eBook

I 6 casi d'uso più convincenti per la sostituzione completa di una VPN legacy

netskope

Introduzione

L'infrastruttura VPN di accesso remoto legacy ha rappresentato a lungo un problema di sicurezza. La sua estesa connettività di rete attira gli aggressori e consente movimenti laterali non autorizzati. Costringere gli utenti remoti a effettuare il backhaul del traffico non locale attraverso la VPN solo per tornare su internet compromette l'esperienza utente e comporta sia costi elevati che complessità di routing.

ZTNA è l'alternativa moderna alle VPN di accesso remoto legacy per le aziende che intendono modernizzare la connettività per la forza lavoro ibrida. Ma non tutte le soluzioni ZTNA consentono di sostituire completamente le VPN.

Per eseguire con successo l'upgrade da VPN legacy a ZTNA, consigliamo di identificare e dare la priorità ai casi d'uso principali quando si pianifica una migrazione completa. Combinare una pianificazione ben fatta con gli investimenti tecnologici giusti consentirà ai team di soddisfare finalmente la promessa di mandare definitivamente in pensione la VPN.

1. Emancipare i lavoratori ibridi

Ormai la gran parte dei dipendenti preferisce il modello di lavoro ibrido, ma le soluzioni VPN legacy si rivelano inadeguate ad affrontare le sfide essenziali in termini di sicurezza e connettività necessarie per emancipare la forza lavoro. L'accesso remoto con VPN fornisce poca visibilità sulle attività relative alle applicazioni, soffre di problemi di latenza e prestazioni a causa del backhauling del traffico, e fornisce ampio accesso a livello di rete per gli utenti autenticati, estendendo quindi la superficie d'attacco a causa dell'assenza di limitazioni ai movimenti laterali. Inoltre, i concentratori VPN con vulnerabilità non patchate sono i principali vettori per gli attacchi informatici.

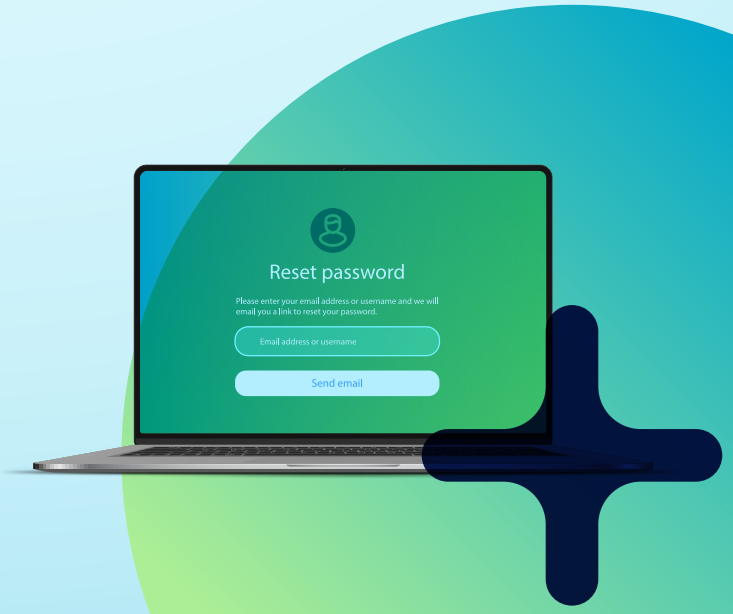
Passare da una soluzione VPN remota legacy a una soluzione ZTNA come Netskope One Private Access consente alle organizzazioni di affrontare i rischi per la sicurezza legati alle VPN, grazie all'accesso con privilegi minimi consapevole dell'identità e del contesto alle applicazioni private, minimizzando i movimenti laterali non autorizzati. Netskope One Private Access offre visibilità in tempo reale sul traffico delle applicazioni e sulle attività degli utenti, consentendo un'applicazione coerente delle policy per i dipendenti che si collegano da qualsiasi posizione, sia remota che on-premise. Inoltre, la soluzione può stabilire una connettività di pre-accesso sicura, facilitando l'onboarding in sicurezza di nuovi dispositivi e il ripristino della password per i lavoratori remoti, nonché garantire che solo i dispositivi autorizzati abbiano accesso a risorse interne critiche come i servizi directory.

