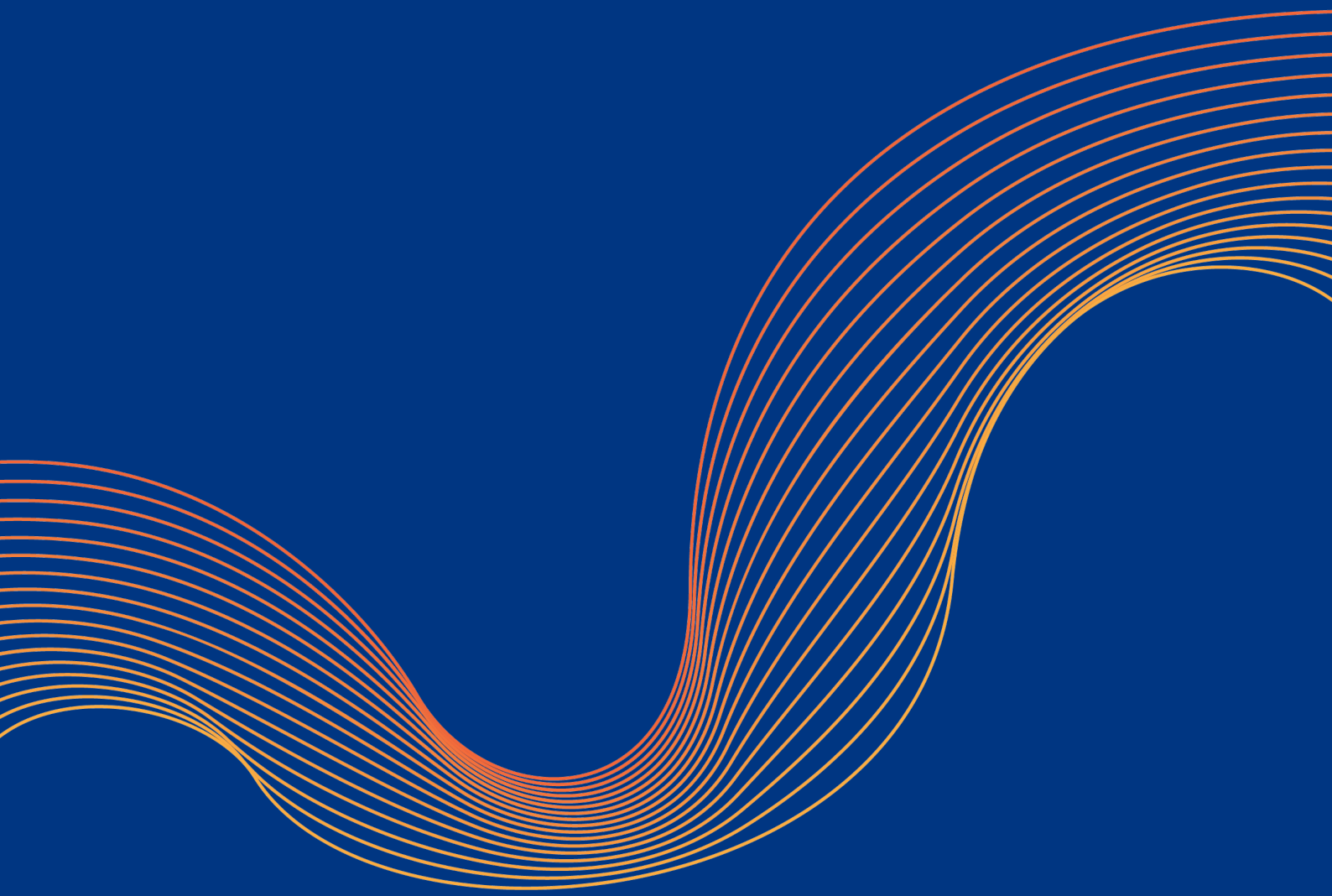
WHITEPAPER

CLOUDFLARE

ZTNA può sostituire la tua VPN? Confronta tre approcci di accesso remoto



+44 20 3514 6970 | enterprise@cloudflare.com | www.cloudflare.com/it-it/

INDICE

INTRODUZIONE

L'accesso remoto sicuro e senza interruzioni è un fattore abilitante per il business, aumentando la produttività degli utenti remoti e riducendo il tempo impiegato dai team IT per integrare e mantenere la connettività utente-applicazione con agilità e resilienza. Eppure, l'accesso remoto rimane un problema per molte organizzazioni.

