HPE aruba networking

Sostituire completamente la VPN con il servizio ZTNA HPE Aruba Networking

Nei moderni ambienti di lavoro serve un nuovo approccio all'accesso remoto

Coniato ad aprile 2019 da Gartner®, il termine ZTNA (Zero Trust Network Access) si riferisce a una serie di nuove tecnologie progettate per proteggere l'accesso alle applicazioni private. Anche dette SDP (Software-Defined Perimeter), le tecnologie ZTNA si basano su policy di accesso granulari per connettere gli utenti autorizzati a specifiche applicazioni, senza la necessità di accedere alla rete aziendale, e per stabilire una segmentazione a livello di applicazione con privilegi minimi in sostituzione della segmentazione della rete, senza esporre la posizione dell'applicazione su Internet pubblico.

Per accelerare la transizione verso un ambiente di lavoro moderno, bisogna abbandonare la VPN

Spinte dall'esigenza di garantire continuità operativa durante la pandemia per superare la concorrenza, le organizzazioni si sono affrettate a implementare le soluzioni digitali più indicate per mantenere gli utenti soddisfatti, motivati e produttivi, attraverso l'adozione di nuove applicazioni di collaborazione, come Zoom e Microsoft Teams, l'aumento di servizi di cloud pubblici scalabili e l'implementazione di ambienti di lavoro più flessibili. Con questa modernizzazione in corso, i responsabili IT hanno iniziato a valutare soluzioni più efficaci per fornire l'accesso remoto alle applicazioni private per dipendenti e soggetti esterni, abbandonando la VPN.

Prima della pandemia, appena il 30% di dipendenti lavorava da casa. Oggi, il 77% di aziende prevede di adottare il lavoro ibrido per trattenere i migliori dipendenti che ora preferiscono lavorare da casa e per accedere a nuovi pool di talenti meno dispendiosi. Tuttavia, le VPN tendono a ostacolare la produttività e a frustrare i dipendenti.

Anche i partner, i fornitori e i clienti ricoprono un ruolo nel generare ricavi per l'azienda. Un terzo degli utenti che richiedono l'accesso alle risorse sono soggetti esterni e raramente consentono l'installazione di un client VPN nei loro dispositivi.

Come si può immaginare, questo ambiente di lavoro moderno ha anche un costo. Secondo le stime, la spesa in IT è destinata a raggiungere 2 trilioni di dollari nel 2022, in gran parte per modernizzare l'infrastruttura IT e supportare questo nuovo ambiente di lavoro. Eppure, si tratta di un incremento di appena il 4% nei tipici budget IT, quindi non è accettabile continuare a investire pesantemente in tecnologie di accesso remoto legacy.

HPE GreenLake

Nonostante l'esigenza di consentire ai dipendenti di lavorare ovunque, proteggere l'accesso da parte di soggetti esterni e modernizzare l'infrastruttura, le aziende devono comunque proteggere le loro risorse e la propria reputazione. La potenziale superficie di attacco aumenta esponenzialmente con ogni utente, dispositivo e applicazione che si connette tramite Internet, e il principale rischio in assoluto è rappresentato dagli utenti collegati alla rete aziendale tramite una VPN.

Per supportare questo nuovo ambiente, entro il 2023 il 60% di aziende sostituirà la VPN con una soluzione ZTNA.

