentity · CITRIX · Centrify · onelogin · SAML OIDC

Integrazioni con Endpoint Protection Platform (EPP)

CROWDSTRIKE · vmware Carbon Black · SentinelOne · TANIUM

Funzionalità principali

Criteri omogenei	
Criteri personalizzati per l'accesso alle applicazioni, alle reti private e a Internet	**Illimitato**
Autenticazione tramite provider di identità aziendali e social	✓
Posizione del dispositivo tramite integrazioni di terze parti e Cloudflare	✓
Importazione in blocco basata su CSV per elenchi di numeri di serie dei dispositivi aziendali	✓

Aumenta la visibilità	
Conservazione del registro attività	**6 mesi**
Vista dettagliata del paese e del dispositivo in base all'identità	✓
Invia i log all'archiviazione su cloud o ai SIEM	✓

Connettività sicura	
Connessioni a Internet crittografate basate su client (client WARP)	**Win, Mac, iOS, Android**
Accesso sicuro clientless alle applicazioni self-hosted e SaaS	✓
Connessioni private per applicazioni self-hosted e IP interni e nomi host (Cloudflare Tunnel)	✓

Interoperabilità semplice	
Endpoint e integrazioni di gestione della mobilità	✓
Tunneling suddiviso per connettività locale o tramite VPN	✓
Registrazione automatica del client dispositivi non gestiti	✓
Programma di avvio app personalizzabile	✓
Più provider di identità supportati contemporaneamente dall'autenticazione	✓
Connettori generici e personalizzati per il supporto di SAML e OIDC	✓
Autenticazione basata su token per servizi automatizzati	✓
Autenticazione basata su certificati per IoT e altri casi d'uso di mTLS	✓

Nessuna riduzione delle prestazioni	
SLA con uptime	**100%**
Una delle reti più veloci (A meno di 50 ms dagli oltre 250 PoP)	✓
Il resolver DNS più veloce e al primo posto per la privacy (a 7-31 dagli oltre 250 PoP)	✓
Aggiornamenti rapidi dei criteri (A meno di 500 ms dagli oltre 250 PoP)	✓
Browser remoto rapidissimo (nessun pixel pushing, viene eseguito sulla nostra rete; non è un cloud di terzi)	**Componente aggiuntivo**

Vuoi saperne di più?

Visita www.cloudflare.com/it-it/products/zero-trust/access/ per creare un account, gratuito per un massimo di 50 utenti.