Una volta, le VPN offrivano un modo semplice per connettere alcuni utenti remoti alle reti aziendali per brevi periodi di tempo. Man mano che la forza lavoro è diventata più distribuita, tuttavia, e le organizzazioni hanno dovuto mantenere gli utenti remoti connessi in modo sicuro per periodi di tempo più lunghi, i difetti di questo approccio sono diventati evidenti, da prestazioni lente e maggiori rischi per la sicurezza a problemi di scalabilità.

Con l'aumento delle esigenze di accesso remoto, le organizzazioni si stanno allontanando sempre più dalle tradizionali implementazioni VPN verso soluzioni più sicure e performanti. Zero Trust Network Access, o ZTNA, crea confini sicuri attorno ad applicazioni, IP privati e nomi host, sostituendo le connessioni VPN predefinite con criteri di negazione predefinita che concedono l'accesso in base all'identità e al contesto.

Nel 2020, circa il 5% di tutto l'utilizzo dell'accesso remoto è stato servito principalmente da ZTNA. A causa delle limitazioni dell'accesso VPN tradizionale e della necessità di fornire un accesso più preciso e un controllo della sessione, si prevede che tale numero salirà al 40% entro il 2024.[1]

Sebbene ZTNA offra alle aziende diversi chiari vantaggi, e funzionalità estese, rispetto alle VPN, molte organizzazioni l'hanno trovato un sostituto incompleto dell'infrastruttura VPN. Ma dato che gli ZTNA diventano più solidi e le VPN diventano più problematiche, le cose stanno cambiando rapidamente. Questo documento mette a confronto le VPN e le soluzioni di accesso remoto ZTNA per chiarirne vantaggi e limiti, facendo luce sulle considerazioni più importanti per i progetti di migrazione. Viene spiegato come Cloudflare offre ZTNA ed è consigliata una serie di passaggi per la transizione dell'infrastruttura VPN legacy a una connettività Zero Trust più rapida e sicura per gli utenti remoti.

[1] Riley, Steve, MacDonald, Neil e Orans, Lawrence. "Market Guide for Zero Trust Network Access." Gartner Research, https://www.gartner.com/en/documents/3986053/market-guide-for-zero-trust-network-access. Accesso effettuato il 21 giugno 2021. Consulta la Tabella 1 per maggiori dettagli.

APPROCCIO 1: VPN LEGACY

Per decenni, le VPN hanno consentito alle organizzazioni di connettere i propri utenti remoti alle reti aziendali con una certa misura di privacy e sicurezza. Invece di accedere a informazioni sensibili tramite Internet pubblico, dove qualsiasi utente malintenzionato potrebbe spiare o rubare dati, le VPN consentono agli utenti di accedere in sicurezza alle risorse interne tramite una connessione crittografata.

Le due modalità più comuni di implementazione della VPN sono le VPN basate su client e le VPN clientless SSL-VPN. Ognuna di queste modalità ha i propri vantaggi e i propri problemi:

