Migrare su AWS in modo semplice e sicuro con Zscaler

Zscaler Private Access e il framework di adozione del cloud AWS

Indice

Introduzione

Questo documento intende mostrare il modo in cui Zscaler™ è in grado di accelerare l'adozione da parte degli utenti eliminando gli attriti associati al raggiungimento degli obiettivi di rete e di sicurezza. Analizzando il modo in cui Zscaler Private Access™ (ZPA™) risponde ai casi d'uso della migrazione su AWS, sarà possibile fornire un approccio strutturato alla soluzione completa e illustrare come ZPA accelera la migrazione delle applicazioni.

Quando Zscaler è coinvolto in progetti commerciali e per il settore pubblico, l'architettura di ZPA agisce da fattore abilitante per offrire una maggiore agilità a utenti e applicazioni e accelerare la migrazione di queste ultime.

La funzione principale di ZPA consiste nel gestire attivamente l'accesso e l'interazione degli utenti autorizzati con i carichi di lavoro, prima, durante e dopo la migrazione sul cloud, migliorando al contempo l'esperienza complessiva dell'utente finale.

Le best practice impiegate nell'architettura di Zscaler Private Access svolgono una funzione chiave nelle fasi di migrazione sul cloud dei clienti, tra cui:

- Preparazione e pianificazione
- Portfolio e rilevamento
- Pianificazione operativa e distribuzione
- Migrazione e convalida
- Funzioni operative continue

I vantaggi di Zscaler Private Access (ZPA):

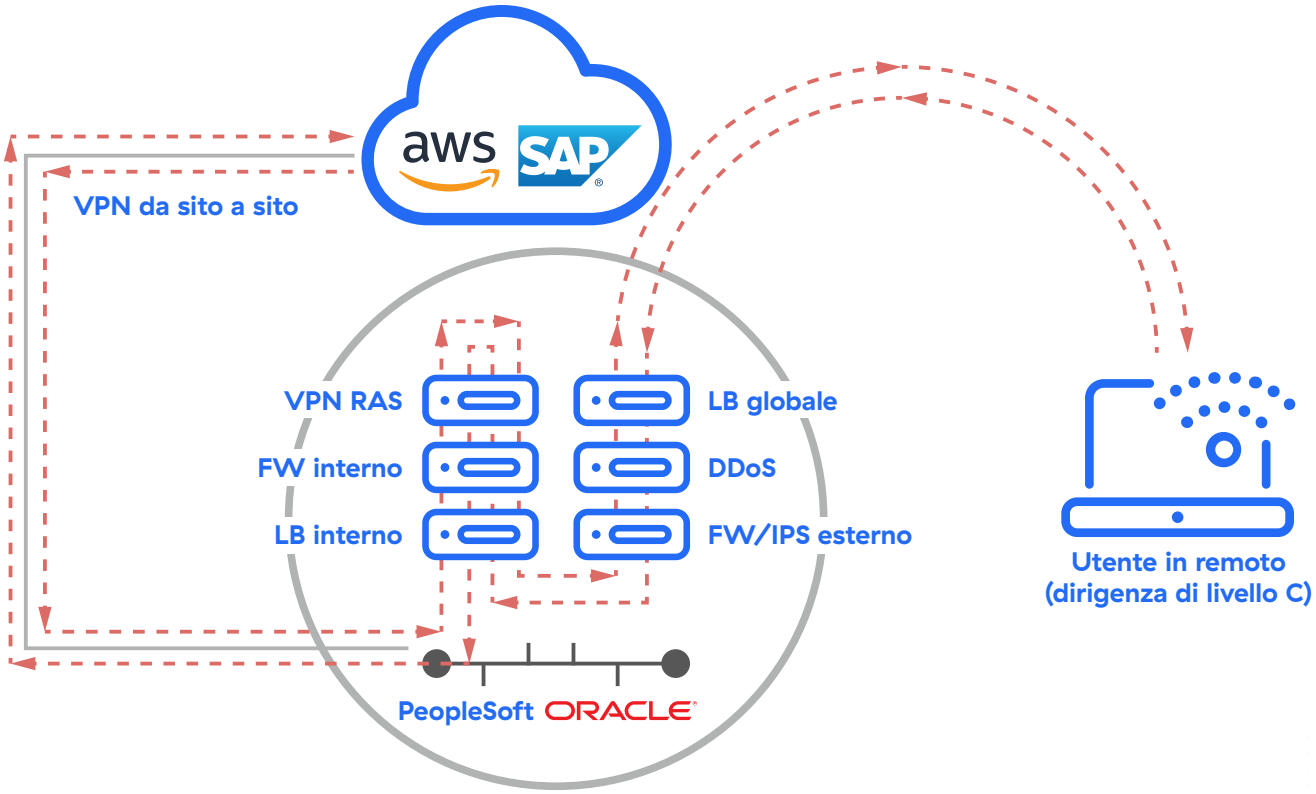
- **Accelera la migrazione delle applicazioni e l'adozione del cloud**
- **Consente un controllo granulare dell'accesso degli utenti alle applicazioni ospitate su AWS**
- **Gestisce attivamente l'accesso ai carichi di lavoro, prima e dopo la migrazione**
- **Fornisce una visibilità end-to-end sulle app e migliora l'esperienza utente**