11 ore all'anno
perse dai dipendenti per reimpostare le password[1]

CONSIGLI PER L'IMPLEMENTAZIONE:

Un inventario delle implementazioni VPN è un buon modo per iniziare ad aggiornare la tua infrastruttura. Questo deve includere:

- **Quante istanze di servizi VPN di accesso remoto vengono gestite attualmente**
- **Quale flusso di traffico delle applicazioni sta attraversando queste VPN di accesso remoto**
- **Utenti nominati con accesso VPN a queste applicazioni**



[1]Business Reporter, "*How much time does your organisation spend on managing passwords?*", 7 settembre 2022. https://www.independent.co.uk/news/business/business-reporter/time-organisation-managing-passwords-b2161856.html

2. Accelerare la migrazione al cloud

La trasformazione digitale ha raggiunto un punto di svolta: Più carichi di lavoro sono ora ospitati su cloud pubblici rispetto ai data center privati. Di conseguenza, la connettività ai servizi IaaS per gli utenti sia on-premises che remoti è stata al centro dell'attenzione e rappresenta una delle principali preoccupazioni quando le organizzazioni pianificano la loro strategia e implementazione cloud. In una tipica infrastruttura VPN di accesso remoto, il traffico utente viene instradato attraverso il data center privato e quindi collegato ai cloud IaaS tramite MPLS o altri tunnel pin-up come AWS Direct Connect o Azure ExpressRoute. Oltre a rendere insoddisfacente l'esperienza utente, il backhauling del traffico aumenta le spese per l'infrastruttura, e in più richiede un routing di rete complesso.

Come alternativa moderna alle VPN di accesso remoto legacy, Netskope consente una connettività efficiente al cloud pubblico senza necessità di percorsi tortuosi. La connessione è sicura, flessibile e altamente scalabile. Netskope One Private Access contribuisce alla protezione dei dati e delle risorse con il controllo dell'accesso a livello di applicazione basato sull'identità dell'utente e il posizionamento di sicurezza del dispositivo. Grazie alla connettività logica e non basata sull'indirizzo IP, semplifica notevolmente le operazioni cloud e di rete, supporta l'automazione ed elimina il backhauling del traffico.

CONSIGLI PER L'IMPLEMENTAZIONE:

Le organizzazioni che mirano a sostituire l'accesso remoto VPN devono anche cercare istanze cloud VPN, come AWS Client VPN o Azure VPN Gateway. Devono sfruttare strumenti di automazione come i moduli Terraform per automatizzare la distribuzione, la configurazione e la scalabilità di Netskope One Private Access Publishers in esecuzione in EC2 e altri ambienti cloud.

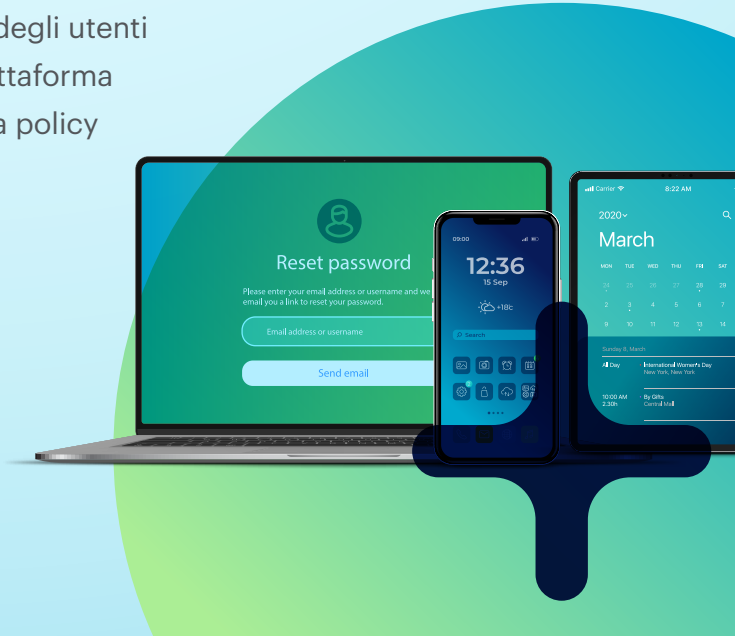
3. Facilitare l'accesso ai dispositivi non gestiti (quando è una scelta sensata)

Le organizzazioni devono garantire a collaboratori esterni, fornitori di servizi e partner un accesso sicuro alle risorse aziendali. Allo stesso tempo, i dipendenti devono disporre di un accesso fluido alle risorse private tramite i propri dispositivi personali. Ciò comporta la sfida di facilitare l'accesso ai dispositivi non gestiti senza il rischio di esporre le risorse sulla rete Internet pubblica o DMZ. Richiedere l'utilizzo di software client dedicato potrebbe non essere praticabile, poiché gli utenti potrebbero essere riluttanti a installare software sui propri dispositivi personali. Concedere l'accesso VPN a dispositivi non gestiti può comportare un accesso toppo esteso.