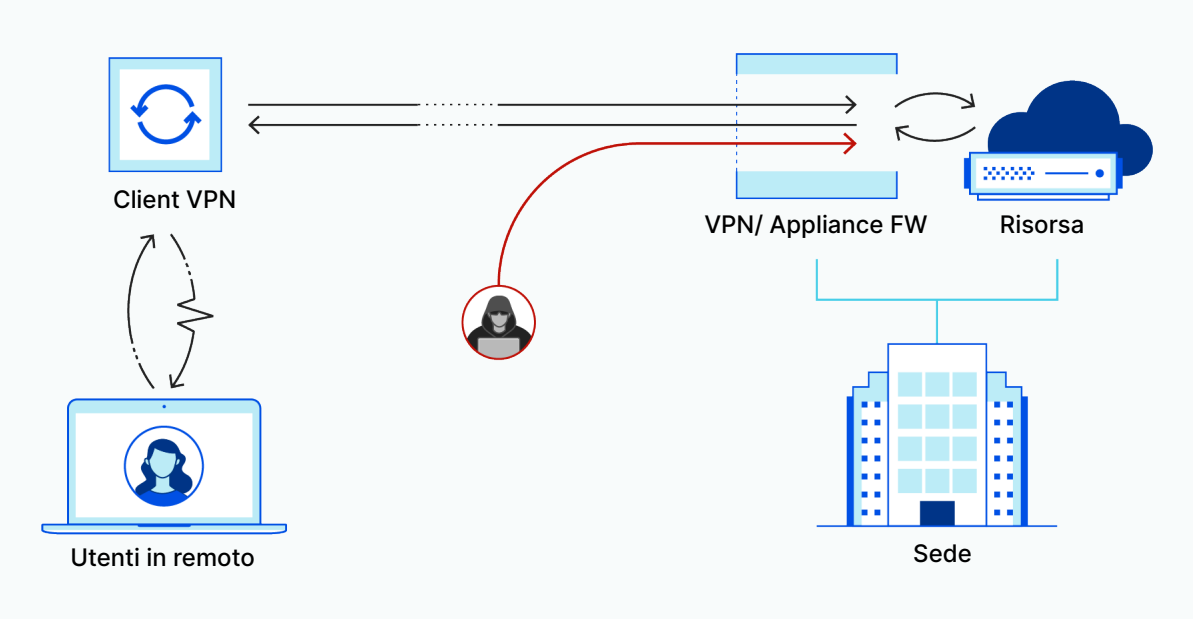
Le **VPN basate su client** collegano gli utenti remoti a una rete privata tramite un tunnel crittografato. Questa connessione viene stabilita tramite un'applicazione software, o client, che richiede agli utenti di autenticarsi una volta con un nome utente e una password per ottenere l'accesso permanente a qualsiasi risorsa all'interno di quella rete.

Vantaggio: una volta connesso, il movimento laterale libero consente agli utenti di accedere rapidamente a più risorse accedendo alle applicazioni e collegandosi agli host interni.

Problemi:

- **Non progettato per utenti in roaming e dispositivi mobili**. Mentre gli utenti vagano, sia i loro laptop che i loro dispositivi mobili si riconnettono senza problemi mentre le reti wireless cambiano da una posizione all'altra. Tuttavia, i client VPN non sono in grado di gestire in modo fluido queste riconnessioni, richiedendo agli utenti di forzare ripetutamente il riavvio e la riautenticazione del client VPN, causando una perdita di produttività e provocando la creazione di ticket IT.
- **Scarsa visibilità.** Con questo metodo, l'infrastruttura della VPN termina il tunnel crittografato dal client VPN dietro il firewall interno del datacenter. Sebbene queste connessioni siano registrate, non esistono registri centralizzati specifici dell'applicazione che rivelano a quali applicazioni hanno avuto accesso gli utenti o le azioni che hanno intrapreso all'interno dell'applicazione.

I **portali SSL-VPN clientless** consentono ad alcuni utenti remoti di connettersi ad alcune applicazioni basate su browser all'interno di una rete privata. Questa connessione è possibile utilizzando un server Web integrato nell'appliance di rete che esegue il servizio VPN.	**Vantaggio:** invece di utilizzare un client su un dispositivo, qualsiasi browser Web può utilizzare il certificato SSL del portale per stabilire una connessione HTTPS crittografata e supportare gli appaltatori su dispositivi non gestiti. **Problemi:** • **Problemi di sicurezza.** La maggior parte delle configurazioni VPN all'interno del data center garantisce l'accesso totale agli utenti, il che rappresenta un problema per le organizzazioni che non vogliono che i non dipendenti, come gli appaltatori, ottengano un accesso illimitato a risorse e applicazioni sensibili. • **Non progettato per supportare un numero elevato di utenti simultanei.** A differenza dei moderni servizi cloud, il server Web del portale non può essere ampliato in modo elastico per soddisfare una domanda maggiore. Al contrario, è necessario installare più dispositivi di rete e bilanciare il carico per scalare il portale, operazione spesso costosa, complessa e inefficace, poiché il resto delle funzionalità dell'appliance potrebbe essere sottoutilizzato. • **I portali SSL-VPN clientless espongono le porte del firewall e i server Web agli attacchi.** Per consentire al server Web che ospita il portale di raggiungere le applicazioni interne, gli amministratori devono aprire le porte del firewall in entrata, esponendole ad attacchi esterni. Sia le porte aperte che il server Web stesso devono essere protetti da attacchi DDoS e applicazioni Web, che richiedono una configurazione più complessa e costi più elevati per proteggere questo metodo di connettività.



