HPE aruba networking

White paper aziendale

Il passaggio da VPN a ZTNA

Vantaggi di ZTNA e da dove iniziare

HPE GreenLake

60%

delle organizzazioni sostituiranno la VPN con un servizio ZTNA

La progressiva affermazione del lavoro da remoto ha introdotto nuove problematiche di sicurezza per le organizzazioni. Con il numero crescente di dipendenti che lavorano ovunque, le organizzazioni devono trovare soluzioni per proteggere l'accesso remoto e ibrido alle loro reti e ai dati. Una di quelle tipicamente utilizzate è la VPN (Virtual Private Network). Tuttavia, con la continua evoluzione delle minacce informatiche, la protezione delle VPN si è dimostrata inadeguata. ZTNA (Zero Trust Network Access) è una soluzione più efficace per la protezione dell'accesso remoto.

Che cos'è ZTNA?

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. ZTNA si basa su policy di accesso granulari per connettere gli utenti autorizzati a specifiche applicazioni, senza concedere l'accesso alla rete, ma attraverso un accesso segmentato con privilegi minimi senza mai esporre le posizioni delle applicazioni su Internet, a differenza delle VPN.

Secondo le previsioni di Gartner, entro il 2023 il 60% di organizzazioni sostituirà la VPN con un servizio ZTNA. ZTNA è quindi diventato il prodotto zero trust in più rapida crescita nel settore, con il 47% di responsabili IT che lo identificano come punto di partenza per le organizzazioni che intendono adottare una piattaforma SSE (Security Service Edge) come parte di un framework SASE (Secure Access Service Edge) più ampio.

ZTNA migliora la sicurezza

Uno dei principali motivi per cui le aziende adottano ZTNA è da attribuire alla maggiore sicurezza che offre. Con una VPN, gli utenti vengono inseriti direttamente nella rete aziendale. Una volta ottenuto l'accesso alla rete, possono spostarsi lateralmente e potenzialmente accedere a risorse o dati sensibili. Non c'è da stupirsi se una delle principali problematiche legate alle attuali soluzioni per l'accesso sicuro sia il fatto di concedere troppa fiducia agli utenti, come rilevato dal report SSE Adoption Report del 2023. Anche se si potrebbe dire che la questione è meno importante per gli utenti interni, è preoccupante sapere che un utente malintenzionato potrebbe approfittarsi della mancanza di segmentazione.

Al contrario, ZTNA non estende mai l'accesso alla rete e lo concede in base al contesto, che può essere l'identità dell'utente, il dispositivo che usa e le applicazioni e i dati a cui sta provando ad accedere. Questo significa che un utente malintenzionato che prova a ottenere l'accesso alla rete non sarà in grado di accedere ai dati sensibili senza una corretta autenticazione, ma non solo: il servizio ZTNA nasconderà l'esistenza stessa della rete, rendendola invisibile e irrintracciabile.

Le soluzioni ZTNA sono in genere meno costose da implementare e gestire rispetto alle soluzioni VPN. La VPN comporta costi che vanno ben oltre quelli iniziali.

ZTNA aumenta la scala e la flessibilità

Un altro motivo per cui le aziende adottano ZTNA è legato alla maggiore scala e flessibilità che fornisce. Mentre le soluzioni VPN sono in genere basate su hardware e appliance, le soluzioni ZTNA vengono distribuite tramite cloud, per cui sono facilmente accessibili dagli utenti e possono essere gestite dall'IT da qualsiasi posizione. Questo si rivela particolarmente utile per le aziende con dipendenti ibridi o da remoto oppure che hanno bisogno di accedere alle risorse da località diverse. Mentre le VPN hanno limiti di capacità statici basati sulle dimensioni delle appliance, l'architettura distribuita tramite cloud di ZTNA consente alle aziende di aumentare o ridurre facilmente la capacità per soddisfare le esigenze in evoluzione del business.

