Guida all'adozione di un servizio ZTNA per gli architetti di rete

Le strategie da adottare per utilizzare lo ZTNA come alternativa alla VPN

zscaler™

Con le applicazioni private che si spostano verso il cloud e gli utenti che lavorano da remoto, le aziende hanno bisogno di un servizio in grado di garantire l'accesso sicuro a queste app e di offrire agli utenti un'esperienza fluida e rapida. Nonostante il fermento intorno al tema della sicurezza zero trust, per limitare la connettività degli utenti alle applicazioni, alcune aziende tentano di utilizzare le architetture già esistenti incentrate sulla rete e basate su firewall di nuova generazione concepiti per l'accesso a quest'ultima. Queste architetture ormai datate non sono adatte a rispondere alle esigenze attuali, e non sono state progettate per collegare gli utenti autorizzati a delle app specifiche. Collocando gli utenti sulla rete, queste tecnologie aumentano il rischio di movimento laterale verso altre app, di esposizione degli indirizzi IP a Internet e di attacchi DDoS attraverso concentratori VPN che si trovano all'edge della rete e che ascoltano i ping in entrata.

Sono molte le aziende che stanno considerando lo ZTNA (Zero Trust Network Access) come alternativa alla VPN. Infatti, secondo quanto stimato da Gartner per il 2021, il 60% delle imprese avrebbe eliminato le VPN esistenti per adottare un servizio ZTNA. Ma la realtà è che, in qualsiasi grande organizzazione globale, anche un piccolo cambiamento nel modo in cui gli utenti accedono alle applicazioni può dar vita a enormi complessità da gestire. Questo documento ti aiuterà a capire da dove iniziare per adottare lo ZTNA in modo rapido e senza interruzioni per il business.

In questa guida troverai:

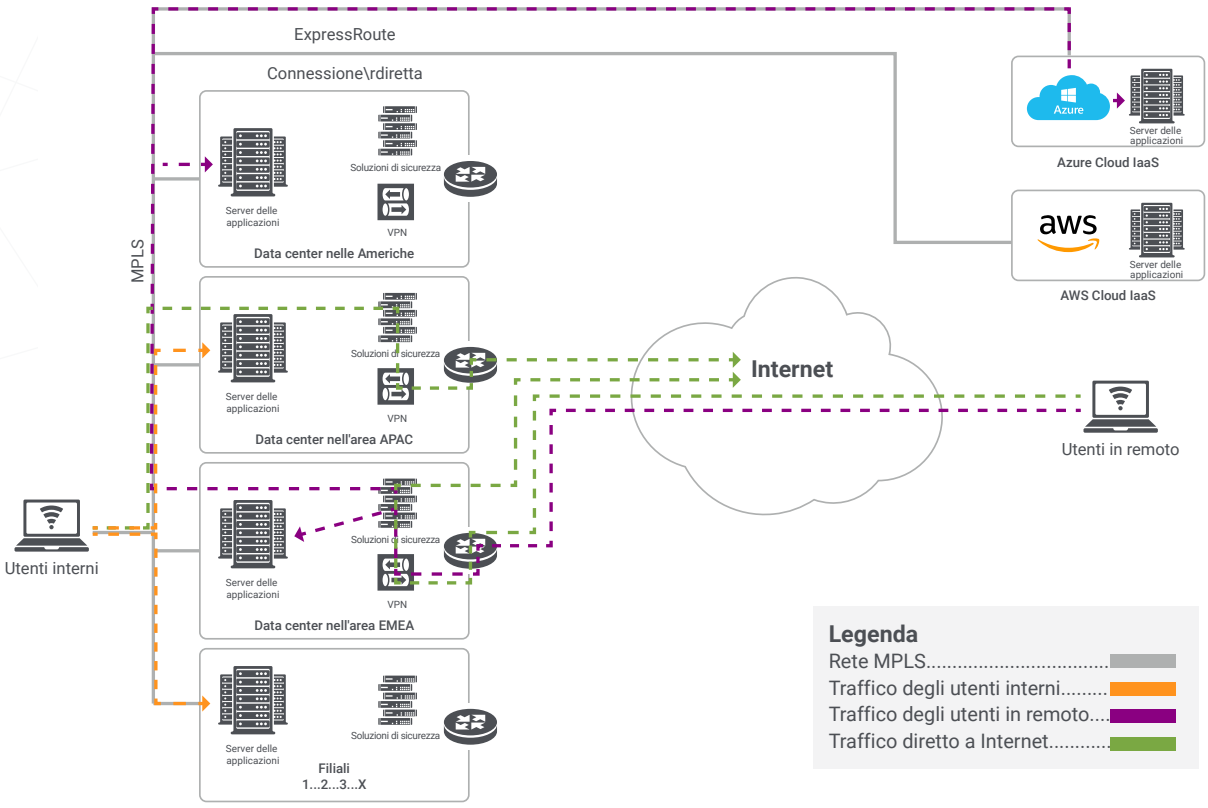
- le differenze architetturali tra la tecnologia di accesso esistente e lo ZTNA;
- Una panoramica su un'architettura di riferimento per la distribuzione dello ZTNA
- Tre fasi da considerare quando si adotta lo ZTNA in un'azienda
- Suggerimenti e considerazioni degli esperti per ottenere il massimo dalla distribuzione dello ZTNA

