HPE aruba networking

White paper aziendale

GUIDA ALLA SOSTITUZIONE DELLA VPN PER ARCHITETTI

HPE

Sommario

3 La vecchia tecnologia in un nuovo mondo

3 Cosa si intende per SSE e dove si inserisce ZTNA?

4 ZTNA come alternativa alla VPN

5 Inizia il tuo percorso verso SSE con ZTNA

5 Scegli da dove iniziare

5 Casi d'uso di ZTNA

8 ZTNA HPE: l'alternativa ideale alla VPN

9 Scopri HPE Aruba Networking SSE con ZTNA

La vecchia tecnologia in un nuovo mondo

Negli ultimi anni, l'ambiente di lavoro è cambiato drasticamente. Il panorama stava già iniziando a mutare con l'invenzione e la crescita del cloud, ma la pandemia da COVID-19 ha portato a un incremento notevole del lavoro da remoto.

Di conseguenza, è cambiato anche il nostro modo di pensare ai progetti architettonici. Gli utenti non sono più protetti da un muro perimetrale. La forza lavoro è ovunque. Non solo, le applicazioni a cui devono poter accedere quotidianamente sono ora distribuite tra ambienti SaaS, on-premise e IaaS.

Oggi i team devono supportare una connettività sicura ad applicazioni interne ed esterne per una base di utenti che possono essere dislocati ovunque. Gli architetti devono supportare l'accesso sicuro a tutte le applicazioni legacy e anche valutare le possibili trasformazioni di tale accesso in futuro.

Il nuovo mondo di cloud e mobilità cambia il nostro modo di connetterci e anche il modo in cui proteggiamo tale connettività. E le soluzioni legacy, come la tradizionale VPN, non rispondono adeguatamente alle esigenze di oggi. Molte organizzazioni hanno iniziato a sostituire la loro VPN con una tecnologia moderna nota come ZTNA (Zero Trust Network Access), disponibile in molte piattaforme SSE (Security Service Edge).

Cosa si intende per SSE e dove si inserisce ZTNA?

SSE fa parte del più ampio framework SASE (Secure Access Service Edge), introdotto da Gartner® nel 2019. Quando il lavoro da remoto è aumentato vertiginosamente durante la pandemia del 2021, Gartner® ha introdotto SSE.

Il framework SSE è una raccolta di funzionalità di sicurezza integrate, incentrate sul cloud, che agevolano l'accesso sicuro alle applicazioni private, ai prodotti SaaS (software-as-a-service) e a Internet, grazie alle seguenti tecnologie: ZTNA (Zero Trust Network Access), CASB (Cloud Access Security Broker) e SWG (Secure Web Gateway).

— **ZTNA** fornisce l'accesso zero trust alle applicazioni private.

— **CASB** protegge l'accesso a tutte le applicazioni basate su SaaS.

— **SWG** garantisce la sicurezza di tutti gli accessi a Internet

Una soluzione SSE dovrà fornire una singola piattaforma unificata per l'accesso a tutte le applicazioni, separandolo dalla rete aziendale. Dovrà servire da overlay sulla rete esistente, consentendo all'IT di modernizzare e semplificare la connettività rafforzando al contempo la sicurezza, senza dover

“Entro il 2025, almeno il 70% delle nuove distribuzioni di accesso remoto verranno gestite prevalentemente tramite ZTNA anziché con servizi VPN”.

– Gartner® Forecast Analysis: Information Security and Risk Management, Worldwide, settembre 2022

apportare modifiche complesse all’architettura di rete.

Poiché una piattaforma SSE è costituita da diverse tecnologie core implementabili separatamente, da dove iniziare? Come adottare il framework SSE? La risposta a questa domanda è identica a quella per qualsiasi altro progetto o iniziativa di sicurezza: dalle aree di maggior rischio. Nel nuovo mondo di applicazioni e utenti distribuiti, è necessario iniziare sostituendo la tecnologia VPN e proteggendo l’accesso alle applicazioni private con ZTNA.

