eBook

10 funzionalità essenziali per ZTNA

netskope

Indice

Introduzione

L'ascesa delle tecnologie cloud, delle infrastrutture decentralizzate e della forza lavoro remota ha reso obsoleti i tradizionali perimetri di sicurezza, esponendo le limitazioni delle VPN. Oggi, le VPN sono spesso inadeguate, in difficoltà a causa delle superfici di attacco più ampie, dei costi elevati, della maggiore latenza e di una visibilità limitata sulle prestazioni delle applicazioni.

Zero Trust Network Access (ZTNA) offre un'alternativa basata sul cloud, adattata alle attuali esigenze nell'ambito della sicurezza. ZTNA minimizza i rischi, riduce le superfici di attacco e impedisce movimenti laterali non autorizzati all'interno delle reti poiché concede un accesso alle applicazioni controllato e basato sui ruoli, in base all'identità dell'utente e al contesto del dispositivo. A differenza delle VPN, ZTNA si avvale di un broker affidabile per connettere gli utenti alle applicazioni, senza esporli alla rete pubblica. Grazie all'integrazione perfetta nelle soluzioni Security Service Edge (SSE), ZTNA garantisce una connettività sicura e flessibile tra ambienti locali, cloud e ibridi, migliorando la sicurezza e le prestazioni.

Non tutte le soluzioni ZTNA sono uguali: scopri i 10 fattori indispensabili che rendono eccezionale una soluzione ZTNA.

Ritorno alle origini: Che cosa è ZTNA?

ZTNA fornisce un accesso controllato, basato sui ruoli e con privilegi minimi alle applicazioni e alle risorse, valutando l'identità degli utenti e dei loro dispositivi, nonché fattori contestuali come ora, data, geolocalizzazione e posizionamento del dispositivo. Crea un perimetro sicuro attorno alle risorse e gestisce il flusso di rete, in cui anche piccoli cambiamenti, come una modifica al posizionamento del dispositivo, possono innescare la revoca dell'accesso in tempo quasi reale.

ZTNA opera secondo un approccio che nega l'accesso per impostazione predefinita, e aderisce ai principi Zero Trust che lo concedono su base "just-in-time" solo a risorse specifiche. Agli utenti viene concesso l'accesso solo alle applicazioni autorizzate, e questo accesso viene continuamente monitorato e rivalutato. L'obiettivo è ridurre il rischio riducendo la superficie di attacco e avvicinando i controlli di sicurezza alle risorse protette.

Inoltre, ZTNA elimina la necessità di esposizione diretta delle applicazioni alla rete Internet pubblica. Invece di connettersi direttamente, un broker di fiducia facilita la connessione tra utenti e applicazioni. Questo broker può essere un servizio cloud gestito, un servizio autonomo in un data center o un apparecchio virtuale in un cloud IaaS. Una volta verificate le credenziali dell'utente e il contesto del dispositivo, il broker comunica con un connettore di app, situato vicino all'applicazione. Il connettore di app stabilisce quindi una connessione sicura all'applicazione privata e un percorso di comunicazione in uscita con il broker.