Prima di iniziare, ti consigliamo di leggere "La mitigazione del rischio attraverso il perimetro definito da software". Questo blog fornisce una panoramica iniziale dei servizi ZTNA.

Ora esploreremo l'architettura ZTNA come mezzo per connettere gli utenti autorizzati a delle applicazioni private specifiche senza mai collocarli sulla rete.

Dove si colloca oggi la tua azienda? - Uno sguardo alla VPN in azienda

In questo diagramma generale è rappresentata l'architettura che ritroviamo in un gran numero di organizzazioni. Ovviamente, il numero e l'ubicazione dei data center, dei router, dei firewall, dei concentratori VPN e della rete MPLS non saranno identici a quelli indicati in questa immagine, ma si tratta comunque una rappresentazione sufficientemente fedele dei vari componenti. Ci sono anche molti altri dispositivi di rete e sicurezza distribuiti dalle organizzazioni, tra cui proxy inline, sandbox, firewall L7, soluzioni di AV e DLP, ecc. Per semplicità, nelle immagini, l'intero concetto di sicurezza diretta a Internet è stato consolidato con l'espressione "Soluzioni di sicurezza".



Ci sono alcune cose importanti da notare in questo tipo di architettura tradizionale:

01 Gli utenti in remoto si collegano tramite VPN a uno dei data center e vengono collocati sulla rete aziendale. In base alla mia esperienza con molte organizzazioni, la rete è relativamente piatta, e le ACL sono piuttosto limitate; in questo modo, l'intera infrastruttura dei data center e le reti dell'azienda sono esposte a tutti gli utenti in remoto.