ZTNA come alternativa alla VPN

Le ZTNA représente une alternative de choix aux VPN traditionnels pour les équipes qui s’attellent à la difficulté de sécuriser des environnements de télétravail. Le ZTNA permet de contourner une grande partie des contraintes des VPN traditionnels et offre les avantages suivants aux entreprises modernes.

Sicurezza

— **Problematica della VPN:** le VPN espongono le reti a minacce come attacchi malware, ransomware e DDoS, esponendo gli indirizzi IP e consentendo quindi a utenti malintenzionati di accedere all’intera rete.

— **Soluzione ZTNA:** ZTNA riduce il rischio di attacchi basati su Internet nascondendo le risorse private da Internet. Con connessioni solo outbound, la rete e le applicazioni diventano invisibili e irrintracciabili, mentre agli utenti non viene mai consentito l’accesso alla rete. Inoltre, l’accesso viene consentito in base all’identità dinamica dell’utente, al dispositivo e al contesto dei dati, evitando di fatto gli spostamenti laterali non autorizzati.

Scala e flessibilità

— **Problematica della VPN:** le VPN sono costituite da appliance fisiche, quindi il ridimensionamento dell’infrastruttura può rivelarsi complicato e problematico. Con la crescita della forza lavoro mobile, molte organizzazioni devono ampliare significativamente il proprio investimento nell’infrastruttura VPN per supportare più connessioni e gestire l’aumento del traffico.

— **Soluzione ZTNA:** l’architettura cloud di ZTNA offre scalabilità e gestione centralizzata dell’accesso remoto. Le policy zero trust possono essere personalizzate a livello di utente e di applicazione e possono essere applicate globalmente in pochi secondi.

Produttività

— **Problematica della VPN:** poiché il traffico viene sottoposto a backhaul attraverso la rete aziendale, le VPN possono ostacolare la velocità delle connessioni e le prestazioni delle applicazioni, con conseguente perdita di produttività e aumento del carico di lavoro dell’IT per la gestione dell’accesso.

— **Soluzione ZTNA:** ZTNA ottimizza l’esperienza utente avvicinando quanto più possibile l’accesso all’utente tramite sedi all’edge globali nel cloud, per cui il traffico viene automaticamente instradato verso il percorso di accesso più veloce. ZTNA elimina i rallentamenti, le disconnessioni e i problemi di accesso della VPN, pur integrandosi perfettamente con SSO e i sistemi di gestione delle identità.

Costo

— **Problematica della VPN:** le VPN comportano costi elevati a causa dell’esigenza di hardware costoso on-premise e di personale dedicato per il monitoraggio e la gestione, senza contare lo stack di sicurezza inbound esteso, necessario per ridurre il rischio di attacchi.

— **Soluzione ZTNA:** ZTNA elimina i costi associati all’hardware delle tradizionali VPN, alla protezione da DDoS e ai firewall, semplificando il monitoraggio e liberando risorse da dedicare ad altri progetti critici

Inizia il tuo percorso verso SSE con ZTNA

Le soluzioni ZTNA si sono evolute oltre i confini del semplice accesso remoto per diventare un concetto fondamentale per l'accesso alle applicazioni in generale. Non si tratta di un gateway, ma di un approccio trasformativo che prepara il terreno a una visione più ampia e completa. ZTNA è un singolo servizio distribuito tramite cloud che soddisfa tutti i requisiti di accesso.

Scegli da dove iniziare

Per l'implementazione di ZTNA, è fondamentale individuare la forza propulsiva alla base della decisione. L'obiettivo principale è ottimizzare la sicurezza, semplificare l'esperienza utente o risparmiare sui costi? Una volta compresa la motivazione sottostante, potrai scegliere il punto di partenza più appropriato per il percorso verso ZTNA.

"Entro la fine del 2024, il cambiamento nella natura del lavoro farà aumentare il mercato dei dipendenti da remoto fino al 60% del totale, con un incremento rispetto al 52% del 2020".