Sebbene le VPN forniscano un livello base di privacy per gli utenti remoti, non sono state progettate pensando alla sicurezza o alla scalabilità. Tradizionalmente, le organizzazioni hanno sempre utilizzato le VPN per connettere alcuni utenti remoti alla rete aziendale per brevi periodi di tempo. Man mano che il lavoro remoto è diventato più diffuso, tuttavia, i problemi VPN hanno iniziato a moltiplicarsi:

- **Gli utenti sperimentano prestazioni lente.** Se l'infrastruttura VPN non è in grado di gestire il throughput del traffico e le connessioni simultanee create dalla propria forza lavoro, gli utenti subiscono un rallentamento della connessione Internet. Inoltre, quando le VPN si trovano a grande distanza sia dall'utente che dal server delle applicazioni a cui stanno tentando di accedere, il tempo di percorrenza risultante crea latenza.
- **Le reti aziendali restano vulnerabili agli attacchi.** Le VPN in genere utilizzano un modello castello e fossato, in cui a un utente viene concesso l'accesso illimitato a tutte le risorse aziendali una volta connesso a una rete. Senza un metodo integrato per limitare l'accesso all'infrastruttura e ai dati critici, le organizzazioni sono costrette a configurare servizi di sicurezza complessi e costosi come i firewall di nuova generazione e il controllo dell'accesso alla rete o sono vulnerabili a movimenti laterali dannosi, con conseguenti violazioni dei dati più grandi.

Il problema dei servizi VPN in hosting

Alcuni fornitori hanno spostato l'appliance di rete che esegue il servizio VPN nel cloud pubblico, dove viene eseguita come macchina virtuale in uno o più datacenter. La VPN può essere collegata o meno (o con daisy-chain) a servizi di sicurezza aggiuntivi.

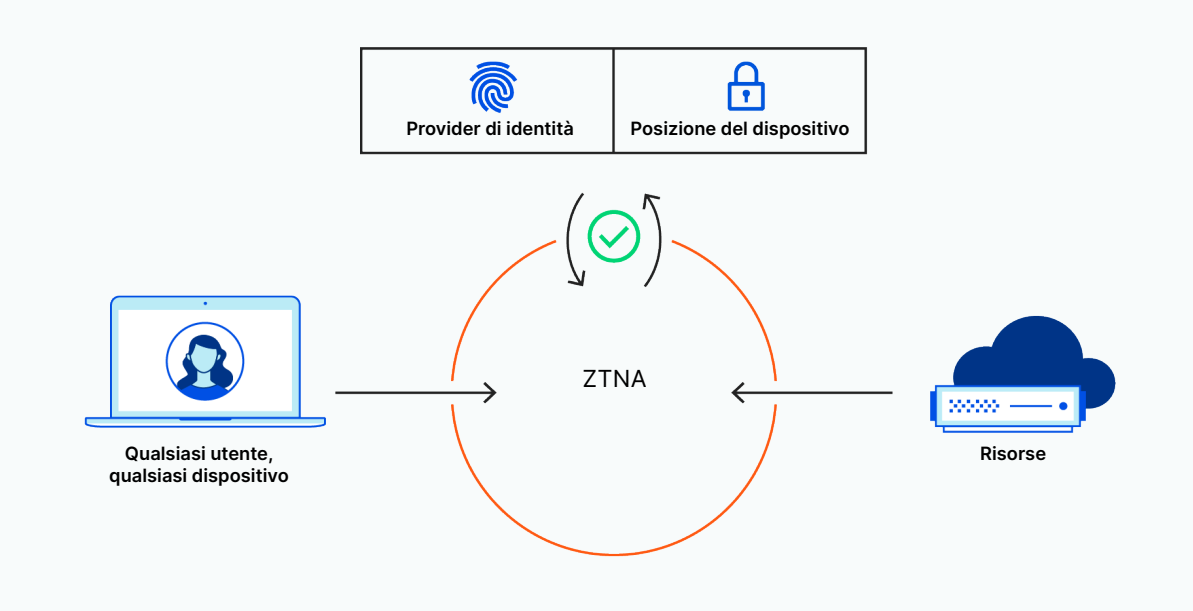
L'inserimento di una VPN nel cloud può sembrare che risolva alcuni dei problemi di scalabilità inerenti alle appliance VPN hardware. Tuttavia, ciò comporta anche alcuni problemi significativi in termini di sicurezza e scalabilità.