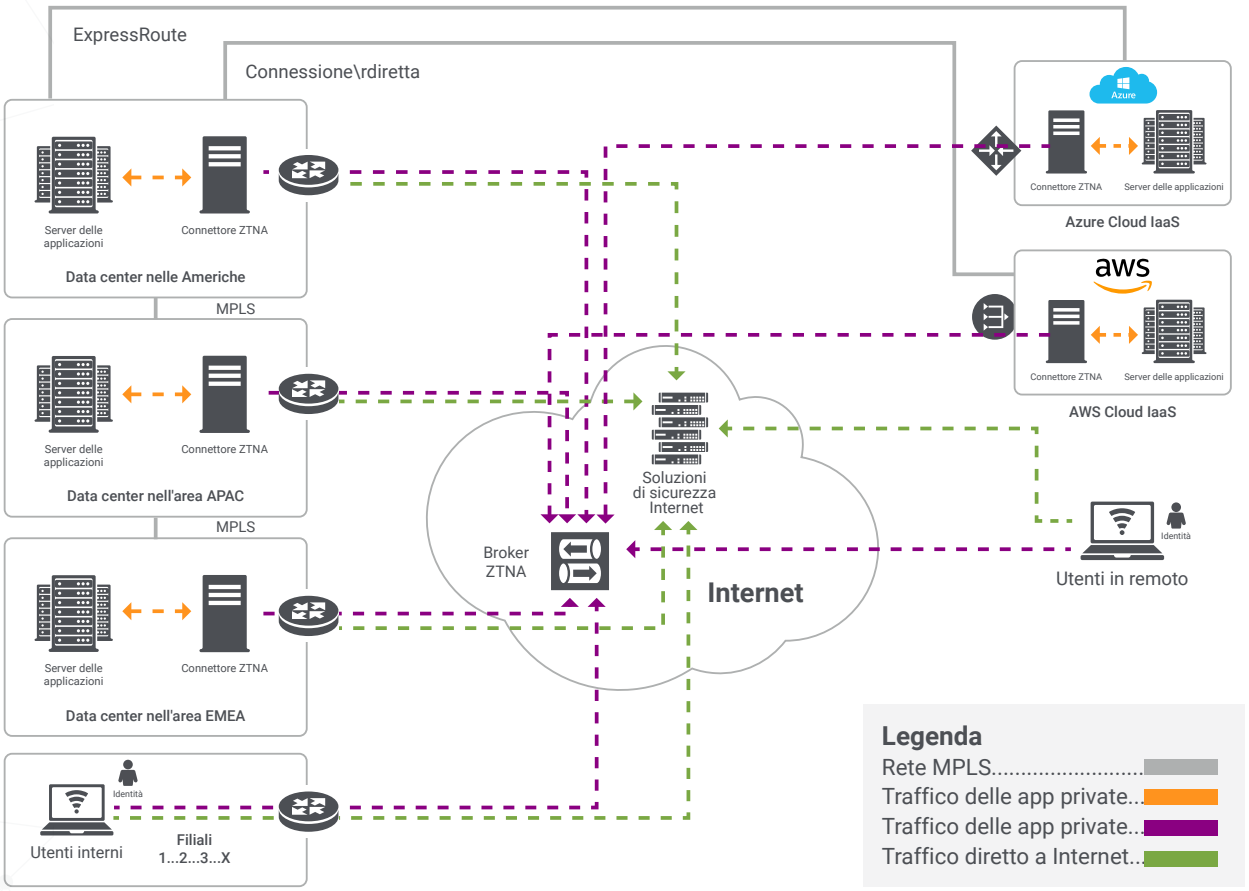
02 Tutto il traffico diretto a Internet di questi ultimi verrà reindirizzato verso il data center affinché venga ispezionato tramite le soluzioni di sicurezza (hardware) di cui l'organizzazione è in possesso. Questa struttura è nota come Full Tunnel VPN, che è ideale per i team di sicurezza che devono garantire la sicurezza quando gli utenti si trovano al di fuori della rete aziendale, ma può influire negativamente sull'esperienza utente, se tutte le applicazioni Internet/SaaS vengono sottoposte al backhauling invece di uscire in locale. Attualmente, molti utenti dispongono di connessioni Internet domestiche a banda larga che sono più veloci di alcune connessioni WAN aziendali (anche in aree piuttosto rurali si può ottenere una connessione in fibra da 1 Gbps tramite un ISP)!

03 Gli utenti interni sono generalmente su reti di dispositivi/utenti, fisiche o wireless, ma possono comunque dirigersi/collegarsi a tutte le reti dei data center, in quanto queste reti sono tradizionalmente ritenute "attendibili". L'accesso ai percorsi delle applicazioni interne avviene tramite LAN, e le applicazioni Internet/SaaS passano attraverso le soluzioni di sicurezza prima di uscire verso l'ISP. Il problema di questa infrastruttura è dato dalla concezione errata che, solo perché la rete è "di proprietà" e la si controlla, ci si debba fidare automaticamente di tutti gli utenti e i dispositivi presenti su di essa.

Ricorda che, per l'accesso remoto, è richiesto prima l'accesso in entrata (VPN) da Internet, e gli utenti interni possono comunicare direttamente con tutti i server delle applicazioni, indipendentemente dall'identità.

Un'architettura di riferimento per fornire l'accesso alle app interne senza incrementare il rischio

L'obiettivo finale di un'architettura definita da software è quello di separare l'accesso alle applicazioni dall'accesso alla rete. Gli utenti non dovranno più essere collocati sulla rete, le applicazioni private saranno accessibili solo agli utenti autorizzati, gli indirizzi IP non saranno mai esposti a Internet e la complessità della gestione dei segmenti di rete, delle policy FW e delle ACL verrà eliminata. Nell'immagine viene rappresentato l'aspetto semplificato del risultato finale.



Con questa nuova architettura definita da software, vi è una netta separazione tra le reti di data center/applicazioni, utenti in remoto e utenti interni. Non importa se l'organizzazione dispone solamente di due data center con sede negli Stati Uniti, di una dozzina di data center in tutto il mondo o di alcuni ambienti Azure/AWS/GCP, ecc.; i risultati sono piuttosto chiari, e sono riportati di seguito.

01 Le reti private, come MPLS o persino VPN site-to-site, dovrebbero essere necessarie solo tra i data center e gli ambienti cloud IaaS in cui è richiesta la comunicazione da server a server. Se l'organizzazione ha spostato il livello del sito web www su AWS, ma il database SQL di backend è ancora collocato in un data center fisico, è comunque necessaria una connettività privata (bassa latenza, alta larghezza di banda) tra queste posizioni.