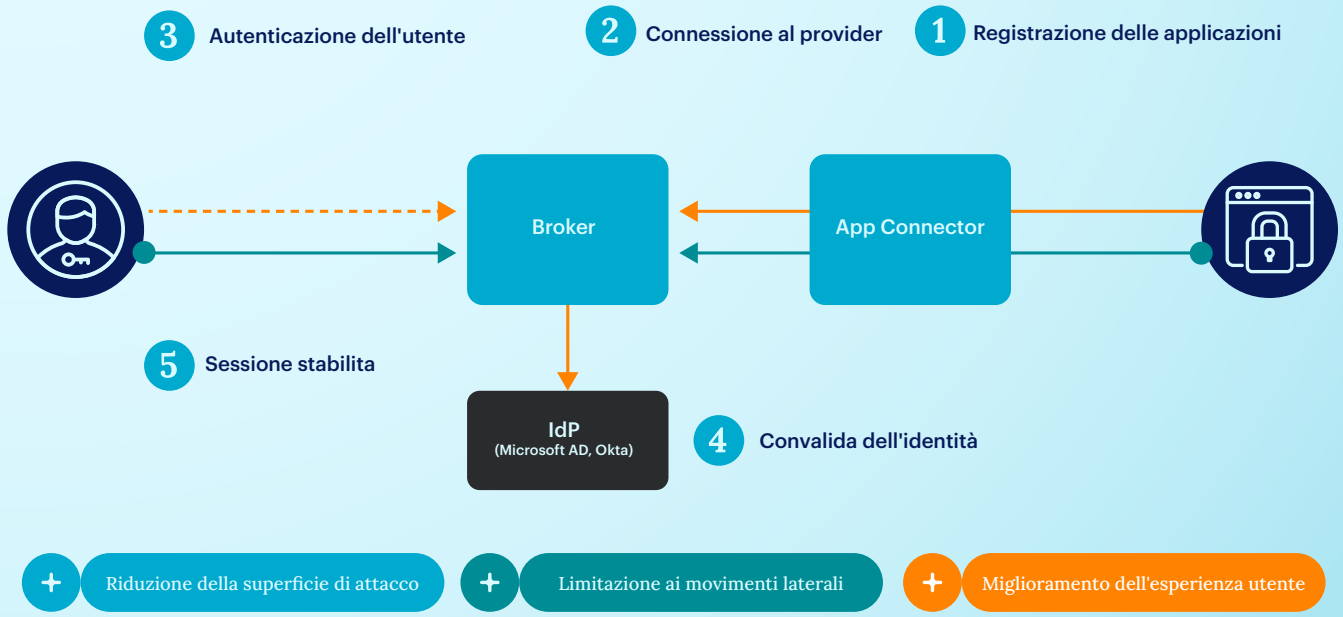


Figura 1: Come funziona Zero Trust Network Access

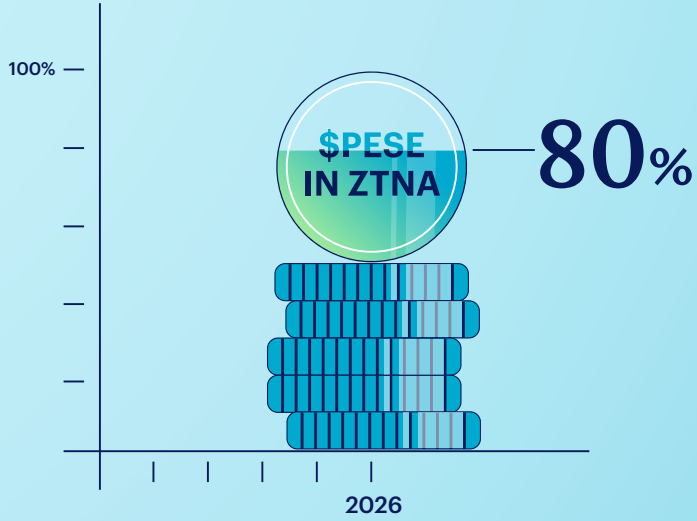
In che modo ZTNA è fondamentale per SSE? E come questa integrazione aiuta i clienti?

Security service edge (SSE) consolida i servizi di sicurezza chiave, tra cui ZTNA, Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) e la prevenzione della perdita dei dati (Data Loss Prevention - DLP), in una piattaforma unificata e basata su cloud.

Come componente centrale di SSE, ZTNA fornisce un accesso sicuro, granulare e condizionato ad applicazioni e servizi. Gestisce i controlli di accesso e l'autenticazione per le risorse sia locali che sul cloud. ZTNA applica controlli di accesso adattivi e contestuali basati sul comportamento dell'utente, su salute e posizionamento dei dispositivi nonché su altri indicatori di rischio, garantendo una protezione coerente su tutti i servizi di sicurezza all'interno del framework SSE. Secondo Gartner, entro il 2026 l'80% della spesa ZTNA avrà luogo come parte di acquisti SASE, SASE gestito o SSE più estesi, rispetto al 40% del 2022 [1].

SSE si avvale dei dati in tempo reale di ZTNA per apportare
correzioni dinamiche alla sicurezza. Ad esempio, in caso di compromissione di un dispositivo, SSE può modificare automaticamente i controlli di accesso e attivare servizi aggiuntivi, come DLP, per prevenire violazioni dei dati o accessi non autorizzati.

L'uso di ZTNA all'interno di SSE migliora la sicurezza e l'esperienza utente, semplifica la gestione e supporta la scalabilità. Questo allineamento consente alle organizzazioni di adottare un modello di sicurezza Zero Trust moderno, per proteggere le proprie risorse adattandosi a un panorama delle minacce in continua evoluzione.