Sebbene questo documento si concentri sulla migrazione dei carichi di lavoro su AWS, ZPA e le relative soluzioni di perimetro definito da software non sono specifiche per le distribuzioni di AWS. ZPA supporta gli ambienti IT ibridi e può essere complementare ai framework di migrazione delle applicazioni definiti tramite consulenze.

Zscaler Private Access: proteggere l'accesso alle applicazioni interne

Zscaler Private Access fornisce un accesso sicuro alle applicazioni interne, siano esse ospitate su data center privati o sul cloud pubblico. Zscaler riduce i costi e la complessità delle problematiche associate alle reti e alla sicurezza legacy migliorando al contempo l'esperienza utente di accesso alla rete tramite le tradizionali VPN.

La maggior parte dei clienti inizia con un'infrastruttura di rete tradizionale basata su hardware e incentrata sul data center, con soluzioni di accesso remoto centralizzate simili a quanto segue:



PRIMA DI ZSCALER: approccio all'accesso remoto tradizionale e incentrato sul data center

Zscaler Private Access offre una soluzione di perimetro definito da software (SDP). Questa metodologia incentrata sull'esperienza utente è pensata specificatamente per soddisfare le esigenze di scalabilità e le altre necessità di una comunità aziendale moderna, agile e sempre più cloud, ed è radicalmente diversa dalle tradizionali soluzioni VPN di accesso remoto.

Zscaler Private Access sfrutta l'architettura del nostro cloud globale e fornisce un accesso zero trust alle applicazioni private. L'attendibilità, o trust, non viene mai data per scontata, ma si basa invece sull'autenticazione dell'utente e del dispositivo tramite SAML. Una volta che ogni singolo utente è stato autenticato, viene stabilita una connessione dall'interno verso l'esterno, da un App Connector su AWS verso il cloud Zscaler, dove viene instaurata una connessione sicura tra gli utenti autorizzati e le relative applicazioni.

Con Zscaler Private Access, l'accesso alle applicazioni è gestito tramite un security cloud globale, e la rete diventa semplicemente un mezzo di trasporto. L'accesso granulare e basato su policy viene utilizzato per collegare gli utenti autenticati alle applicazioni a cui questi ultimi sono autorizzati ad accedere, in modo che i clienti possano mantenere privato il proprio cloud pubblico.

CON ZSCALER: accesso sicuro e basato su policy, con gli utenti fuori dalla rete

Dato che l'accesso alle applicazioni viene concesso dopo la valutazione del profilo di sicurezza di utenti e dispositivi, le app sono invisibili a chi non dispone dell'autorizzazione pertinente. Inoltre, poiché le applicazioni sono gestite tramite il cloud Zscaler, non ci sono connessioni in entrata all'istanza di AWS o al data center del cliente; questo significa che le liste di controllo degli accessi (ACL) e i gruppi di sicurezza diventano più semplici. Le policy sono basate sulle informazioni relative a utenti/dispositivi e non su oggetti di rete, e garantiscono quindi maggiore visibilità e flessibilità.

Zscaler Private Access permette agli utenti di accedere simultaneamente alle applicazioni consentite, sia nei loro VPC AWS che nei loro data center fisici. La separazione netta tra la rete e l'utente, insieme alla creazione di una connessione con il percorso più breve per raggiungere l'applicazione, migliorano l'esperienza utente, semplificano l'architettura della rete e offrono maggiore visibilità e controllo per la sicurezza.

Accelerare la migrazione delle applicazioni

La soluzione Zscaler Private Access può supportare il business case preliminare di una migrazione. La quantificazione di un'infrastruttura applicativa comporta varie difficoltà; con questo approccio, Zscaler fornisce un framework per offrire un'esperienza utente senza ostacoli, sia negli ambienti legacy che in AWS. Il controllo degli accessi basato su policy sostituisce l'infrastruttura tradizionale, la relativa configurazione e la sua amministrazione continua.

I responsabili dell'architettura o i consulenti possono potenzialmente abbreviare le tempistiche della migrazione. ZPA fornisce una piattaforma dalla quale è possibile controllare l'accesso dell'utente durante la migrazione dei carichi di lavoro su AWS senza che sia necessario apportare modifiche all'infrastruttura di rete legacy. Con ZPA è possibile evitare di ricorrere all'hardware delle VPN tradizionali per la connessione degli utenti alle applicazioni private ospitate su AWS e di impiegare AWS Direct Connect per gestire il percorso del traffico non ottimale del passaggio degli utenti in remoto sul data center per raggiungere l'ambiente AWS.