02 L'accesso remoto non richiede più la connettività in entrata per gli utenti, come ad esempio tramite vpn. azienda.it! Questa architettura colloca il piano di orchestrazione (controllo) sul cloud, dove la comunicazione da parte degli utenti viene interrotta. I gateway, noti nel mondo Zscaler come ZPA App Connector, non richiedono porte di ascolto in entrata, un record IP/DNS pubblico. Questi connettori comunicano in uscita tramite TLS con il piano di orchestrazione basato su SaaS. Le connessioni alle applicazioni interne vengono concesse solo dopo che l'identità dell'utente è stata verificata e valutata in base alle policy di accesso.

- Se un utente è autorizzato ad accedere a un'applicazione o alle risorse interne, il piano di orchestrazione collega le connessioni TLS in uscita ai connettori e ai dispositivi dell'utente. Tuttavia, l'utente non viene collocato sulla rete, quindi le applicazioni basate su DNS vengono offuscate; questo significa che i veri indirizzi IP privati dei server delle applicazioni non vengono esposti ai dispositivi degli utenti. Viene invece creato dinamicamente un indirizzo IP sintetico sul client per ogni applicazione a cui viene effettuato l'accesso.

- Se a un utente non viene consentito l'accesso a un'applicazione interna, non verrà mai generato alcun traffico di rete in ingresso nel data center. La richiesta viene bloccata sul cloud, eliminando così il rischio relativo alla possibilità degli utenti di raggiungere la "porta di ingresso" dei server delle applicazioni critiche. In poche parole, in questo sistema gli utenti vengono bloccati sul cloud, prima di poter creare una sessione SSH o RDP con un server. Anche se molto probabilmente l'utente non sarebbe comunque in grado di autenticare la sessione SSH/RDP (se non con tecniche di forza bruta o credenziali rubate), questa architettura elimina completamente questo rischio. Qual è la parte migliore? Ognuno di questi tentativi viene registrato per consentire ai team responsabili della sicurezza di monitorare in modo proattivo (e reattivo) l'attività degli utenti. Ad esempio, tutti i log possono essere inviati a un SIEM, come Splunk, e può essere creato un avviso se un utente genera un determinato numero di policy bloccate in un determinato numero di minuti sugli stessi server o porte; ad esempio, nel caso in cui un utente abbia provato a effettuare connessioni SSH su sap.azienda.it 20 volte in 5 minuti. Se l'utente viene bloccato dalle policy, ci si può ritenere al sicuro ed è possibile agire proattivamente per verificare se il dispositivo dell'utente è stato compromesso o se l'utente ha intenzioni dannose. Se invece non fosse stato bloccato dalle policy, le sessioni SSH sarebbero state avviate, ma il server avrebbe rifiutato le credenziali errate; questo significa che l'utente era autorizzato, ma che aveva dimenticato la password di amministratore (root)!

03 Tutte le reti degli utenti devono essere trattate come degli Internet point o delle reti Wi-Fi per ospiti. Che l'utente si trovi nella hall principale della sede centrale, in una filiale, in uno stabilimento di produzione o semplicemente in viaggio, non dovrebbe mai esserci un motivo per collocarlo sulla rete, da cui è in grado di esplorare l'ambiente e dirigersi verso i server delle applicazioni e i data center. È importante notare che alcuni siti di filiali potrebbero avere requisiti che vanno al di là dell'utente per l'accesso alle app. In questo caso, i dispositivi IoT e le comunicazioni da server a server necessitano comunque di una connettività alle reti private. Tuttavia, anche in presenza di questo requisito, è meglio separare tali reti da quelle degli utenti.

04 Anche l'accesso a Internet con le soluzioni di sicurezza deve essere modernizzato, per offrire una sicurezza e un'esperienza utente di livello superiore. Quando si separano gli utenti dalla rete, è necessario considerare la possibilità di inviare il traffico Internet direttamente dagli utenti, anziché farlo passare attraverso un data center centrale per l'ispezione. Per gli uffici delle filiali, questo può essere semplice come utilizzare un router, un firewall o un dispositivo SD-WAN esistente per indirizzare tutto il traffico Internet verso una soluzione di sicurezza sul cloud, come la piattaforma Zscaler Internet Access. Tutte le soluzioni di sicurezza sono offerte come servizio e, con oltre 100 sedi nel mondo, questo significa che è possibile inviare tutto il traffico delle sedi aziendali ai siti Zscaler più vicini per l'ispezione! Anche se un utente è in viaggio, il client unificato Zscaler App, un agente di inoltro leggero distribuito sui dispositivi mobili e sui laptop degli utenti, è in grado di offrire un'ottima esperienza utente (attraverso l'invio locale del traffico Internet al nodo di Zscaler più vicino, invece di effettuare il backhauling), fornendo però al team IT i controlli di sicurezza e la visibilità di cui necessita.