Differenza tra VPN e ZTNA HPE Aruba Networking

VPN per l'accesso remoto

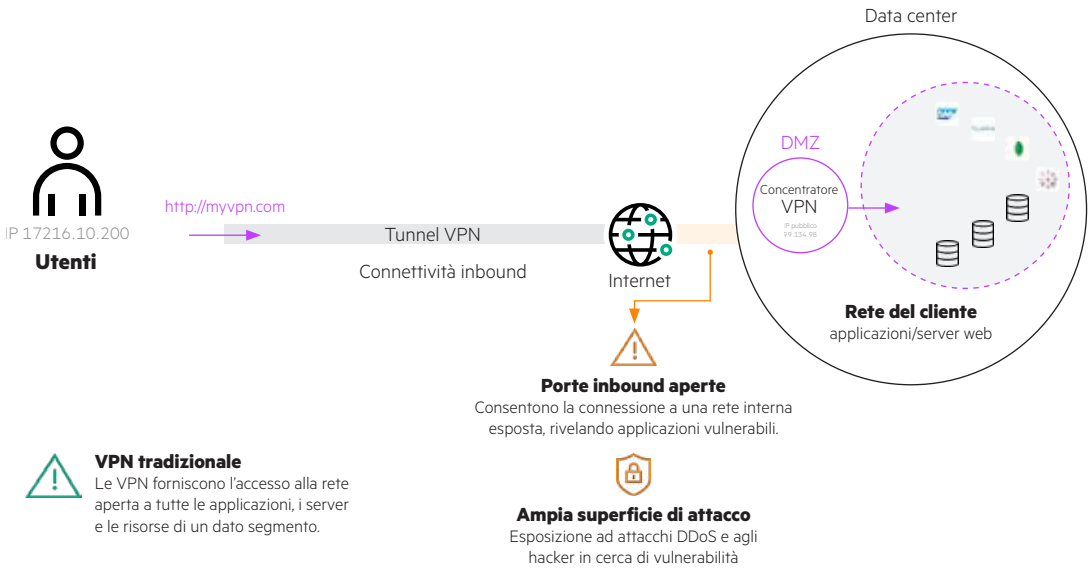

Figura 1. VPN tradizionale

Negli ultimi 20 anni, la VPN ha consentito a dipendenti e soggetti esterni di accedere alla rete e alle risorse private in esecuzione al suo interno. I concentratori VPN restano in ascolto di chiamate inbound da parte dei client VPN e servono da beacon per i client, fornendo un punto di accesso nella rete aziendale. Per ridurre il rischio di questa architettura imperfetta, le organizzazioni richiedono firewall, sistemi di bilanciamento del carico, misure di prevenzione di attacchi DDoS e concentratori VPN per connettere gli utenti alle applicazioni private, con un conseguente aumento di complessità, costi e rischi. Negli ultimi anni, i servizi VPN più diffusi di aziende ben note hanno subito exploit a causa di questa architettura.

ZTNA HPE Aruba Networking

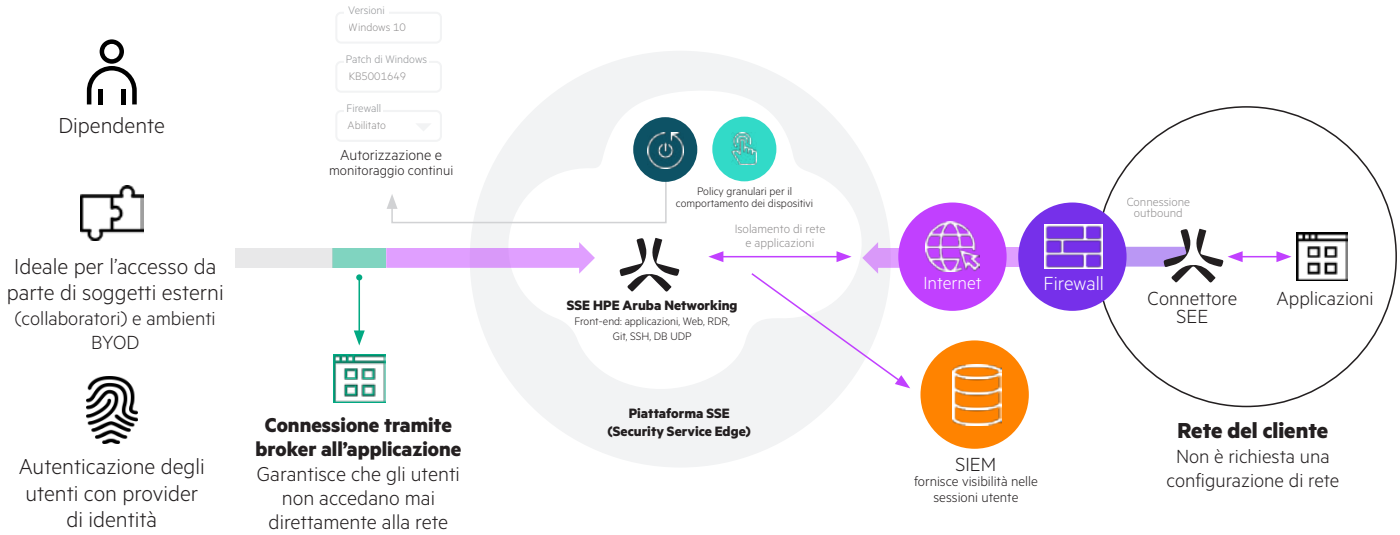

Figura 2. ZTNA HPE Aruba Networking

Con oltre 500 sedi all'edge in tutto il mondo, la piattaforma SSE HPE Aruba Networking è una delle soluzioni zero trust più affidabili, disponibili e scalabili presenti sul mercato, progettata per proteggere la connettività alle risorse aziendali.