Ad esempio, si consideri un'organizzazione che ospita un NGFW completo (firewall di nuova generazione), che combina la VPN con un firewall e funzionalità di sicurezza aggiuntive. Poiché NGFW viene offerto come servizio in bundle, è impossibile scalare in modo indipendente qualsiasi funzionalità specifica su richiesta. L'aumento di una funzione richiede l'aumento dell'intero servizio; per fare ciò, è necessario avviare più macchine virtuali per bilanciare il carico di una piccola quantità di calcolo eseguita in ogni macchina virtuale. Non solo si tratta di una soluzione poco pratica e ingombrante, ma è probabile che comporti costi elevati poiché le esigenze di accesso remoto dell'organizzazione continuano ad espandersi.

APPROCCIO 2: ZERO TRUST NETWORK ACCESS

La sicurezza Zero Trust aggira molti dei problemi inerenti alle VPN. Si basa sul principio che nessun utente o dispositivo all'interno o all'esterno di una rete può essere considerato affidabile per impostazione predefinita. Al fine di ridurre il rischio e l'impatto di violazioni dei dati, attacchi interni e altre minacce, un approccio Zero Trust...

- autentica e registra ogni accesso e richiesta,
- richiede una verifica rigorosa di tutti gli utenti e dispositivi,
- limita le informazioni a cui ogni utente e dispositivo può accedere in base all'identità e al contesto
- e aggiunge la crittografia end-to-end per isolare applicazioni e dati all'interno della rete.



Come con le VPN, ci sono diversi modi in cui ZTNA può essere configurato:

1. **ZTNA clientless (o avviato da servizi)** utilizza il browser esistente, invece di un client, per creare una connessione sicura e autenticare i dispositivi degli utenti. Tradizionalmente, ZTNA clientless era limitato ad applicazioni con protocolli HTTP/HTTPS, ma la compatibilità si sta evolvendo rapidamente.[2]
   - **Vantaggio:** ZTNA clientless utilizza una connessione con proxy inverso per impedire l'accesso diretto alle applicazioni, impedendo agli utenti di accedere ad applicazioni e dati che potrebbero non avere il permesso di visualizzare e consentendo agli amministratori un maggiore controllo e flessibilità nella gestione.
2. **ZTNA basato su client (o avviato da endpoint)** installa il software su un dispositivo utente prima che una connessione crittografata possa essere stabilita tra l'agente di controllo e le applicazioni autorizzate.
   - **Vantaggio:** ZTNA basato su client consente agli amministratori una visione più approfondita della posizione del dispositivo, la posizione e il contesto di rischio degli utenti che accedono alle applicazioni, quindi è possibile creare e applicare criteri più granulari. Inoltre, poiché questo metodo non è limitato a HTTP/HTTPS, può essere utilizzato per accedere a una gamma più ampia di applicazioni non HTTP, come quelle che si basano su SSH, RDP, VNC, SMB e altre connessioni TCP.

[2] A partire da giugno 2021, la soluzione ZTNA di Cloudflare supporta l'accesso clientless alle applicazioni SSH e VNC, con supporto per RDP pianificato in futuro.

Problemi legati all'implementazione di ZTNA

Sebbene ZTNA offra chiari vantaggi rispetto alle VPN tradizionali, non è un approccio impeccabile per la protezione dell'accesso alla rete per gli utenti remoti. Poiché le aziende valutano i pro e i contro dell'adozione di Zero Trust, possono riscontrare uno o più dei seguenti problemi:

Le soluzioni non sono veramente native per il cloud.

Se un fornitore non offre ZTNA basato su cloud, il che significa che i suoi clienti sono tenuti a distribuire il software nei propri datacenter, gli utenti perdono vantaggi chiave come scalabilità istantanea e throughput illimitato.

I fornitori potrebbero non offrire opzioni ZTNA basate su client e clientless.

Ciò limita il valore per le organizzazioni che devono connettere gli utenti ad applicazioni non HTTP come desktop remoti, applicazioni SSH o condivisioni di file.

La configurazione può essere complessa e richiedere molto tempo.