Le tre fasi necessarie per adottare un'architettura ZTNA

Gli architetti si chiedono spesso quale sia il modo migliore di iniziare questo percorso. La risposta più adeguata: "Dipende". Molti ingegneri e architetti si riconosceranno in questa risposta, perché si possono ottenere molti risultati diversi in base alle esigenze specifiche, ai requisiti e alla configurazione. Tuttavia, è nostra responsabilità fornire alle organizzazioni i consigli su quali strategie adottare per affrontare questo percorso. È necessario sottolineare che l'approccio discusso in questa sezione, che prevede la suddivisione di questo processo in più fasi, non consiste in un elenco fisso di passaggi che deve essere seguito indistintamente da tutte le organizzazioni. Si tratta di un approccio generale che sarà efficace in diversi contesti per soddisfare i requisiti attuali, ma che allo stesso tempo consentirà all'organizzazione di adottare il concetto di rete zero trust. L'attendibilità, o trust, non è mai implicita, e l'accesso è adattivo, ossia basato sulle policy contestuali stabilite dagli amministratori (utente, dispositivo, servizio, ecc.).

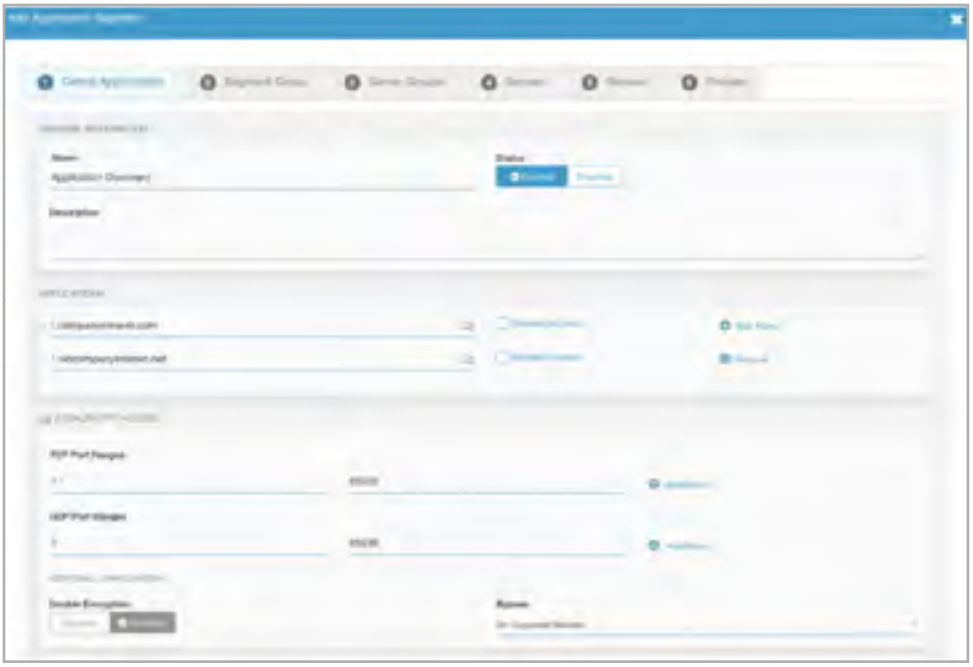
Questo approccio va considerato come un insieme di piccoli passaggi: inizia con gli utenti in remoto, sviluppa dei segmenti, quindi sfrutta lo ZTNA per consentire l'accesso alle app private a tutti gli utenti, indipendentemente dalla posizione. Andranno considerati il modo in cui gli utenti accedono alle applicazioni e ai servizi, la distribuzione (quantità e tipologia) delle sedi aziendali (data center, ambienti cloud IaaS e sedi fisiche da cui lavorano i dipendenti) ed eventuali tempistiche dei progetti. In molti casi, un aggiornamento della VPN potrebbe servire da catalizzatore per adottare lo ZTNA, invece di acquistare una VPN di nuova generazione o "always-on", che porta con sé le stesse sfide della VPN di cui già si dispone.