Il servizio ZTNA HPE Aruba Networking fornisce agli utenti accesso rapido, sicuro e affidabile a risorse private. Ecco cosa succede in tempo reale quando ci si connette tramite una funzionalità senza client.

1. L'utente richiede l'accesso a un'applicazione interna, ad esempio hr-app-tenant.axisapps.io
2. Se l'utente non ha effettuato l'accesso a un'applicazione gestita da HPE Aruba Networking, viene reindirizzato al provider di identità associato all'applicazione.
3. Il servizio ZTNA HPE Aruba Networking verifica la richiesta di accesso dell'utente rispetto alle policy definite dal cliente.
4. L'utente viene continuamente autorizzato in base alla sua identità, al gruppo e ad altri criteri contestuali. NOTA: la piattaforma SSE HPE Aruba Networking può ispezionare attivamente il traffico e chiude la sessione se si verifica un evento di sicurezza.
5. ZTNA HPE Aruba Networking controlla la presenza di una connessione esistente all'applicazione per verificare un potenziale riutilizzo.
6. Quando avviene una nuova connessione, il connettore SSE più vicino identifica l'applicazione autorizzata e risponde con una connessione outbound al cloud SSE HPE Aruba Networking attraverso una porta specificata.
7. Il cloud SSE HPE Aruba Networking restituisce la nuova connessione al front-end dedicato.
8. Il front-end web stabilisce una connessione con l'applicazione.
9. L'accesso all'applicazione interna richiesta viene quindi esteso all'utente attraverso una connettività basata su browser.

ZTNA HPE Aruba Networking garantisce che venga concesso l'accesso all'applicazione senza richiedere l'accesso alla rete aziendale. Questo disaccoppiamento attenua i rischi di protezione della rete, come minacce interne o diffusione di ransomware, riducendo lo spostamento laterale attraverso una segmentazione a livello di applicazione.

A differenza di un concentratore VPN, ZTNA HPE Aruba Networking si basa su un'architettura avviata dal servizio per sfruttare connessioni solo outbound. Con questo tipo di connessione, l'infrastruttura di rete e le applicazioni aziendali sono nascoste da Internet e non possono essere individuate o verificate perché non restano in ascolto di ping inbound. Risiedono dietro al connettore SSE, che comunica esclusivamente con la piattaforma SSE HPE Aruba Networking. La piattaforma SSE può essere vista come l'intermediario tra l'entità (utente o applicazione) e l'applicazione.

HPE Aruba Networking tratta Internet come la nuova rete aziendale e sostituisce con microtunnel crittografati e dinamici basati su Internet le tradizionali connessioni di rete, come VPN sempre disponibili, MPLS e le connessioni da sito a sito per il cloud pubblico. In questo modo, i costi vengono ridotti e i team di rete e sicurezza sono liberi di dedicarsi a progetti più strategici invece di dover gestire appliance costose, aggiornare le versioni, distribuire hardware e pianificare i rinnovi.

Tabella 1.