> Secondo Gartner, entro il 2026 l'80% della spesa ZTNA avrà luogo come parte di acquisti SASE, SASE gestito o SSE più estesi, rispetto al 40% del 2022 [1]

[1] *Gartner, Competitive Behaviors in the ZTNA Platform Market*, a cura di Evan Zeng, Charanpal Bhogal, 12 agosto 2024

1 | Autenticazione con privilegi minimi basata sull'identità

01

L'autenticazione fornisce sicurezza, ma la sua staticità può comportare lacune, problemi di conformità, insoddisfazione degli utenti una sicurezza più debole per un'organizzazione.

Le credenziali compromesse sono una minaccia comune e i metodi di sicurezza tradizionali spesso applicano una protezione uniforme a tutti gli utenti, con conseguenti vulnerabilità in situazioni ad alto rischio o inutili attriti in quelle a basso rischio. Sebbene l'autenticazione sia cruciale, il suo vero valore sta nel fatto di essere flessibile e consapevole del contesto. Senza un'autenticazione adattiva adeguata, le organizzazioni sono a maggior rischio di violazioni della sicurezza, compromissioni di account e minacce interne, in quanto non hanno la capacità di rispondere ai fattori contestuali in tempo reale.

L'autenticazione con privilegi minimi basata sull'identità affronta queste sfide applicando all'autenticazione un approccio dinamico e consapevole del contesto. Regola le misure di sicurezza in base al livello di rischio valutato per il tentativo di accesso dell'utente. In una soluzione ZTNA, questo metodo migliora la sicurezza valutando continuativamente il rischio di ogni richiesta di accesso e adattando di conseguenza i requisiti di autenticazione. Integrando le valutazioni dei rischi in tempo reale con il controllo degli accessi, questo approccio supporta un solido quadro di sicurezza Zero Trust.

L'implementazione dei privilegi minimi basati sull'identità in ZTNA comporta la definizione di politiche di sicurezza, l'integrazione dell'autenticazione multifattoriale (MFA) e la configurazione delle valutazioni dei rischi contestuali. ZTNA deve includere l'autenticazione basata sull'identità con privilegi minimi, che consente agli utenti di accedere solo a ciò di cui hanno bisogno, quando ne hanno bisogno, in base alla loro identità e al contesto di accesso. Ciò minimizza il rischio, riduce la superficie di attacco e rafforza la sicurezza.

COME FACCIAMO?

Netskope One Private Access impone un accesso basato sull'identità, concedendo agli utenti solo le autorizzazioni necessarie, con supporto sia per i dispositivi gestiti (*agent-based*) che non gestiti (*agentless*).

2 | Valutazione completa del posizionamento del dispositivo

02

Non gestire il posizionamento dei dispositivi in uso aumenta significativamente il rischio di attacchi informatici, violazioni dei dati, problemi di conformità e operazioni di sicurezza inefficienti per le organizzazioni.

Con la diffusione del lavoro remoto e delle pratiche BYOD (*Bring Your Own Device*), gestire il posizionamento del dispositivo è sempre più importante. Senza un monitoraggio continuo e l'applicazione degli standard di sicurezza, le organizzazioni sono vulnerabili alle minacce provenienti da dispositivi non protetti. La gestione del posizionamento del dispositivo verifica che tutti i dispositivi, gestiti o meno, siano conformi alle politiche di sicurezza prima di accedere a risorse sensibili.

Con ZTNA, la gestione del posizionamento del dispositivo verifica la conformità prima di concedere l'accesso alle risorse di rete, valutando dinamicamente la salute e il contesto del dispositivo per consentire solo ai dispositivi sicuri l'accesso ai dati critici. Questo approccio riduce i rischi e migliora la sicurezza generale della rete.

La gestione del posizionamento dei dispositivi è essenziale in qualsiasi soluzione ZTNA per affrontare sicurezza, conformità, mitigazione delle minacce e risposta agli incidenti, applicando i principi Zero Trust. Ad esempio, se un dispositivo con credenziali aziendali viene rubato, i controlli di posizionamento rilevano la non conformità e attivano avvisi durante i tentativi di accesso.

Avere la certezza che solo i dispositivi sicuri accedano alle proprie reti consente alle organizzazioni di mantenere un solido posizionamento di sicurezza Zero Trust.

COME FACCIAMO?

Netskope One Private Access valuta continuamente la salute e la conformità dei dispositivi gestiti e non gestiti, offrendo una valutazione del rischio in tempo reale prima di concedere l'accesso.