È possibile fornire in modo sicuro l'accesso ai dispositivi non gestiti per gli utenti terze e quarti e consentire il BYOD dei dipendenti senza i rischi associati a VPN, DMZ o all'esposizione delle risorse sull'Internet pubblico. Netskope One Private Access supporta la distribuzione senza client per i dispositivi non gestiti, fornendo un accesso Zero Trust sicuro alle applicazioni private, ospitate localmente o sul cloud.

L'implementazione ZTNA senza client consente accessi senza attriti e basati su browser tramite un'architettura reverse-proxy integrata con i provider di identità (IdP) per l'autenticazione degli utenti che tentino di accedere alle applicazioni private. Sfruttare gli stessi controlli DLP sulla piattaforma Netskope One SSE consente alle organizzazioni di mantenere una visibilità granulare e una policy di protezione dei dati coerente su tutti i dispositivi, sia gestiti che non gestiti.

In media, un dipendente utilizza **2,5 dispositivi al lavoro**, inclusi dispositivi non aziendali come laptop personali, smartphone e tablet.[2]



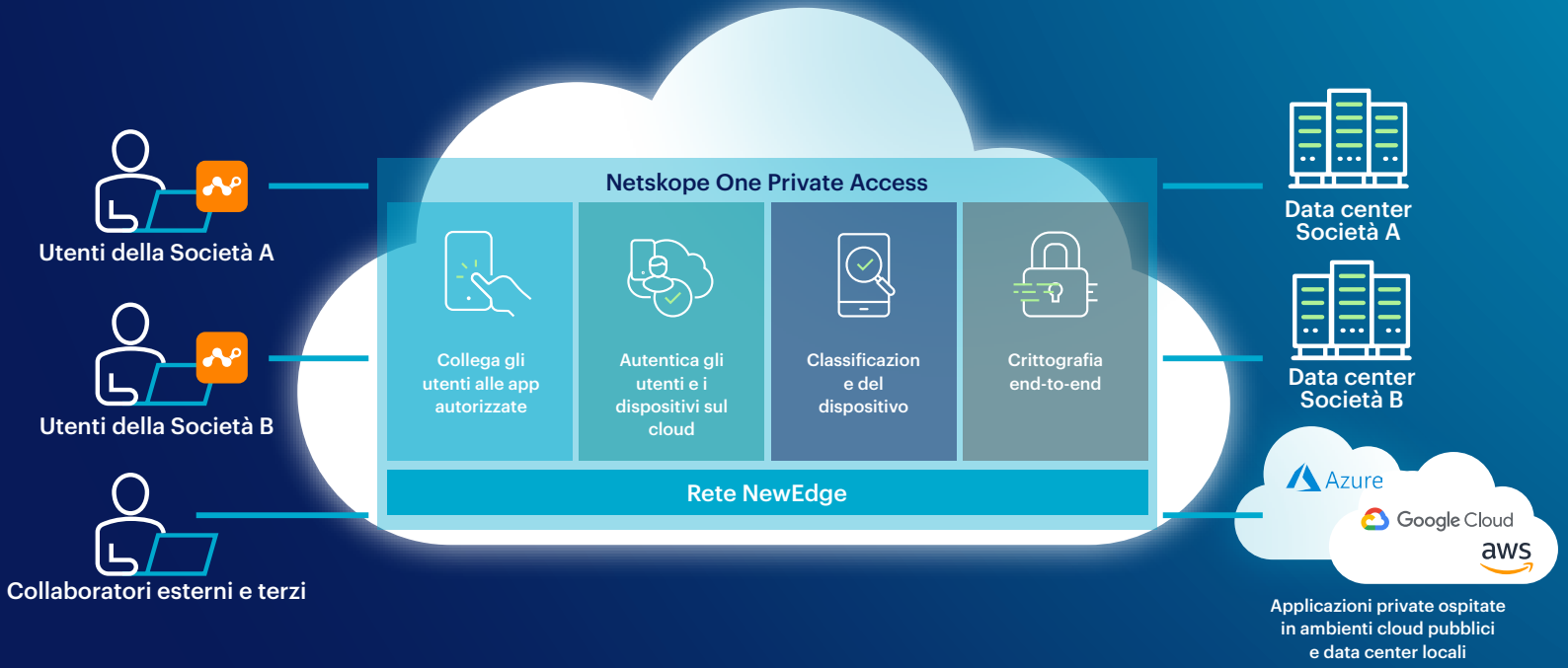
[2]Zippia. *"26 Surprising BYOD Statistics [2023]: BYOD Trends In The Workplace"* Zippia.com. 17 ottobre 2022. https://www.zippia.com/advice/byod-statistics/