	VPN	rispetto a	ZTNA HPE Aruba Networking
Esperienza utente Gli utenti si aspettano che l'accesso ad applicazioni private sia uguale all'accesso alle applicazioni SaaS.	**Esperienza utente insoddisfacente** Le VPN forzano gli utenti a installare un client nei loro dispositivi e a riconnettersi alla rete aziendale ogni volta che cambiano posizione. Poiché i gateway VPN hanno una presenza o punti limitati, i flussi non ottimali aggiungono latenza, a discapito della produttività degli utenti.	**rispetto a**	**Esperienza utente ininterrotta** SSE HPE Aruba Networking offre metodi di accesso con e senza client. Una singola policy zero trust segue l'utente e garantisce che abbia accesso solo alle risorse specifiche necessarie. L'esperienza utente sempre disponibile consente ai clienti di lavorare senza preoccuparsi di riconnettersi alla rete. I servizi ZTNA distribuiti tramite cloud offrono PoP globali che estendono in sicurezza la connettività a ogni posizione degli utenti, attraverso Internet.
Sicurezza L'azienda deve proteggere i dati dai cyberattacchi, a qualunque costo	**Maggiori rischi** I criminali informatici mirano attivamente alle tecnologie VPN e VDI con attacchi basati su Internet. Questi metodi di attacco incentrati sulla rete inseriscono gli utenti nella rete aziendale ed espongono l'infrastruttura alla rete Internet aperta. Con una semplice scansione delle porte, un utente malintenzionato può attaccare un'infrastruttura con un comportamento obsoleto, sottrarre credenziali e accedere alla rete aziendale come se fosse un utente legittimo.	**rispetto a**	**Nessuna superficie di attacco** La piattaforma SSE HPE Aruba Networking è progettata per non considerare mai niente intrinsecamente attendibile. Il servizio ZTNA connette gli utenti a specifiche risorse solo dopo una corretta ispezione e relativa convalida. Queste connessioni 1:1 sono solo di tipo outbound dalle risorse all'utente autorizzato, senza inserire gli utenti nella rete aziendale. Il modello di accesso con privilegi minimi garantisce che utenti e minacce non possano propagarsi lateralmente nell'ambiente. HPE Aruba Networking protegge inoltre le risorse inserendole dietro al servizio ZTNA, rendendole invisibili a Internet. I diritti di accesso possono quindi essere adattati automaticamente in base a cambiamenti del contesto, ad esempio la relazione con l'azienda, il comportamento del dispositivo, la posizione e così via.
Facilità d'uso Con la crescita del business e con la continua adozione del cloud, la semplicità e la scalabilità diventano requisiti prioritari.	**Maggiore complessità e costi elevati** Il ridimensionamento di servizi VPN richiede l'aggiunta di capacità all'intero gateway inbound, con l'acquisto, l'implementazione e la gestione di più appliance. Sono spesso necessari sistemi di bilanciamento del carico, firewall esterni ed esterni, servizi DDoS e altre appliance. Questo aumento di appliance è difficile da gestire e comporta un notevole incremento dei costi se si considera la spesa in termini di CapEx e OpEx associata alla gestione dell'intero gateway.	**rispetto a**	**Semplicità di gestione** I servizi distribuiti tramite cloud non richiedono appliance e vengono gestiti dal fornitore stesso. Sono progettati per offrire affidabilità, disponibilità e scalabilità con la crescita della domanda di traffico. Garantiscono l'esperienza più rapida possibile senza interruzioni per il business. Le integrazioni di API con servizi chiave dell'ecosistema, come IDP, sicurezza degli endpoint e SIEM, contribuiscono ad accelerare il processo di distribuzione. Questi servizi vengono addebitati per utente su base annua, quindi i costi di capacità e appliance non devono essere più considerati. L'IT può dedicare meno tempo e risorse ai servizi di connettività e concentrarsi invece sui progetti strategici fondamentali per le iniziative riguardanti l'ambiente di lavoro moderno.