3 | Micro-segmentazione avanzata con politiche basate sull'identità

03

Modelli di sicurezza e metodi di segmentazione di rete convenzionali spesso non riescono a gestire le complessità dei moderni ambienti IT, portando a un aumento dei rischi e a una maggiore esposizione alle vulnerabilità.

Le organizzazioni che non dispongono di controlli di sicurezza avanzati affrontano rischi maggiori di violazioni dei dati, accesso non autorizzato e uso inefficiente delle risorse di rete, rendendo più difficile la protezione dei i dati sensibili, il rispetto delle normative e la difesa dalle minacce in continua evoluzione. La micro-segmentazione avanzata con politiche basate sull'identità affronta queste sfide offrendo un controllo preciso dell'accesso alla rete e applicando le politiche di sicurezza in base all'identità dell'utente, al posizionamento del dispositivo e al contesto dell'applicazione.

Questo approccio divide la rete in micro-segmenti sicuri, controllando l'accesso a ciascuno di essi in base alle identità degli utenti e ai fattori contestuali. Rafforza la sicurezza implementando il principio del privilegio minimo e applicando controlli di accesso dinamici e granulari per utenti, dispositivi e applicazioni. Ciò impedisce i movimenti laterali, riduce la fiducia implicita, supporta la conformità, mitiga i rischi di terze parti e protegge gli ambienti ibridi e multi-cloud.

In combinazione con ZTNA, la micro-segmentazione avanzata diventa una componente critica di un'architettura Zero Trust. Mentre ZTNA verifica le identità presso il perimetro della rete, la micro-segmentazione assicura una protezione più profonda controllando le interazioni all'interno della rete, limitando l'attività dell'utente in base all'identità e al ruolo, anche dopo aver concesso l'accesso.

Implementare la micro-segmentazione avanzata richiede una combinazione tra tecnologie, best practice e una gestione continua. Per sfruttare appieno tutto ciò in una soluzione ZTNA, le organizzazioni devono integrare controlli di accesso basati sull'identità, il monitoraggio continuo, l'automazione e aggiornamenti regolari delle politiche, per mantenere una segmentazione sicura e applicare politiche dinamiche basate sulle identità degli utenti e dei dispositivi.

COME FACCIAMO?

Netskope One Private Access applica politiche basate sull'identità che limitano l'accesso ad applicazioni specifiche, non all'intera rete.

4 | ZTNA universale

04

Le soluzioni ZTNA tradizionali si concentrano spesso su applicazioni Web o cloud, lasciando lacune nella protezione dei sistemi legacy, delle applicazioni non Web e dei dispositivi non gestiti. Ciò provoca un controllo degli accessi incoerente tra ambienti on-premises, cloud e ibridi e una esperienza utente insoddisfacente.

Le soluzioni ZTNA devono affrontare le sfide delle applicazioni legacy, che spesso si basano su una tecnologia VPN obsoleta, creando rischi per la sicurezza e una esperienza utente insoddisfacente. Molte soluzioni ZTNA instradano il traffico per applicazioni legacy od on-premise attraverso gateway VPN centralizzati, il che comporta colli di bottiglia e latenza e compromette il vantaggio dell'accesso diretto e basato sull'identità offerto da ZTNA. Inoltre, l'applicazione incoerente dei principi Zero Trust, specialmente con i sistemi legacy, espone le organizzazioni a vulnerabilità di sicurezza.

