Accesso zero trust alle app private in ufficio e da remoto con Zscaler™

Migliaia di organizzazioni sono passate al lavoro da remoto e hanno superato con successo molte sfide legate alla protezione dei dati, all'accesso remoto sicuro e alla scalabilità, riuscendo a mantenere la continuità operativa. Indubbiamente, molte organizzazioni sono state spiazzate dall'urgenza e dalla rapidità con cui è stato necessario spostare la maggior parte della forza lavoro locale in remoto a tempo pieno, e nel bel mezzo del caos, per garantire l'accesso alle risorse aziendali, in molti hanno adottato servizi zero trust come alternativa ai metodi tradizionali incentrati sulla rete. Ora, con i team IT che iniziano a pianificare i prossimi anni, molti si chiedono quale sarà il futuro del lavoro e se il lavoro ibrido o completamente in remoto continuerà a essere la norma.

zscaler™

Dal punto di vista della sicurezza, il fatto che gli utenti si colleghino dai loro portatili in ufficio e da remoto può incrementare i rischi, soprattutto se vengono considerati automaticamente attendibili e possono accedere alla rete. Dal punto di vista dell'utente, la facilità di accesso deve essere la stessa, indipendentemente dalla sua posizione.

Tre considerazioni per i team IT guardando al futuro

Sebbene le amministrazioni pubbliche locali stiano adottando le giuste misure per riaprire le sedi fisiche, ci sono tre elementi importanti che un responsabile della sicurezza e/o delle reti dovrebbe considerare prima della riapertura.

1 Fornire l'accesso zero trust alle app private da qualsiasi luogo

Molte aziende commettono l'errore di pensare che lo zero trust sia fondamentale solo per fornire l'accesso remoto alle applicazioni private. Queste aziende utilizzano i servizi zero trust come alternativa alle tecnologie di accesso remoto, come VPN o VDI, che collocano gli utenti sulla rete. Dato che si trovano già all'interno del perimetro, i dipendenti che lavorano dall'ufficio sono generalmente autorizzati a connettersi alle risorse di rete, e vengono implicitamente considerati attendibili. Inoltre, il team potrebbe aver implementato la segmentazione della rete come misura di sicurezza aggiuntiva, operazione che rende la rete estremamente complessa. Alla luce di tutto ciò, non è più necessario segmentare la rete se si utilizzano i servizi zero trust appropriati. Lo stesso servizio zero trust può essere utilizzato sia per utenti che lavorano in sede che per dipendenti in remoto, e può essere impiegato anche per fornire una segmentazione a livello delle applicazioni, senza la necessità di gestire o affrontare la complessità della segmentazione della rete on-premise.

2 Offrire la migliore esperienza utente possibile dando priorità all'uniformità

Diversi sondaggi hanno dimostrato che i datori di lavoro e i dipendenti si sentono a proprio agio a lavorare da remoto. Molte organizzazioni indicano che, nonostante il passaggio al lavoro da remoto del personale, la produttività continua ad aumentare. Inoltre, i dipendenti in genere apprezzano la flessibilità di poter lavorare da qualsiasi luogo. Ecco perché diversi clienti con cui parliamo si stanno orientando verso un modello di lavoro ibrido, che prevede che i dipendenti alternino il lavoro da casa al lavoro in ufficio. I responsabili della rete e della sicurezza devono quindi assicurarsi che i dipendenti usufruiscano di esperienze uniformi e coerenti quando accedono alle applicazioni, da qualsiasi luogo, incluso l'ufficio.

3 Impedire ai dispositivi dannosi di accedere alla rete aziendale

Un altro fattore importante è la crescente popolarità dei servizi di sicurezza degli endpoint, come CrowdStrike, Microsoft e Carbon Black per il lavoro da remoto. Da un po' di tempo ormai, gli utenti hanno iniziato a lavorare con portatili e smartphone e ad accedere alle app da casa, attraverso le loro reti personali. Quando questi stessi dispositivi vengono portati in ufficio o nell'edificio, è importante che i responsabili IT non consentano loro di entrare sulla rete aziendale. Al contrario, l'IT deve assicurarsi che ogni dispositivo che ritorna in ufficio sia sicuro, per ridurre al minimo la superficie di attacco generale e le minacce. Per questo motivo, comprendere il profilo di sicurezza e lo stato del dispositivo è fondamentale, soprattutto con l'affermarsi del lavoro ibrido.

Utilizzare lo zero trust per il lavoro dall'ufficio e da remoto

Lo zero trust si basa su due elementi fondamentali: identità e policy aziendali.