Funzionalità esclusive di ZTNA HPE Aruba Networking

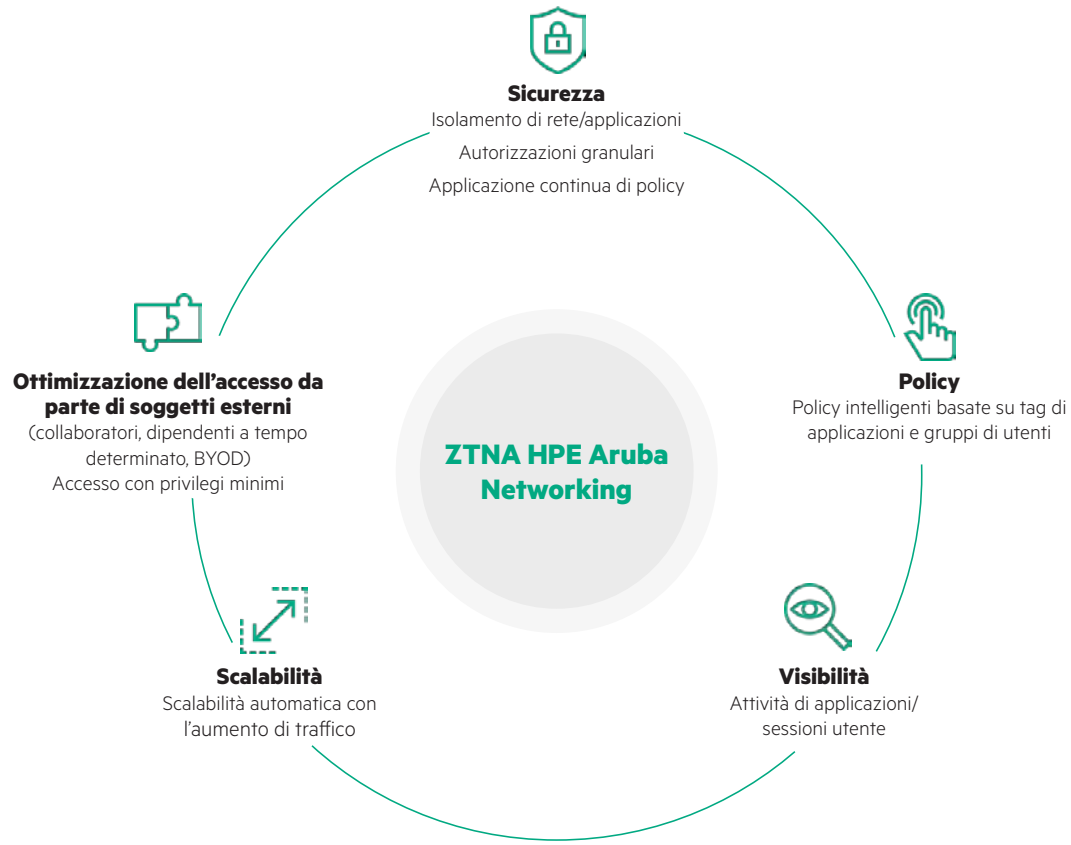

Figura 3. Fattori di differenziazione esclusivi di ZTNA

Consente la segmentazione granulare a livello di applicazione, senza segmentazione della rete
Riduce la potenziale superficie di attacco consentendo l'accesso solo a specifiche risorse. Limita lo spostamento laterale all'interno della rete, rimuove l'esigenza di complessi interventi di segmentazione della rete e riduce la potenziale superficie di attacco dell'azienda.

Supporta l'accesso ininterrotto alle applicazioni da qualsiasi dispositivo, con o senza client
Consente ai dipendenti remoti e ai soggetti esterni autorizzati di accedere in sicurezza alle risorse aziendali da un dispositivo di loro scelta nel modo più semplice possibile. Il metodo senza client supporta anche sessioni RDP basate su browser, riducendo l'esigenza di VDI.

Sintesi della soluzione

Adatta l'accesso in base a controlli contestuali potenziati da API
Adatta automaticamente i diritti di accesso in base a cambiamenti dei criteri chiave, tra cui posizione, identità e comportamento del dispositivo. Questa valutazione continua e adattiva dei rischi contribuisce a proteggere meglio i dati aziendali.

Semplifica la sicurezza con un'architettura interamente distribuita tramite cloud in 500 sedi globali all'edge
L'IT può smettere di dedicare tempo alla gestione di appliance VPN. Con SSE HPE Aruba Networking, ogni connessione viene negoziata nel sito all'edge SSE più indicato per fornirla, anche in caso di calamità. L'IT può avere la certezza che sarà in grado di ridurre le interruzioni e aumentare al massimo l'uptime.

Sostituisce la tecnologia VPN legacy
ZTNA HPE Aruba Networking gode del supporto di applicazioni private più ampio sul mercato. Oltre a tutto il traffico TCP e UDP, tra cui flussi di lavoro VoIP, da peer a peer e da server a client (che sono complessi per la maggior parte di fornitori di ZTNA), il servizio ZTNA supporta anche applicazioni web come SSH, RDP, Git, DB e così via. Ora i team IT possono sostituire completamente la VPN una volta per tutte.

Ispeziona tutto il traffico in entrata e in uscita dalle risorse private
Per la prima volta, è possibile acquisire visibilità completa sulle risorse a cui accedono dipendenti e soggetti esterni, oltre che sull'attività degli utenti, i download di file, gli accessi ai record e i comandi usati durante una sessione, con la possibilità di bloccare eventuali azioni dannose.

Inizia

Per saperne di più su ZTNA HPE Aruba Networking e su come usare il servizio in alternativa alla VPN, contatta uno dei nostri esperti di SSE. Oppure verifica di persona la potenza di HPE Aruba Networking con il nostro Test Drive gratuito di SSE.

arubanetworks.com

Prendi la decisione d'acquisto giusta. Contatta i nostri specialisti della prevendita.

Contattaci

Visita **ArubaNetworks.com**

SB_VPNWithHPEArubaNetworkingZTNA_DTA_013024 a00136658ite

Hewlett Packard Enterprise