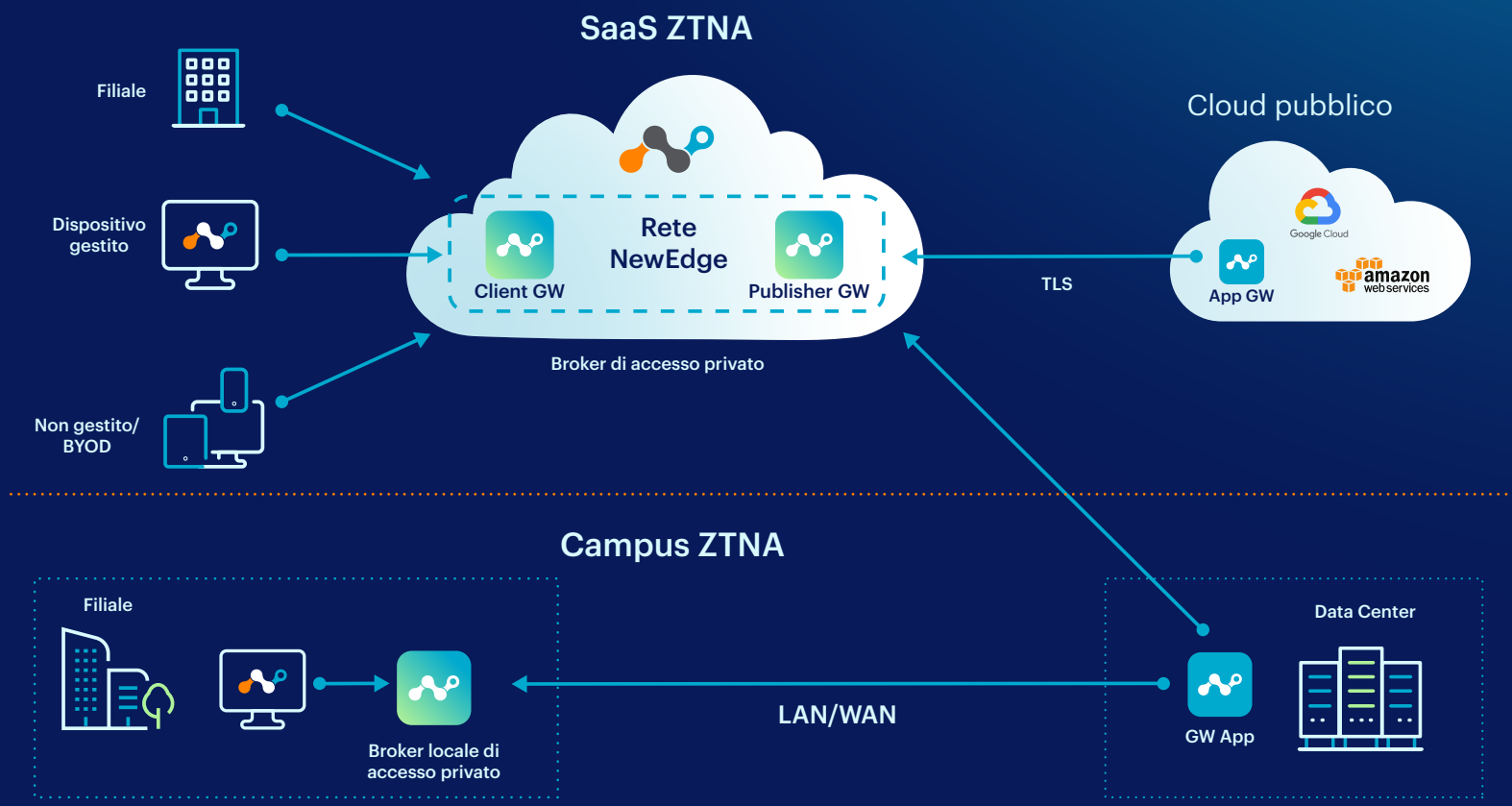
ZTNA universale è la chiave per superare queste sfide. Offre un accesso sicuro a tutti i tipi di risorse: siano legacy, moderne, basate sul cloud od on-premise, indipendentemente dalla posizione o dal dispositivo dell'utente. ZTNA universale consente alle organizzazioni di gestire l'accesso a tutte le applicazioni in ambienti locali e ibridi, mantenendo politiche di sicurezza coerenti. Garantisce una protezione completa applicando in modo uniforme i principi Zero Trust per offrire piena visibilità sulle attività degli utenti e semplificare la gestione degli accessi. Questo approccio assicura agli utenti esperienze senza soluzione di continuità con accesso senza attriti, e agli amministratori con applicazione unificata delle politiche una gestione semplificata con monitoraggio e audit ottimizzati in tutto l'ambiente.

COME FACCIAMO?

Netskope One Private Access integra le funzionalità ZTNA avanzate con le funzioni NAC di base, garantendo un accesso uniforme con privilegi minimi a tutti gli ambienti, sia remoti che on-campus, in filiali e addirittura ad utenti terzi.

ZTNA universale con Netskope One Private Access

Netskope One Private Access garantisce agli utenti un accesso sicuro con privilegi minimi alle applicazioni private, indipendentemente dalla posizione: in ufficio, a casa o in viaggio. Grazie ai principi Zero Trust, assicura controlli di autenticazione, autorizzazione e basati sul rischio coerenti , mitigando le minacce laterali e semplificando l'implementazione. La gestione intelligente del traffico ottimizza le prestazioni, mentre il client unificato consolida le funzioni ZTNA e VPN. Un unico motore di policy impone l'accesso granulare sia per gli utenti locali che remoti, con aggiornamenti in tempo reale basati sui punteggi di rischio.