I fornitori che non offrono supporto per l'orchestrazione e l'automazione delle politiche (tramite strumenti come Terraform) possono introdurre più lavoro manuale per gli amministratori, oltre alla configurazione già in corso in un provider di identità.

APPROCCIO DI CLOUDFLARE ALL'ACCESSO REMOTO

La protezione e la scalabilità dell'accesso remoto dovrebbero essere un processo continuo, che non sovrappone soluzioni di sicurezza ingombranti, non crea compromessi in termini di prestazioni o non comporta costi inutili. Cloudflare consente ai team di gestire tutti i casi d'uso di accesso remoto, con i seguenti vantaggi:

- **Onboarding semplice e senza rischi per utenti e amministratori.** Cloudflare si integra facilmente con i provider di identità e le piattaforme di protezione degli endpoint esistenti per applicare policy Zero Trust che limitano l'accesso alle applicazioni e alle risorse aziendali.
- **Flessibilità per implementazioni ZTNA basate su client e clientless**. Cloudflare fornisce supporto clientless per connessioni ad applicazioni Web, SSH, VNC (e presto, RDP) e supporto basato su client per applicazioni non HTTP e routing privato a IP interni.

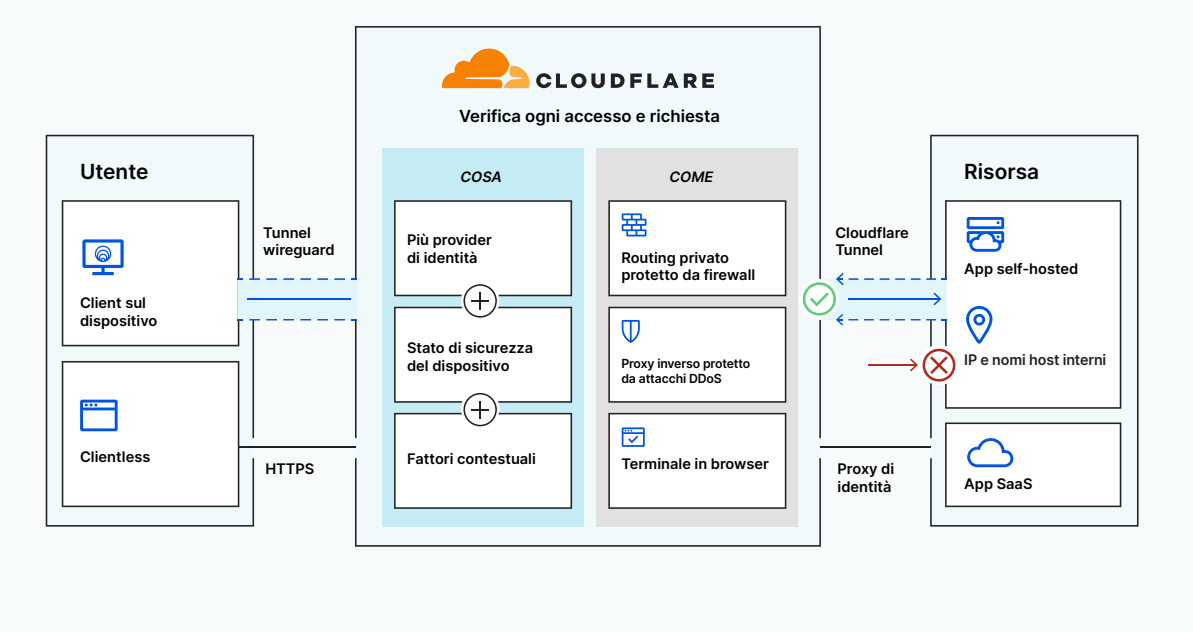


Tabella 1: In che modo Cloudflare affronta i problemi di accesso remoto

⚠ Problema	✓ Soluzione	⚙ Implementazione Cloudflare
Difficile da scalare	Rete perimetrale globale	I problemi di scalabilità affliggono sia le VPN che i servizi ZTNA che non sono nativi del cloud, rendendo difficile per gli utenti remoti l'accesso alle applicazioni e ai dati. La rete globale Anycast di Cloudflare non solo rende le connessioni degli utenti più veloci di una VPN, ma garantisce anche che la forza lavoro remota di qualsiasi dimensione possa connettersi in modo sicuro e rapido alle risorse aziendali secondo necessità senza richiedere una configurazione aggiuntiva che richiede tempo da parte degli amministratori.