Invece di utilizzare un indirizzo IP, l'identità fornisce il contesto utile a capire chi è l'utente. Le policy aziendali, impostate dal team responsabile della rete o della sicurezza, determinano a quale applicazione privata un utente autorizzato può accedere. La piattaforma Zero Trust Exchange™ di Zscaler ospita queste policy, le applica e, se consentito, agisce da broker della connessione tra app e utente su base 1:1, per ogni app e ogni sessione.

Dato che la posizione degli utenti continua a cambiare, non ha più senso focalizzare l'attenzione sulla rete. Man mano che gli utenti si preparano a tornare in ufficio, è ancora più importante allontanarsi dal concetto di attendibilità implicita e implementare delle policy zero trust. Lo ZTNA, o accesso zero trust alla rete, garantisce sicurezza, velocità, coerenza e praticità agli utenti e fornisce flessibilità e scalabilità all'IT.

Zscaler Private Access per l'accesso dei dipendenti alle app private in ufficio o da remoto

Zscaler Private Access™ (ZPA™) è un servizio cloud di Zscaler che fornisce un accesso fluido e zero trust alle applicazioni private che si trovano sul cloud pubblico o all'interno del data center. È in grado di supportare sia le applicazioni legacy che quelle basate sul web. Questo servizio elabora le informazioni provenienti da un provider di servizi di identità basato su SAML e collega l'utente autorizzato a un'applicazione specifica, in base alle policy aziendali definite dal cliente.
A differenza di VPN o VDI, ciò avviene senza collocare l'utente sulla rete aziendale, eliminando così la necessità di disporre di un set di gateway in entrata. Inoltre, questo servizio non espone mai l'applicazione a Internet, rendendola quindi invisibile agli aggressori, un aspetto particolarmente importante nell'ambito dell'accesso remoto.

ZPA utilizza tunnel criptati dall'interno verso l'esterno, uno dall'app e uno dall'utente, quindi agisce da broker delle connessioni in tempo reale in una delle sue posizioni di service edge, in base a dove si trovano l'utente e il dispositivo. Ciò avviene in modo da garantire il percorso più veloce possibile tra l'utente e l'applicazione, eliminando la necessità di effettuare il backhauling verso un data center centrale. Il service edge è ospitato pubblicamente da Zscaler o privatamente dal cliente; in quest'ultimo caso, è esteso alla filiale locale o al data center del cliente per l'applicazione in loco. In entrambi i casi, i service edge sono gestiti da Zscaler.

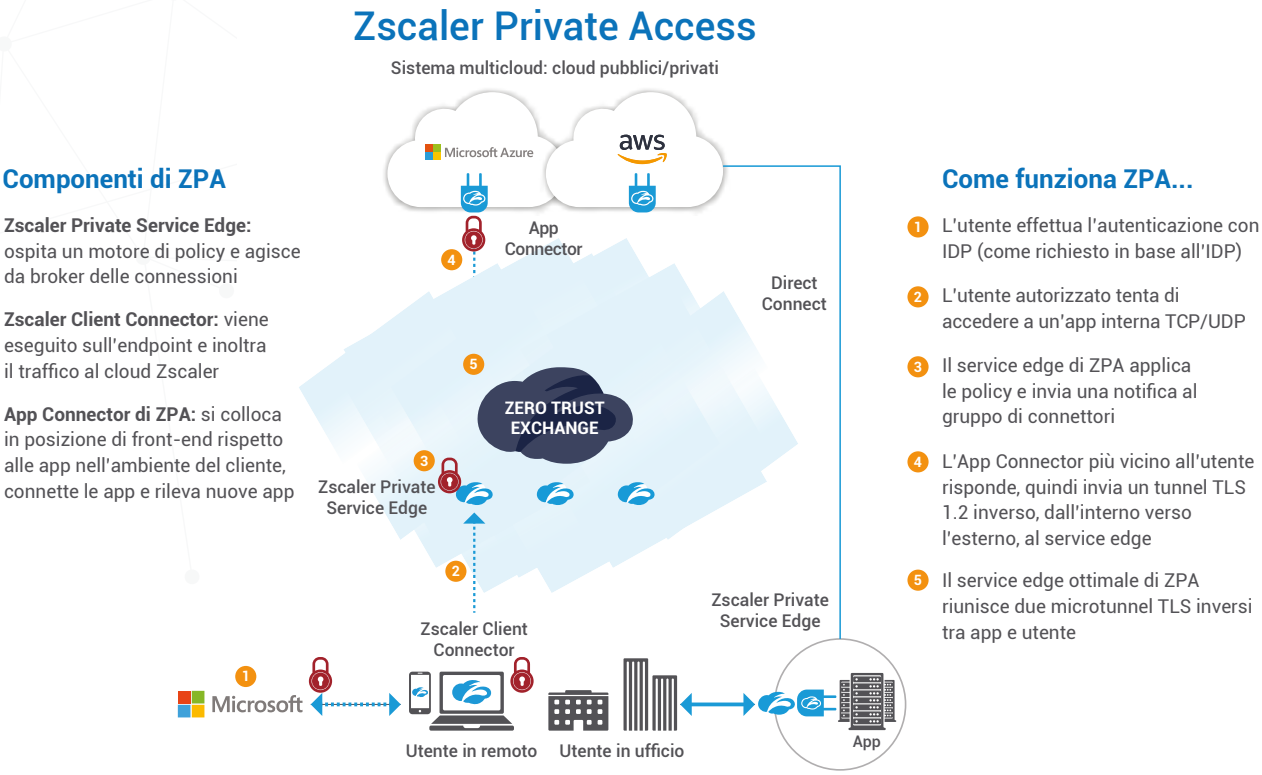
Dato che il servizio effettua la connessione in base all'utente e all'app, le applicazioni vengono segmentate senza la necessità di segmentare la rete. In questo modo, si semplifica la procedura di segmentazione, e l'IT può definire le policy per nome utente e nome host, anziché in base all'IP di origine e all'IP di destinazione.