5 | Supporto per le applicazioni legacy

05

Il mancato supporto alle applicazioni legacy in ZTNA ostacola gli sforzi mirati a modernizzare l'infrastruttura e il passaggio ai servizi basati sul cloud.

Le soluzioni ZTNA devono supportare le applicazioni legacy per garantire una sicurezza completa, l'efficienza operativa e una transizione agevole verso un'infrastruttura moderna.

Molte organizzazioni continuano ad affidarsi ad applicazioni legacy per le funzioni aziendali critiche che gestiscono dati sensibili e processi essenziali. Ne sono un esempio il protocollo Remote Desktop Protocol (RDP), i sistemi ERP locali come SAP o Oracle, i sistemi IoT industriali, le piattaforme VoIP e altro ancora. Questi sistemi più datati, costruiti prima dell'estesa adozione del cloud computing e di molti moderni protocolli di sicurezza, sono spesso difficili da sostituire o aggiornare a causa dei costi, della complessità o delle dipendenze tecniche.

Senza il supporto ZTNA, le applicazioni legacy dipendono da metodi di accesso obsoleti come le VPN, che introducono vulnerabilità, creano lacune di sicurezza e indeboliscono il modello Zero Trust. L'accesso centralizzato alla VPN causa inoltre colli di bottiglia e latenza della rete, soprattutto per gli utenti remoti, con conseguenti prestazioni scarse e una minore produttività.

Inoltre, l'utilizzo di metodi di accesso distinti per le applicazioni moderne e per quelle legacy complica la gestione della sicurezza, aumentando il sovraccarico amministrativo e indebolendo l'applicazione delle politiche. Grazie al supporto alle applicazioni legacy, le soluzioni ZTNA assicurano politiche di sicurezza coerenti in tutti gli ambienti, semplificano la gestione e assicurano che le operazioni critiche non subiscano interruzioni durante la modernizzazione. Ciò consente alle organizzazioni di passare gradualmente a sistemi più recenti, salvaguardando sia una sicurezza robusta che la continuità operativa.

COME FACCIAMO?

Netskope One Private Access porta le funzionalità SD-WAN a ZTNA per consentire una connettività sicura e ottimizzata a tutte le applicazioni private, consentendo alle organizzazioni di sostituire completamente le loro soluzioni VPN di accesso remoto e modernizzare la connettività per la forza lavoro ibrida.

6 | Controlli di sicurezza più vicini agli utenti e alle applicazioni

06

Quando ZTNA non prevede controlli di sicurezza vicini agli utenti e alle applicazioni, provoca latenza, colli di bottiglia e indebolisce l'applicazione del modello Zero Trust, portando a una esperienza utente insoddisfacente e a lacune di sicurezza.

I controlli centralizzati possono rallentare le prestazioni delle app cloud, aumentare la latenza e creare lacune di sicurezza, soprattutto per gli utenti remoti. Senza una sicurezza distribuita, il traffico viene instradato attraverso un gateway centrale, ritardando l'accesso e complicando l'applicazione delle politiche.

In una soluzione ZTNA, i controlli di sicurezza devono essere posizionati presso il punto di connessione tra utenti e applicazioni, per fare sì che le politiche per ogni applicazione vengano applicate senza esporre la rete più estesa. Questo approccio migliora la scalabilità man mano che aumentano le richieste degli utenti e dei servizi, consentendo, al tempo stesso, decisioni di accesso in tempo reale basate su fattori come l'identità e il posizionamento del dispositivo. Per ridurre la latenza e migliorare le prestazioni, le strategie includono la distribuzione di broker locali sul posto, il posizionamento di gateway ZTNA in posizioni chiave, l'integrazione dei controlli di sicurezza sul cloud e l'integrazione di ZTNA con SSE. Inoltre, sfruttare l'edge computing e i punti di presenza locali (PoP) favorisce l'ottimizzazione delle prestazioni e della conformità.

I principali fornitori di ZTNA affrontano queste sfide distribuendo i PoP globali al fine di soddisfare le richieste sensibili alla latenza e i requisiti di conformità regionali.

COME FACCIAMO?

Netskope One Private Access applica le politiche tramite un broker, sia locale che basato sul cloud, posizionato vicino agli utenti per consentire connessioni rapide alle applicazioni, riducendo la latenza e migliorando le prestazioni.