Scarsa compatibilità con i dispositivi mobili	Client leggero	Le soluzioni VPN e ZTNA che utilizzano i protocolli IPSec e SSL hanno spesso scarse prestazioni sui dispositivi mobili e in roaming. Il client Cloudflare WARP utilizza il più moderno protocollo Wireguard, che viene eseguito nello spazio utente per supportare un insieme più ampio di opzioni del sistema operativo con un'esperienza utente più rapida rispetto alle opzioni tradizionali. Il client WARP di Cloudflare può essere configurato su dispositivi Windows, MacOS, iOS, Android e presto Linux.
Nessuna protezione DDoS integrata o debole	Protezione da attacchi DDoS leader del settore integrata	Senza la protezione DDoS integrata, le organizzazioni sono spesso costrette a collegare a cascata i servizi di sicurezza aggiuntivi che possono creare problemi di configurazione, di scalabilità e di sicurezza. La rete da oltre 67 Tb/s di Cloudflare fornisce protezione DDoS integrata per qualsiasi modalità ZTNA, difendendo le reti dai più grandi attacchi volumetrici.
Limitazioni del protocollo	Supporto per le app non Web	✓ Compatibilità tra le modalità: ZTNA clientless per applicazioni SSH/VNC; ZTNA basato su client per tutte le altre applicazioni non Web.
Nessun firewall di rete integrato	Firewall di rete integrato	Man mano che le reti aziendali crescono, cresce anche lo stack di hardware di sicurezza che le organizzazioni devono bilanciare, causando compromessi in termini di costi, prestazioni e sicurezza. Cloudflare consente agli amministratori di applicare le policy del firewall di rete al perimetro, offrendo un controllo dettagliato su quali dati sono consentiti in entrata e in uscita dalla rete e migliorando la visibilità sul modo in cui il traffico scorre attraverso di essa. ✓ Compatibilità tra le modalità: ZTNA basato su client
Mancanza di controllo dettagliato	Secure Web Gateway (SWG) integrato	L'uso non autorizzato delle applicazioni può causare problemi di sicurezza significativi per le organizzazioni; senza politiche rigorose in atto, gli utenti possono accedere e manomettere dati sensibili e altre risorse aziendali. Combinando ZTNA con SWG, Cloudflare consente agli amministratori di esercitare un controllo più dettagliato sui diritti di accesso di utenti e dispositivi all'interno delle applicazioni, in modo che utenti e gruppi basati sui ruoli abbiano accesso solo alle risorse di cui hanno bisogno. ✓ Compatibilità tra le modalità: ZTNA basato su client