– Gartner® Forecast Analysis: Information Security and Risk Management, Worldwide, settembre 2022

Se la priorità è la **sicurezza**, identifica l'area con il massimo rischio e concentrati su soluzioni di accesso sicuro per gruppi specifici, come dipendenti o soggetti esterni. Se l'obiettivo è **migliorare l'esperienza utente**, identifica i gruppi di utenti con problemi di accesso (ad esempio dirigenti o dipendenti da remoto) e ottimizza il loro accesso alle applicazioni private. Se l'obiettivo è il **risparmio sui costi**, analizza quali sono le tecnologie legacy più costose (ad esempio le VPN) e scopri come sostituirle con ZTNA.

Casi d'uso di ZTNA

Può risultare difficile decidere quale sarà il caso d'uso iniziale. Per offrirti il supporto necessario, ne abbiamo identificati tre principali. Le seguenti sezioni descrivono questi scenari e la perfetta integrazione di ZTNA al loro interno.

Protezione dell'accesso remoto e ibrido per i dipendenti

Nel mondo mobile, le tradizionali VPN hanno difficoltà a tenere il passo. Mentre una volta le VPN erano strategiche per facilitare l'accesso remoto dei dipendenti, oggi comportano rischi significativi per la sicurezza in termini di connettività. Con l'attuale forza lavoro che opera da casa, in ufficio o in qualsiasi altro luogo provvisorio, è fondamentale mantenere un approccio coerente e non invasivo all'accesso zero trust.

Il diagramma seguente mostra come la tecnologia ZTNA sostituisce i framework VPN obsoleti in genere ospitati nei data center. ZTNA funge da intermediario tra l'utente e l'applicazione, concedendo l'accesso solo agli utenti autorizzati e alle applicazioni approvate, indipendentemente dalla posizione, ovvero on-premise o nel cloud pubblico.

Questo risultato si ottiene tramite un connettore leggero che risiede nell'ambiente applicativo, concedendo l'accesso solo se soddisfa requisiti contestuali. Una volta soddisfatti i criteri, viene stabilita una connessione outbound grazie alla quale gli utenti non vengono inseriti direttamente nella rete e l'accesso viene consentito solo all'applicazione autorizzata designata.

Inoltre, il passaggio dall'accesso remoto a quello in ufficio non influisce sull'esperienza utente, dato che ZTNA opera costantemente in background. Protegge anche la rete impedendo l'accesso da dispositivi potenzialmente compromessi mentre si trovano nella sede aziendale.