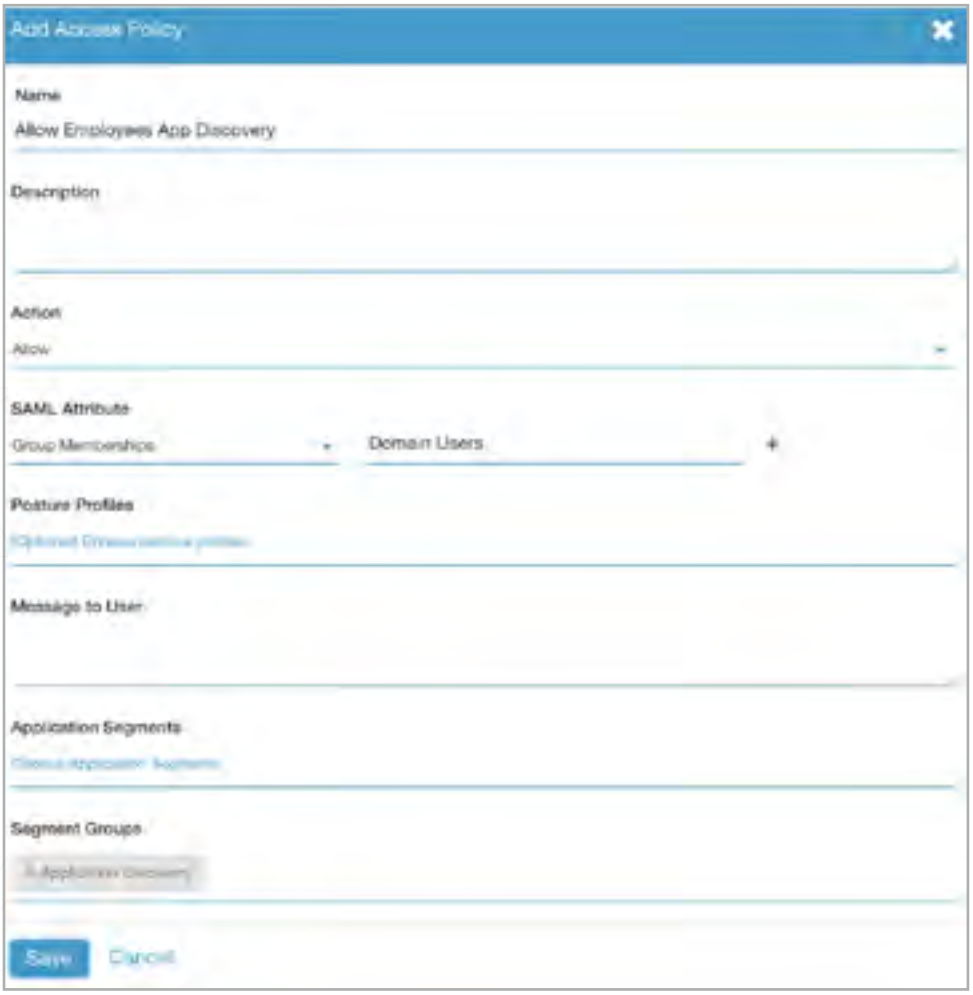
Fase 1 Come distribuire lo ZTNA per l'accesso remoto e il rilevamento delle applicazioni

In questa fase, inizierai sostituendo la soluzione VPN di accesso remoto esistente. A tale scopo, potrebbe essere necessario distribuire lo ZTNA con dei livelli di accesso simili alla VPN di accesso remoto di cui già disponi. Si tratta di un aspetto fondamentale per assicurarti che la nuova iniziativa non venga vista come un ostacolo alla produttività degli utenti in remoto.

Dovrai inoltre capire quali applicazioni private sono in esecuzione nell'ambiente aziendale, per ridurre la superficie di attacco ed eliminare lo Shadow IT. È molto probabile che esistano molte più applicazioni di quelle di cui sei a conoscenza. La nostra soluzione Zscaler Private Access (ZPA) risolve questo problema, grazie alla funzione Application Discovery. È impossibile essere a conoscenza di tutte le applicazioni e dei servizi interni a cui ogni utente deve accedere; ecco perché Application Discovery consente di utilizzare dei caratteri jolly, come *.azienda.it, *.azienda.net, tutte le porte TCP e UDP.