Soprattutto, i servizi ZTNA garantiscono policy di controllo degli accessi estremamente granulari e flessibili, che possono essere applicate fino al livello di utente e applicazione. La segmentazione degli accessi con la VPN implica una complessa segmentazione della rete, mentre con ZTNA l'implementazione di accessi con privilegi minimi richiede una semplice modifica delle policy.

ZTNA favorisce una maggiore produttività

Le soluzioni ZTNA forniscono un'esperienza di accesso migliore rispetto alle VPN. Le VPN ostacolano la produttività aziendale, perché gli utenti si ritrovano a fare i conti con velocità di connessione lente (a causa del backhaul della VPN), disconnessioni disagevoli e costanti e procedure di accesso complesse e ripetitive. Tutto questo interrompe il lavoro degli utenti e crea frustrazione.

La tecnologia ZTNA, al contrario, offre un'esperienza più intuitiva agli utenti finali. Consente di accedere facilmente alle applicazioni private perché elimina il backhaul del traffico, rimane sempre disponibile anche in caso di cambiamenti nella rete e crea una procedura di accesso semplice con profonde integrazioni con SSO e altre soluzioni di gestione delle identità.

ZTNA prevede costi più contenuti

Le soluzioni ZTNA sono in genere meno costose da implementare e gestire rispetto alle soluzioni VPN. La VPN comporta costi che vanno ben oltre quelli iniziali. In aggiunta ai concentratori, le VPN richiedono infatti hardware costoso on-premise, ad esempio misure di protezione da DDoS, firewall interni ed esterni, sistemi di bilanciamento del carico e così via. Tutto questo per un singolo stack di sicurezza inbound (le organizzazioni in media ne hanno 3-5). Oltretutto, i team di sicurezza devono in genere assegnare uno o più dipendenti dedicati al monitoraggio e alla gestione della VPN, distogliendo risorse da altri progetti più urgenti e importanti. Questo approccio alla protezione degli accessi incentrato sul perimetro è costoso da gestire.

Al contrario, le soluzioni ZTNA non richiedono l'installazione e la gestione di hardware o software ad alto costo on-premise. Inoltre, le organizzazioni vogliono implementare piattaforme SSE per eliminare la necessità di concentratori VPN (63%), le ispezioni SSL (50%) e la protezione da DDoS (44%). Infatti, le migliori piattaforme SSE offrono tecnologie ZTNA che eliminano completamente la VPN e lo stack di sicurezza inbound, con conseguenti risparmi significativi sui costi. Le soluzioni ZTNA sono inoltre intuitive e facili da gestire, consentendo alle organizzazioni di ridurre drasticamente il numero di risorse necessarie per gestire l'accesso sicuro. Infine, le soluzioni ZTNA sfruttano un modello di determinazione dei prezzi basato su abbonamento, che garantisce trasparenza sui costi ed evita alle organizzazioni di spendere più del necessario in licenze.

Non farti ostacolare dalla VPN

Con il numero di lavoratori ibridi e da remoto che continua ad aumentare, è importante per le aziende implementare una moderna soluzione per l'accesso sicuro. ZTNA è una soluzione moderna che supera ai limiti delle VPN e offre livelli superiori di sicurezza, flessibilità, scalabilità e prestazioni a costi contenuti per l'accesso remoto.

Il principale vantaggio di ZTNA è che rientra in una strategia di sicurezza di più ampio respiro. Tra le organizzazioni che intendono implementare una piattaforma SSE (Security Service Edge), vediamo che circa il 50% inizia con l'adozione di ZTNA. Da dove iniziare?

Sostituisci completamente la VPN con ZTNA HPE Aruba Networking

Ulteriori informazioni sull'uso di ZTNA HPE Aruba Networking in alternativa alla VPN

Scopri la piattaforma SSE HPE Aruba Networking

arubanetworks.com/products/sse

Visita **ArubaNetworks.com**

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

Contattaci

Hewlett Packard Enterprise

BWP_Switch-to-ZTNA_A4_RB_022224 a00136655ite