4. Accelerare l'integrazione M&A

Le attività di fusione e acquisizione (M&A) sono rapide e ad alto rischio, e il tempo è un fattore determinante. Le operazioni di fusione e acquisizione presentano ai team IT, di networking e di sicurezza una serie unica di sfide. Il successo delle operazioni di fusione e acquisizione è determinato dalla rapidità con cui viene completata l'integrazione tra le due aziende.

La sfida per i team operativi IT è quella di fornire l'accesso fin dal primo giorno, collegando gli utenti di entrambe le entità alle applicazioni interne mission-critical ma assicurando nel contempo la sicurezza dei dati sensibili. I metodi tradizionali di fusione di due reti rappresentano un processo costoso, dispendioso in termini di tempo e complesso, che spesso si traduce in conflitti di Proprietà Intellettuale, e richiede la nuova numerazione degli indirizzi. Le regole del firewall spesso non sono in grado di offrire un controllo granulare dell'accesso, rendendo vulnerabili entrambe le reti.

Fornito come soluzione unica, Netskope One Private Access integra le funzionalità ZTNA/SD-WAN in un unico client end-point leggero e consente la totale eliminazione, e non solo la sostituzione parziale, delle VPN di accesso remoto per tutti i casi d'uso relativi all'accesso alle applicazioni. Un client SASE unificato dirige automaticamente il traffico degli utenti verso le proprie destinazioni, siano esse applicazioni cloud, private, IaaS o Web. Netskope One Private Access consente alle organizzazioni di acquisire rapidamente valore commerciale durante le attività di M&A connettendo dipendenti, collaboratori e consulenti alle risorse essenziali fin dal primo giorno, anche in caso di applicazioni legacy. Questa soluzione elimina la necessità di configurare e fondere le reti VPN, consentendo alle aziende di avviare immediatamente l'integrazione in tutta sicurezza. L'accesso viene concesso in base a criteri di fiducia adattiva, tenendo conto dell'identità dell'utente, della sicurezza del dispositivo e di altri fattori contestuali. Fornire un accesso selettivo alle applicazioni e ai dati consente a Netskope One Private Access di ridurre il rischio di movimenti laterali e di esposizione delle informazioni sensibili.



Fornire accesso immediato alle risorse interne evitando la complessità di dover combinare le reti e configurare le regole VPN e i firewall da sito a sito.

5. Supportare i centri di contatto remoti

In tutto il mondo ci sono **1,8 milioni** di dipendenti di call center, e solo negli Stati Uniti il 52% di questi sono agenti da remoto.[3] Questi agenti sono rappresentanti del servizio clienti, agenti di prenotazione viaggi, fornitori di consulenza sanitaria e altri ruoli. Mentre molti call center stanno passando alla comunicazione unificata UCaaS (Unified Communication as a Service), molte organizzazioni utilizzano ancora il VoIP legacy ospitato on-premises, spesso instradando le chiamate tramite VPN di accesso remoto. Per i dipendenti dei call center in remoto, la qualità VoIP può rappresentare un problema quando si fa affidamento sulle VPN. Tendono a essere sovraccaricati, incrementando il jitter e la latenza con chiamate VoIP che possono essere frustranti per le persone su entrambe le estremità delle linee.

Fino ad ora, la maggior parte delle soluzioni ZTNA cloud non supporta i sistemi VoIP ospitati on-premise che obbligano le organizzazioni a mantenere sia l'infrastruttura ZTNA che quella VPN.

Il
52%
dei call center solo negli Stati Uniti impiega agenti da remoto

Netskope One Private Access offre funzionalità convergenti ZTNA e SD-WAN in un'unica soluzione.
La gestione dinamica del traffico e il QoS sensibile al contesto accresce la produttività dei dipendenti dei call center in remoto, grazie all'esperienza assicurata per applicazioni vocali e video, mentre il livello di sicurezza migliora con l'accesso Zero Trust a tutte le risorse interne.

[3]Fonte: *"Call Center Statistics – 2023"* Truelist.com. 1° gennaio 2023. https://truelist.co/blog/call-center-statistics/#:~:text=The%20number%20of%20people%20working,million%20currently%20to%201.8%20million.