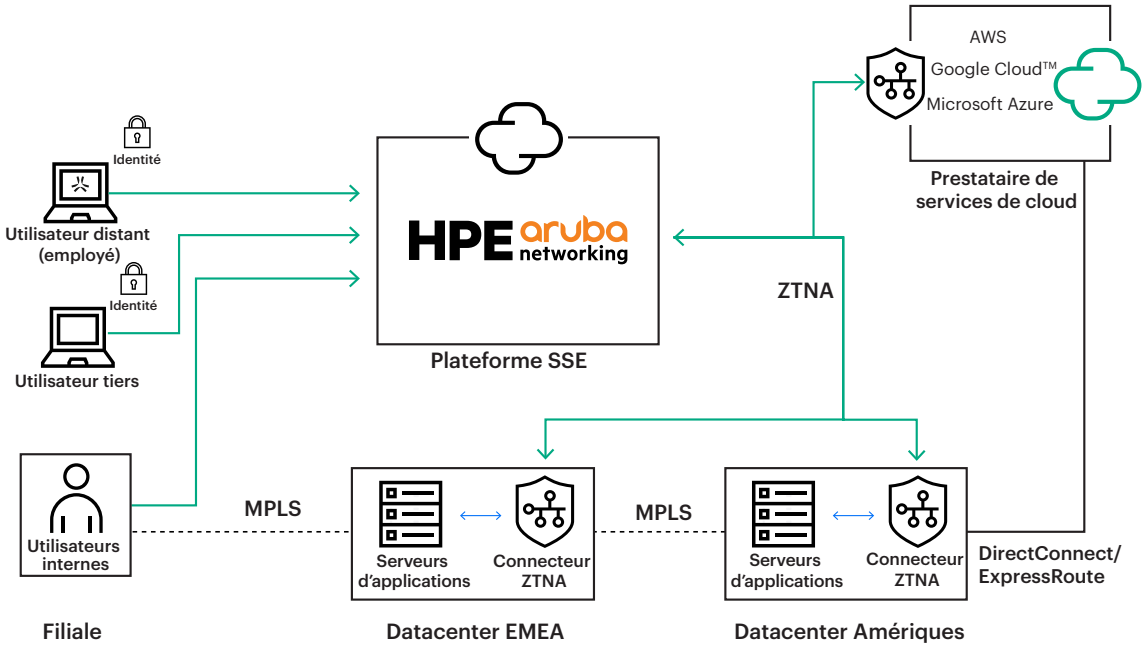

Figura 1. Protezione dell'accesso remoto e ibrido

Protezione dell'accesso da parte di soggetti esterni e utenti BYOD

In genere, l'accesso da parte di soggetti esterni si basa sulla tecnologia VPN di accesso remoto. Gli utenti devono installare un client, attendere gli aggiornamenti manuali alle policy di ACL e firewall eseguiti da un amministratore e provare a connettersi. Le connessioni riuscite concedono l'accesso ad asset sensibili, esponendo enormemente la rete ai rischi. La VPN estende l'accesso alla rete per utenti e dispositivi non attendibili provenienti da reti non affidabili e, una volta entrati, gli utenti esterni spesso possono accedere liberamente all'intera rete.

ZTNA supera i rischi di questo approccio con le connessioni solo outbound. ZTNA nasconde l'infrastruttura di rete, le applicazioni aziendali e i portali di terzi da Internet, salvaguardandoli dalla localizzazione e da attacchi DDoS, dal momento che non possono essere individuati da probe inbound. Le applicazioni private e i portali di terzi vengono nascosti in sicurezza dietro un connettore applicativo, che consente il traffico solo attraverso il cloud di ZTNA.

ZTNA consente inoltre di applicare le policy dei privilegi minimi, anche per utenti BYOD esterni. La perfetta integrazione con tutte le principali soluzioni SSO facilita un'esperienza di accesso fluida alle applicazioni private attraverso un semplice browser web, senza compromettere la sicurezza.