Una volta che un utente si è registrato con successo al servizio, il client rileva automaticamente quando non si trova più sulla rete aziendale; inoltre, tutte le applicazioni interne ora passano attraverso lo ZTNA quando l'utente non è sulla rete. Non è più necessario avviare un client VPN, e l'utente può accedere alle risorse interne esattamente come prima. Tutti questi log di accesso si trovano nella console di amministrazione di ZPA, e possono anche essere trasmessi quasi in tempo reale a un SIEM, per ottenere una visibilità granulare sulle applicazioni a cui gli utenti accedono.





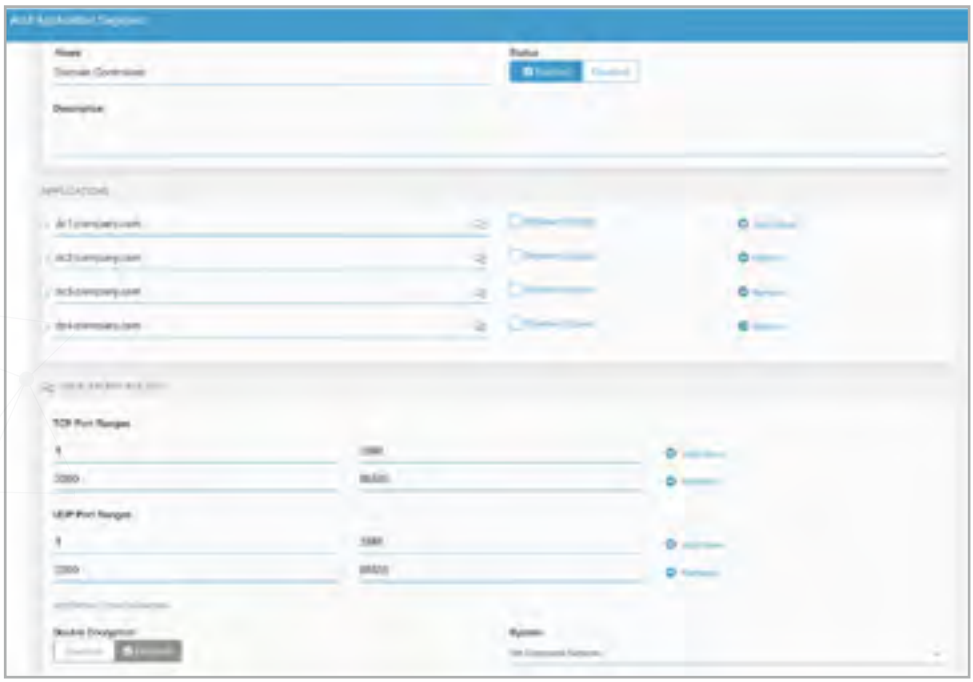
Poiché la rete privata interna (MPLS, VPN da sito a sito) molto probabilmente esiste ancora, il client Zscaler App disattiverà automaticamente ZPA quando l'utente tornerà sulla rete aziendale. Ora, tutti gli accessi alle applicazioni interne avvengono sulla LAN, senza la presenza di Zscaler nel percorso.

Fase 2

Sfruttare la microsegmentazione per garantire una connettività a privilegi minimi

In questa fase, dovrai definire le policy che separano le applicazioni private in segmenti e fornire l'accesso a tali segmenti tramite degli attributi relativi all'identità degli utenti

Dato che le grandi organizzazioni possono avere centinaia o migliaia di applicazioni/servizi specifici, per molte di esse potrebbe essere meglio segmentare le porte di gestione, come TCP 22 (SSH) e TCP/UDP 3389 (RDP), e fornire solo l'accesso a queste porte a livello globale per gli utenti IT. Naturalmente, ogni organizzazione ha le proprie esigenze specifiche, ma questo tipo di segmentazione può aiutare a ridurre la superficie degli utenti che si connettono a server a cui non dovrebbero essere in grado di accedere. Ad esempio, il personale addetto alle vendite non dovrebbe essere in grado di accedere alla porta TCP 3389 su un server Windows che ospita l'applicazione SAP; dovrebbe poter accedere solo alla parte web front-end, che si trova sugli stessi server, ma solo sulle porte TCP 80/443.



I server dell'infrastruttura, che possono essere servizi/controller di dominio, client di software di sicurezza, client di distribuzione di software, ecc., possono essere facilmente segmentati in quanto gli host sono noti.

La segmentazione delle applicazioni è un processo continuo, e il consiglio generale è quello di dare la priorità alle applicazioni più critiche per l'azienda, che devono essere accessibili solo agli utenti noti.