6. Abilitare le applicazioni legacy

La verifica della compatibilità è un passaggio critico dell'aggiornamento tecnologico. Le organizzazioni che stanno implementando ZTNA devono comunque testare la compatibilità delle applicazioni. Durante questo processo, è probabile che le organizzazioni scoprano alcune applicazioni legacy incompatibili con la maggior parte delle soluzioni ZTNA più moderne. Ad esempio, le applicazioni legacy che richiedono l'avviamento del traffico dal server non funzionano bene con la "connettività inside-out" di una soluzione ZTNA moderna, che richiede che il traffico venga avviato dall'end-point. Questi sistemi legacy sono spesso proprietari e richiedono tempo e risorse, mentre riprogettazione modernizzazione devono essere pianificate attentamente (e spesso questo significa migrare verso ambienti IaaS ospitati sul cloud).

Tuttavia, Netskope One Private Access risolve tutti questi esempi relativi alle applicazioni legacy, grazie a un accesso sicuro e ottimizzato a tutte le applicazioni private da un singolo client integrato. Le organizzazioni possono quindi estendere la longevità delle applicazioni legacy, ridurre il costo della gestione di più soluzioni di accesso remoto e fornire un accesso rapido e affidabile alle applicazioni, indipendentemente da dove sono ospitate.

Conclusioni

Tenuto conto di come una volta fossero tecnologie all'avanguardia, le VPN di accesso remoto legacy ormai costituiscono una sfida sia per i team di sicurezza (come fonte di vulnerabilità a molte minacce) sia per i team di infrastruttura e operativi, per i quali influenzano le prestazioni della rete degradando di conseguenza l'esperienza utente complessiva.

Ma la maggior parte delle attuali soluzioni ZTNA non sono una panacea; se non son o in grado di risolvere tutti i casi d'uso rilevanti, le organizzazioni possono procedere solo a una sostituzione parziale delle VPN e si trovano a dover gestire un mix di infrastrutture: VPN legacy più "alcune" ZTNA, e ciò può risultare ancora più complesso della situazione precedente.

Netskope One Private Access è progettato per aiutare le organizzazioni ad accelerare l'adozione di ZTNA Zero Trust utilizzando una soluzione completamente integrata che favorisce la sostituzione riuscita dell’intera infrastruttura VPN. Fornisce un percorso chiaro per completare la sostituzione delle VPN di accesso remoto per tutti i casi d'uso di accesso alle applicazioni, riduce la superficie digitale di attacco e migliora la postura di sicurezza grazie ai principi Zero Trust, aumentando la produttività dei lavoratori in remoto con un'esperienza di accesso ottimizzata e priva di intoppi alle applicazioni.

A proposito di Netskope One Private Access

Netskope One Private Access offre funzionalità SD-WAN a ZTNA per consentire una connettività sicura e ottimizzata a tutte le applicazioni private, tra cui VoIP ospitate on-premises, video e assistenza da remoto, consentendo alle organizzazioni di:

- Modernizzare la connettività e aumentare la sicurezza.
- Migliorare l'esperienza utente.
- Offrire un accesso ottimizzato e altamente affidabile alle applicazioni vocali e video.
- Ridurre la complessità e i costi operativi.
- Accelerare i piani per eliminare l'infrastruttura VPN legacy di accesso remoto eliminando la necessità di mantenere strumenti di accesso da remoto separati.
- Ottenere visibilità e controllo senza precedenti sul traffico delle applicazioni.

Netskope One Private Access consente la completa eliminazione, e non solo la sostituzione parziale, delle VPN di accesso remoto per tutti i casi d'uso relativi all'accesso alle applicazioni, migliorando nel frattempo il posizionamento di sicurezza con accessi ottimizzati e senza interruzioni alle applicazioni.

A proposito di Netskope

Netskope, leader globale SASE, aiuta le organizzazioni ad applicare i principi Zero Trust e le innovazioni AI/ML per proteggere i dati e difendersi dalle minacce informatiche. Veloce e intuitiva, la piattaforma Netskope One e il suo motore Zero Trust brevettato offrono accesso ottimizzato e sicurezza in tempo reale a persone, dispositivi e dati, ovunque vadano. Migliaia di clienti si affidano a Netskope e alla sua potente rete NewEdge per ridurre i rischi e ottenere una visibilità senza pari su qualsiasi attività cloud, web e applicazioni private, fornendo sicurezza e accelerando le prestazioni senza compromessi. Per saperne di più su **netskope.com**.

Interessati ad approfondire?

Richiedi una DEMO

netskope

06/25 EB-674-3-IT