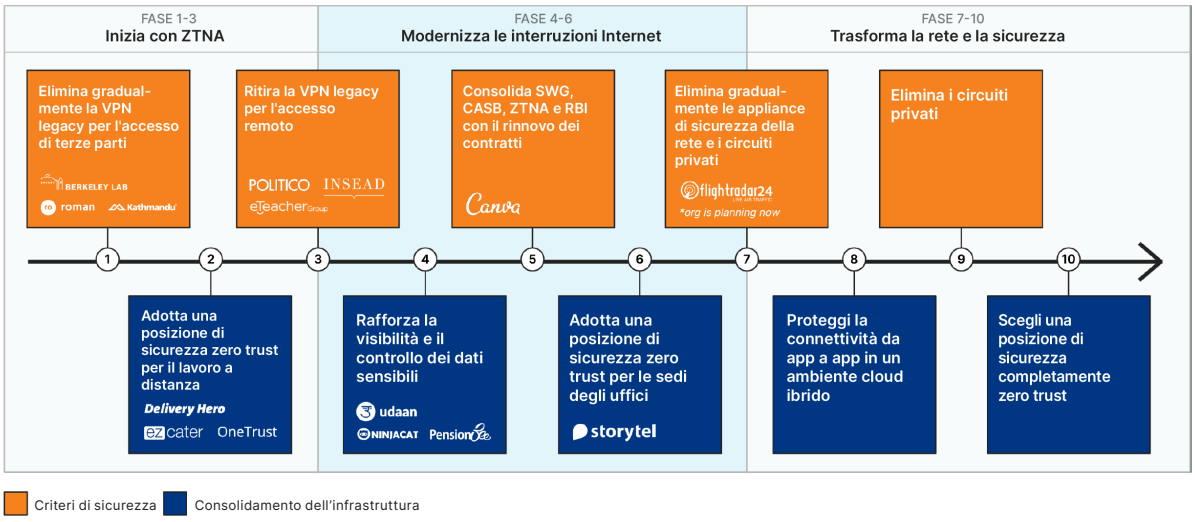
SOSTITUISCI LA TUA VPN LEGACY CON ZERO TRUST NETWORK ACCESS

Le promesse di Zero Trust possono sembrare vane per i leader della sicurezza IT nel mezzo di una lunga e dolorosa transizione verso una sicurezza senza VPN. Ma è possibile sostituire la tua VPN con Zero Trust Network Access senza fare compromessi nel supporto del protocollo o nella funzionalità.

Il percorso di migrazione consigliato varia in base alle priorità aziendali che guidano il tuo progetto:

- Se la connettività più rapida alle applicazioni è la tua priorità, distribuisci prima **ZTNA basato su client per app non Web**.
- Se è più importante migliorare la sicurezza delle regole di accesso alle applicazioni, inizia con le **applicazioni Web**.

La sostituzione della tua VPN è solo il primo passo di una trasformazione completa della rete. Poiché la transizione a un modello SASE può essere schiacciante, abbiamo suddiviso un percorso comune verso la sicurezza Zero Trust in base all'approccio adottato dai nostri clienti:



Scopri di più su come la piattaforma Zero Trust di Cloudflare può aiutarti a ridurre la dipendenza dalla tua VPN ed eventualmente a sostituirla.

Ulteriori informazioni

Guarda un confronto nel mondo reale tra VPN e ZTNA e come Cloudflare Access migliora la sicurezza per l'accesso alle applicazioni.

Guarda la demo

APPENDICE

Modernizza le interruzioni Internet

L'implementazione di ZTNA è un passo importante nella distribuzione di un modello Secure Access Service Edge (SASE). **Cloudflare One** è una soluzione NaaS (network-as-a-service) completa che semplifica e protegge la rete aziendale per team di tutte le dimensioni. Con Cloudflare One, le organizzazioni possono:

- **Adottare l'accesso Zero Trust.** Sostituisci ampi perimetri di sicurezza con una verifica individuale di ogni richiesta a ogni risorsa. Applica le regole Zero Trust a ogni connessione alle tue applicazioni aziendali, indipendentemente da chi siano gli utenti e dove si trovino.
- **Proteggere il traffico Internet.** Quando le minacce su Internet si muovono velocemente, le difese che usi per fermarle devono essere più proattive. Cloudflare One protegge i dipendenti remoti dalle minacce su Internet e applica policy che impediscono ai dati preziosi di lasciare l'organizzazione applicando l'isolamento zero trust del browser su qualsiasi sito con un'esperienza utente fluida e immediata.
- **Proteggere e connettere uffici e datacenter.** Il networking aziendale è diventato eccessivamente complicato, il che significa che il traffico degli utenti deve spesso viaggiare attraverso più hop per arrivare dove deve andare. Con Cloudflare One, le aziende possono proteggere uffici e data center attraverso un'unica piattaforma cloud unificata e coerente.

Per ulteriori informazioni su Cloudflare One, guarda una introduzione e una demo di 10 minuti.

Trasforma la tua rete

Prossimamente, le offerte Zero Trust e WAN as-a-service di Cloudflare convergeranno all'unisono, consentendo ai tuoi dipendenti di accedere alle risorse aziendali in modo coerente, ovunque lavorino.

Oggi, i tuoi prodotti VPN e WAN consentono ai tuoi dipendenti di accedere alle risorse che si trovano all'interno della tua rete aziendale privata, ma ti obbligano a gestire la connettività e le politiche di sicurezza in modo diverso.

Ora, Cloudflare fornisce un piano di controllo unificato, offrendoti una maggiore flessibilità per applicare le stesse politiche di sicurezza Zero Trust all'intera forza lavoro e al posto di lavoro senza dover destreggiarsi tra più prodotti puntuali.

Per saperne di più, visita il sito all'indirizzo https://www.cloudflare.com/it-it/cloudflare-one/.

TIPO DI DOCUMENTO