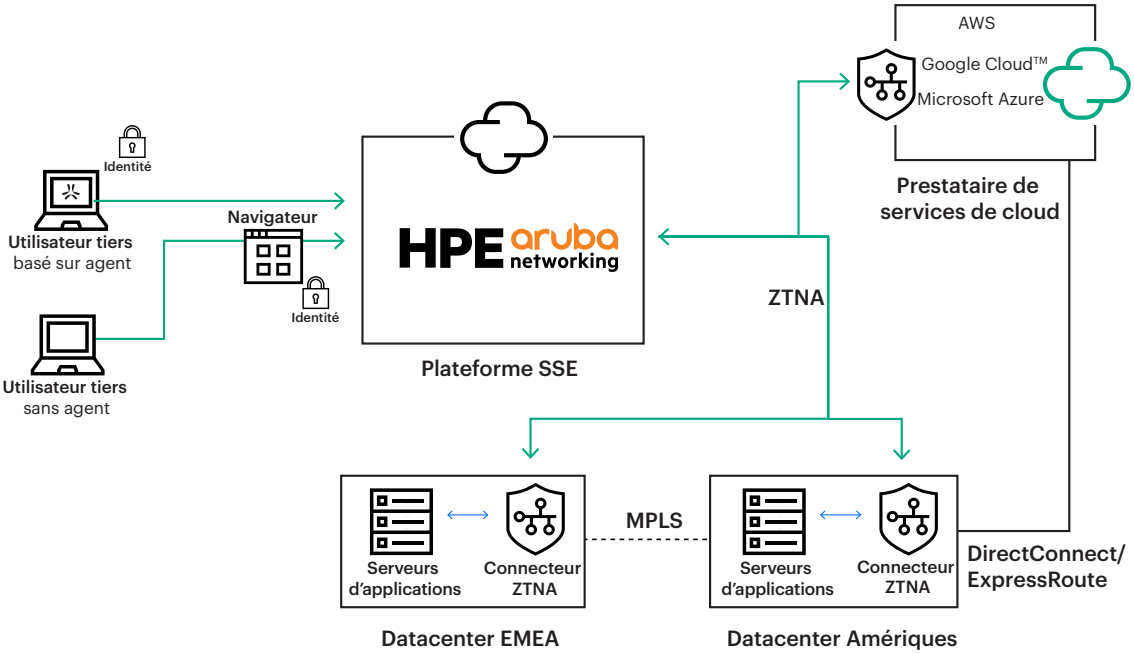

Figura 2. Protezione dell'accesso da parte di soggetti esterni e utenti BYOD

Accelerazione di fusioni e acquisizioni

Fusioni e acquisizioni presentano problematiche complesse, ma ZTNA offre una soluzione semplificata per l'accesso immediato alle applicazioni critiche fin dall'inizio. Questo approccio elimina la necessità di VPN, integrazione di rete o modifiche dell'infrastruttura. La strategia si basa su un elenco predefinito di applicazioni essenziali, come sistemi HR, ERP e altri tool basati su web, accessibili attraverso la piattaforma SSE.

ZTNA prevede una strategia solida per la gestione delle identità, garantendo che gli utenti possano autenticarsi e accedere alle applicazioni in sicurezza, anche prima del consolidamento di directory, utenti e gruppi tra le entità da accorpare. La piattaforma SSE si integra con vari provider di identità, un aspetto cruciale per soddisfare le esigenze diversificate di accesso alle applicazioni di tutti gli utenti.

Le funzionalità agentless di ZTNA accelerano la procedura di fusione e acquisizione, fornendo agli utenti accesso zero trust basato su browser, con tempi di integrazione decisamente più brevi.