7 | Integrazione con un ecosistema di sicurezza più ampio

07

Se gli eventi ZTNA non sono collegati ad attività di rete più ampie o al comportamento degli endpoint, i team di sicurezza possono non notare i primi segnali di pericolo, dando agli aggressori più tempo per diffondere o rubare dati. Questo ritardo nell'identificazione aumenta in modo significativo il rischio e l'esposizione alle violazioni.

La perfetta integrazione di ZTNA con altri sistemi IT, di sicurezza e di rete migliora la sicurezza, razionalizza le operazioni e migliora l'esperienza utente. Le principali integrazioni includono IAM (SSO e MFA), Endpoint Detection and Response (EDR), SIEM, CASB, SD-WAN, VPN, firewall tradizionali, intelligence delle minacce e strumenti per l'infrastruttura applicativa o cloud.

L'integrazione di ZTNA con strumenti di monitoraggio più ampi come SIEM o con sistemi di gestione dei log è essenziale per una visibilità completa sul traffico ZTNA e sul comportamento degli utenti. In assenza di questa integrazione, i team di sicurezza potrebbero non notare eventuali pattern di accesso anomali o minacce, aumentando il rischio di violazioni. Collegando ZTNA con altri sistemi come la sicurezza di rete e la protezione degli endpoint, i team possono correlare gli eventi con più efficacia, migliorando il rilevamento degli incidenti e i tempi di risposta. L'integrazione con IAM e SSO semplifica anche la gestione delle identità e degli accessi degli utenti.

Queste integrazioni rendono ZTNA più efficiente, scalabile e reattivo rispetto alle moderne esigenze aziendali, migliorando la sicurezza, la flessibilità e l'esperienza utente.

COME FACCIAMO?

Come componente di Netskope One SASE, si integra con CASB, SWG, DLP e partner chiave in materia di sicurezza, identità, ITSM, mobile e SecOps, ed offre politiche unificate, protezione dalle minacce in tempo reale e visibilità su dati e applicazioni.

8 | Piena visibilità e analisi della rete

08

La mancanza di una visibilità completa sulla rete crea punti ciechi per la sicurezza e problemi di conformità e inefficienza, che indeboliscono il livello di sicurezza Zero Trust dell'organizzazione e aumentano la vulnerabilità a potenziali minacce.

Mantenere la piena visibilità e analisi della rete all'interno di un framework ZTNA è essenziale per proteggere le organizzazioni dai rischi di sicurezza. Senza tali capacità, le organizzazioni non riescono ad applicare i principi Zero Trust ed hanno difficoltà sia a rilevare le minacce interne che ad affrontare le sfide nella gestione dei rischi BYOD e del lavoro remoto.

Il monitoraggio in tempo reale di tutto il traffico di rete aiuta a rilevare anomalie e violazioni della sicurezza, nonché minacce in evoluzione. Con una visibilità completa, i team di sicurezza possono identificare movimenti laterali, comportamenti dannosi e utilizzare algoritmi avanzati di rilevamento. Le analisi di rete e l'apprendimento automatico migliorano ulteriormente il rilevamento e la conformità, ottimizzando le prestazioni.

Il monitoraggio continuo, l'analisi in tempo reale e l'applicazione dinamica delle politiche sono fondamentali per affrontare le minacce in evoluzione ed essenziali per una soluzione ZTNA. Per raggiungere questo obiettivo, le organizzazioni devono implementare strumenti di monitoraggio, analisi comportamentale e controllo degli accessi, integrandoli con l'infrastruttura di sicurezza esistente come SIEM, CASB e intelligence delle minacce.

COME FACCIAMO?

Con Netskope One DEM, forniamo una visione a 360 gradi delle esperienze digitali dagli utenti alle applicazioni, coprendo punteggi utente, salute del dispositivo, connettività locale (Wi-Fi), on-ramp SD-WAN, servizi SSE e altro ancora.

9 | Garantire scalabilità e agilità

09

Con la crescita delle organizzazioni o l'aumento della domanda di accesso remoto, l'assenza di una soluzione ZTNA scalabile può limitare la capacità degli utenti, ostacolare le connessioni e limitare l'accesso alle applicazioni cloud, rendendo l'organizzazione vulnerabile e inefficiente.

Molte organizzazioni oggi operano con un mix di infrastrutture on-premise, cloud pubblici e privati e svariate applicazioni SaaS. Gestire soluzioni di sicurezza separate per ciascun ambiente può essere complesso e costoso, e spesso porta a politiche incoerenti. ZTNA semplifica questo processo con una visibilità unificata e il controllo dell'accesso degli utenti in tutti gli ambienti, riducendo la complessità e migliorando la sicurezza.