Con la segmentazione, le applicazioni vengono rimosse dal "pool" della funzione di rilevamento delle applicazioni. Ciò significa che è possibile combinarle, per garantire che gli utenti possano comunque accedere alle applicazioni nei domini aziendali che non sono stati definiti esplicitamente e anche raggiungere le applicazioni note sulle porte di servizio richieste.

NOTA: non dimenticarti della sicurezza su Internet

In questa guida ci concentriamo sulle applicazioni private, ma è importante rendersi conto che è altrettanto fondamentale fornire delle soluzioni di sicurezza anche per tutto il traffico diretto a Internet. Molte organizzazioni stanno esplorando delle soluzioni di sicurezza in entrata e in uscita più moderne e completamente cloud, invece di affidarsi a dispositivi fisici o virtuali (come i firewall). La soluzione di sicurezza sul cloud in uscita di Zscaler è chiamata Zscaler Internet Access (ZIA).

Fase 3 Lo ZTNA per l'accesso alle app private per tutti gli utenti (non solo quelli in remoto)

Ora, è giunto il momento di passare alla fase finale. Ciò significa che, da adesso in poi, tutto l'accesso alle applicazioni private si baserà su impostazioni precise che abiliteranno automaticamente solo una connettività esplicita e a privilegi minimi.

ZPA fornisce tutto questo attraverso una connettività dall'interno verso l'esterno tramite microtunnel TLS a doppia crittografia, che vengono utilizzati per ogni singola sessione e creano un segmento sicuro singolo tra un utente autorizzato e un'app privata specifica.

Come già indicato in precedenza, Zscaler App è in grado di rilevare la rete aziendale. Ciò significa che, su ZPA, ogni segmento di applicazione ha un'opzione di configurazione per (1) bypassare ZPA quando si trova sulla rete aziendale, (2) bypassare ZPA sempre o (3) mai. Nella fase 1, hai distribuito i segmenti delle app utilizzando l'opzione 1, ma se l'accesso sicuro dovesse essere fornito a tutti e non solo agli utenti in remoto? Per fare questo, è sufficiente cambiare i segmenti delle app affinché la soluzione ZPA non venga mai bypassata. Ciò significa che, anche quando gli utenti si trovano in un ufficio fisico, la soluzione, che sfrutta un'architettura basata sull'attendibilità esplicita, medierà tutti gli accessi alle risorse interne, e gli utenti non verranno mai instradati dalla LAN direttamente ai server delle applicazioni sul data center!

Da

A

Semplice, no? La nostra piattaforma è in grado di superare le sfide di questo cambiamento. L'obiettivo finale in genere è quello di rimuovere completamente le reti dei server delle applicazioni/data center da tutte le reti degli utenti. Ciò significa che non vi sarà più connettività tra filiali, stabilimenti di produzione, ecc. (per essere chiari, intendiamo la connettività dalle reti degli UTENTI in queste sedi) e il data center.

Considerazioni finali e suggerimenti degli esperti:

Potrebbe essere più semplice iniziare con un piccolo ufficio nuovo, che non sia già sulla rete. Apri l'ufficio con una semplice connessione Internet a banda larga. Fai in modo che tutto il traffico diretto a Internet venga indirizzato verso una piattaforma di sicurezza sul cloud (come ZIA) e che tutto il traffico delle applicazioni private passi attraverso la piattaforma ZPA.

Tratta il nuovo ufficio come un Internet point. Tieni sempre a mente che ora siamo in grado di fornire questa connettività per consentire agli utenti di accedere alle applicazioni; alcune sedi, però, come un impianto di produzione con sensori, dispositivi IoT e server, avranno probabilmente bisogno di comunicare comunque con i data center tramite MPLS o VPN private. Tratta le reti di queste sedi come dei data center, e allontana semplicemente gli utenti da esse; tutti gli utenti avranno accesso alla "rete Wi-Fi guest" e l'accesso alle app interne sarà consentito agli utenti autorizzati.

In conclusione, possiamo dire che c'è molto entusiasmo e interesse verso le architetture ZTNA, ma il vero obiettivo, quando si tratta di utilizzare le app private, è quello di offrire l'esperienza che gli utenti desiderano, con la sicurezza di cui hanno bisogno. Ci vorrà del tempo prima che l'organizzazione adotti questo nuovo metodo, ma tutti gli architetti di rete possono fare la propria parte per gettare le basi (piattaforme) che lo renderanno possibile.

Scopri ZPA in prima persona, e registrati per una prova in hosting di 7 giorni all'indirizzo **https://www.zscaler.it/zpa-interactive.**

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.it