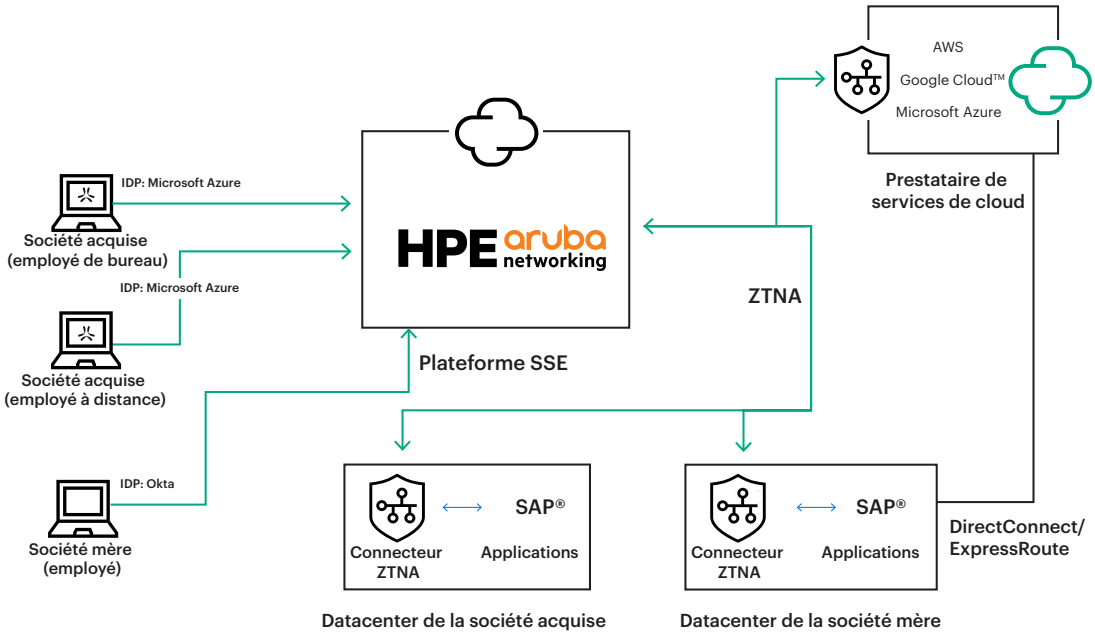

Figura 3. Accelerazione di fusioni e acquisizioni

ZTNA HPE: l'alternativa ideale alla VPN

L'avvio del percorso verso SSE non deve essere inevitabilmente difficile. I nostri esperti di SSE sono qui per supportarti. Ecco alcuni motivi per cui diversi team hanno scelto di collaborare con HPE Aruba Networking per il loro percorso verso SSE e oltre.

- **Sostituzione totale della VPN:** la tecnologia ZTNA HPE Aruba Networking supera le aspettative del mercato con il supporto completo delle applicazioni private. Gestisce tutto il traffico TCP/UDP, tra cui VoIP e peer-to-peer, ed è compatibile con moderne applicazioni web come SSH, RDP, Git e database.
- **Accesso con privilegi minimi senza segmentazione:** senza richiedere una complessa segmentazione della rete, il servizio ZTNA limita l'accesso a specifiche risorse, riducendo la superficie di attacco e impedendo l'attraversamento di rete non autorizzato.
- **Accesso flessibile con agenti o agentless:** gli utenti possono accedere liberamente alle applicazioni da qualsiasi dispositivo, con o senza client. L'opzione senza client facilita le sessioni RDP basate su browser, eliminando l'esigenza di una VDI.
- **Ispezione granulare del traffico:** il servizio garantisce visibilità dettagliata sul traffico delle risorse private. Consente di monitorare le azioni degli utenti, i download dei file e l'utilizzo comune, oltre che di bloccare le attività dannose.
- **Controlli dell'accesso adattivi:** i controlli basati su API regolano i diritti di accesso in base alla posizione degli utenti, all'identità e allo stato dei dispositivi, ottimizzando la sicurezza dei dati.
- **Architettura interamente cloud:** con HPE Aruba Networking SSE, le connessioni vengono gestite attraverso la sede all'edge SSE ottimale, garantendo un uptime costante senza la necessità di gestire le appliance VPN.

Scopri HPE Aruba Networking SSE con ZTNA

Valuta le esigenze specifiche dei tuoi casi d'uso e contatta i nostri professionisti esperti per identificare le aree in cui ZTNA può offrire vantaggi significativi alla tua organizzazione. Inizia oggi stesso a rafforzare le applicazioni più critiche con le nostre soluzioni di sicurezza all'avanguardia.

Per saperne di più

Contatta un esperto SSE

Test Drive di ZTNA per 24 ore

Visita HPE.com

Chatta ora (commerciale)

© Copyright 2025 Hewlett Packard Enterprise Development LP. Le informazioni contenute nel presente documento sono soggette a modifica senza preavviso. Le uniche garanzie per i servizi e i prodotti Hewlett Packard Enterprise sono quelle espressamente indicate nelle dichiarazioni di garanzia che accompagnano tali prodotti e servizi. Nulla di quanto contenuto nel presente documento potrà essere interpretato come garanzia supplementare. Hewlett Packard Enterprise declina ogni responsabilità per eventuali omissioni ed errori tecnici o editoriali contenuti nel presente documento.

GOOGLE CLOUD è un marchio di Google LLC. Microsoft e Azure sono marchi o marchi registrati di Microsoft Corporation negli Stati Uniti e/o in altri paesi. SAP è un marchio o un marchio registrato di SAP SE (o un'affiliata di SAP) in Germania e altri Paesi. Tutti i marchi di terzi sono di proprietà dei rispettivi titolari.

a00141301ITE, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com