Negli ambienti ibridi in cui applicazioni e dati si estendono sia ai sistemi on-premises che sul cloud, le soluzioni ZTNA devono applicare politiche di sicurezza coerenti e adattarsi a carichi di lavoro dinamici. Una soluzione ZTNA cloud-native è fondamentale per ottenere una scalabilità fluida senza modifiche hardware e in funzione della crescita degli utenti o di nuove applicazioni.

ZTNA dovrebbe anche offrire API e SDK per l'integrazione con le piattaforme cloud, migliorando controllo e visibilità. Per gestire efficacemente le risorse in diversi ambienti, ZTNA deve fornire politiche di sicurezza unificate, controlli adattivi, esperienze utente prive di interruzioni e funzionalità di integrazione. Una soluzione ZTNA solida deve sfruttare l'infrastruttura cloud-native, il provisioning automatizzato e politiche adattive per garantire scalabilità, prestazioni e reattività alle esigenze in continuo mutamento, come un maggior numero di utenti, nuove applicazioni o minacce emergenti. Queste caratteristiche sono essenziali per garantire sicurezza e agilità nel dinamico panorama IT di oggi.

COME FACCIAMO?

L'architettura cloud-native e scalabile di Netskope NewEdge Network e la sua portata globale consentono un'espansione fluida, una distribuzione rapida e un accesso sicuro ai lavoratori remoti.

10 | Strumenti amministrativi efficaci

10

L'assenza di solidi strumenti amministrativi nelle soluzioni ZTNA legacy limita la capacità dei team di sicurezza di applicare controlli granulari sugli accessi, di reagire rapidamente agli incidenti e di migliorare continuamente il livello di sicurezza dell'organizzazione.

Una soluzione ZTNA con un'interfaccia amministrativa inefficiente complica la gestione e frammenta la supervisione, causando ritardi nella risposta agli incidenti. La lentezza di accesso ai registri di sicurezza e la complessità di gestione delle politiche possono fare sì che la loro applicazione nell'organizzazione sia incoerente.

Ottimizzare l'esperienza amministrativa in ZTNA comporta il miglioramento dell'usabilità per utenti finali e amministratori. Una console unificata per la gestione di utenti, dispositivi, applicazioni e policy semplifica il monitoraggio, la configurazione e la risoluzione dei problemi, garantendo politiche di sicurezza coerenti e facilità di onboarding.

L'implementazione del modello con privilegi minimi semplifica ulteriormente la gestione limitando l'accesso alle risorse in base a ruoli e condizioni, rendendo le politiche più semplici da implementare e verificare. Gli strumenti di rilevamento automatico, analisi e risoluzione dei problemi migliorano ulteriormente il processo. Inoltre, l'utilizzo di modelli di policy, dell'automazione e di dashboard dettagliati aumenta la sicurezza e l'efficienza operativa in un ambiente ZTNA.

COME FACCIAMO?

Netskope One Private Access mette a disposizione una console unificata per la gestione di utenti, dispositivi e policy, garantendo coerenza all'applicazione e agli audit in tutti gli ambienti.

Il passaggio alla forza lavoro ibrida e l'adozione di applicazioni cloud e SaaS hanno rimodellato le aziende moderne, cambiando come, dove e quali risorse siano accessibili.

Mentre le organizzazioni si spostano verso i servizi sul cloud e si adattano al lavoro in remoto in ambienti distribuiti, hanno bisogno di soluzioni più scalabili, flessibili e sicure. Una soluzione ZTNA moderna soddisfa queste esigenze fornendo un accesso sicuro e adattabile e aiuta le organizzazioni ad affrontare le sfide di sicurezza in continua evoluzione del panorama digitale odierno.

Prova la potenza di Netskope One Private Access.
Effettua una prova su strada di Netskope One Private Access.

Fai il test

La piattaforma Netskope One Platform

Netskope One SSE si basa su **Netskope One Platform**, una piattaforma che offre visibilità senza pari e protezione in tempo reale dei dati dalle minacce quando si accede a servizi cloud, siti web e app private da qualsiasi luogo, su qualsiasi dispositivo.

- Cloud Access Security Broker
- Secure Web Gateway
- Accesso Zero Trust alla rete
- Protezione dei dati + DLP
- Protezione dalle minacce
- Gestione del posizionamento

- SD-WAN
- Client SASE
- Gestione dell'esperienza digitale
- Firewall e IDS/IPS
- IoT intelligente

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