ZPA utilizza tunnel criptati dall'interno verso l'esterno, uno dall'app e uno dall'utente, quindi agisce da broker delle connessioni in tempo reale in una delle sue posizioni di service edge, in base a dove si trovano l'utente e il dispositivo.

Gli stessi vantaggi dell'architettura zero trust, anche on-premise

Per le aziende che preferiscono ospitare un service edge di ZPA, abbiamo introdotto ZPA Private Service Edge. ZPA Private Service Edge è un'istanza privata, single-tenant, che fornisce le funzionalità complete della soluzione ZPA Service Edge pubblica all'interno dell'ambiente di un'organizzazione. Il cliente ospita ZPA Private Service Edge in sede o su un servizio cloud, e la soluzione viene gestita da Zscaler. ZPA Private Service Edge scarica le policy e le configurazioni pertinenti dal cloud, in modo che possa applicare tutte le policy di ZPA localmente.

ZPA Private Service Edge e i classici servizi di ZPA ospitati da Zscaler possono essere utilizzati in tandem. ZPA sceglierà automaticamente il percorso più veloce tra l'utente e la destinazione per eliminare la latenza.



Vantaggi principali di ZPA Private Service Edge

Riduzione della complessità e dei costi

Con ZPA Private Service Edge, firewall interni e apparecchi aggiuntivi non sono più necessari. In questo modo, non solo si abbattono i costi, ma si elimina anche la necessità di costruire segmenti di rete complessi per fornire l'accesso alle applicazioni agli utenti che lavorano on-premise.

Alta disponibilità

ZPA Private Service Edge archivia nella cache le policy di accesso per settimane, consentendo agli utenti di connettersi in modo sicuro, anche se la connettività a Internet viene persa. Così si garantisce la disponibilità continua dell'accesso alle applicazioni, indipendentemente dalla connettività.

Esperienza utente rapida

ZPA decide in automatico qual è il percorso più breve e veloce per consentire all'utente di connettersi alle applicazioni, dando la priorità al service edge locale di ZPA. Le funzionalità di doppio accesso della mediazione di connessioni in locale e su cloud pubblico ottimizzano automaticamente le prestazioni, indipendentemente dalla posizione degli utenti e delle applicazioni.

Conformità

Settori come quello dei servizi bancari e finanziari richiedono delle linee guida rigorose per l'utilizzo dei servizi con base cloud. ZPA Private Service Edge aiuta le aziende a garantire la conformità alle normative consentendo loro di ospitare il servizio on-premise.

Policy centralizzata con applicazione locale

ZPA Private Service Edge rimane sempre al passo con le policy aziendali collegandosi al servizio cloud di ZPA. Ciò garantisce l'applicazione di tutte le policy e le configurazioni pertinenti. In caso di guasto di Internet, ZPA Private Service Edge memorizza tutte le policy per 14 giorni, per garantire che l'accesso degli utenti on-premise alle applicazioni private non subisca interruzioni.

ZPA Private Service Edge offre un modo più semplice per consentire l'accesso sicuro alle app private, garantendo la stessa esperienza agli utenti locali o da remoto che accedono alle app nel data center o nel cloud.

Desideri saperne di più su ZPA? Contatta il nostro team in qualsiasi momento: **sales@zscaler.com**.

Scopri di più su **ZPA Private Service Edge**

Richiedi una demo

Informazioni su Zscaler

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale, in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati, grazie alla connessione sicura di utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in più di 150 data center a livello globale, Zero Trust Exchange, basata su SASE, è la più grande piattaforma di cloud security in linea del mondo. Scopri di più su **zscaler.it** o seguici su **Twitter @zscaler**.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.it