L'adozione della piattaforma ZPA offre un controllo granulare dell'accesso degli utenti alle applicazioni ospitate su AWS in più aree geografiche e in un ambiente ibrido. Questo approccio è in grado di semplificare l'adozione del cloud e permette al cliente di incrementare la fiducia della propria comunità di utenti durante la migrazione.

Migliorando l'esperienza utente, riducendo drasticamente i processi di controllo delle modifiche, offrendo una visibilità end-to-end sulle applicazioni e fornendo la possibilità di scegliere gruppi/località distinte per la migrazione, che viene intrapresa semplicemente con la gestione centralizzata delle policy, ZPA consente alle aziende di accelerare la migrazione e di fornire la migliore esperienza possibile all'utente.

Gestione avanzata delle identità e degli accessi:

- **Le applicazioni sono invisibili agli utenti/dispositivi che non dispongono della preautorizzazione**
- **Aiuta a rispondere alle minacce moderne alla sicurezza, come gli attacchi DDoS e gli accessi dolosi da fonti terze**
- **Limita la capacità dei malware di muoversi orizzontalmente sulla rete interna**

Quando le applicazioni aziendali, come SAP, Oracle o i carichi di lavoro di Microsoft, vengono spostate su AWS, capita spesso che le questioni relative agli approcci da adottare in merito a rete e sicurezza vengano rimandate a un secondo momento del ciclo di pianificazione ed esecuzione della migrazione. Di conseguenza, i Solution Architect e i Partner di consulenza di APN e AWS riferiscono regolarmente di riscontrare problematiche e ritardi. Con una soluzione efficiente e facile da usare come ZPA tra gli strumenti di pianificazione a disposizione all'inizio del progetto, queste problematiche possono essere comprese, previste ed evitate.

Questo processo spesso riunisce architetti del cloud e stakeholder di IT, reti e sicurezza, i quali vengono coinvolti in attività che altrimenti non farebbero parte della fase di preparazione e pianificazione.

Per queste applicazioni, la migrazione verso l'infrastruttura IaaS rappresenterà un'opportunità interessante e spesso scontata, date le dimensioni e la portata della loro distribuzione. Tuttavia, abbiamo riscontrato che una delle difficoltà iniziali è quella di identificare tutte le applicazioni a cui gli utenti accedono e che sono idonee alla migrazione. A volte, il numero delle app rilevate è significativamente superiore rispetto a quello stimato dai dirigenti IT. ZPA fornisce servizi di rilevamento delle applicazioni private e reportistica per consentire ai clienti di visualizzare tutte le applicazioni a cui viene effettuato l'accesso nel loro data center fisico. In questo modo, l'organizzazione di consulenza e il cliente possono assegnare le priorità alle applicazioni da spostare sul cloud IaaS e migliorare i controlli di sicurezza su di esse.

I clienti possono quindi identificare più facilmente i carichi di lavoro da spostare su AWS, ma dovranno decidere come fornire in modo sicuro le applicazioni ai propri utenti. Questo può rivelarsi problematico se l'applicazione non è stata progettata per la distribuzioni sul cloud.

La gestione delle identità e degli accessi è essenziale per la distribuzione tramite IaaS. Tuttavia, questo controllo degli accessi può essere ulteriormente affinato rendendo le applicazioni invisibili a tutti, tranne agli utenti/dispositivi che dispongono di una preautorizzazione. In questo modo, è possibile affrontare le minacce moderne alla sicurezza, come gli attacchi DDoS, gli accessi dolosi da fonti terze e lo spostamento orizzontale delle minacce nella rete interna.

Siamo stati in grado di implementare lo zero trust [...] e di sostituire gli approcci tradizionali con questo modello moderno, sicuro e incentrato sul cloud. Disponiamo inoltre di un controllo granulare sulle autorizzazioni degli utenti, in modo che ogni dipendente e collaboratore possa accedere solo a ciò di cui a bisogno.

Tony Fergusson, IT Infrastructure Architect, MAN Energy Solutions

Sicurezza avanzata

Zscaler Private Access fornisce un framework di policy granulari per connettere gli utenti alle applicazioni, indipendentemente dalla posizione di queste ultime. ZPA non connette gli utenti alla rete, ma al contrario separa completamente queste due entità. Questo tipo di connettività alle applicazioni offre diversi vantaggi:

- Gli utenti possono accedere alle applicazioni in più ambienti (AWS, on-premise o ibridi) tramite tunnel TLS criptati che vengono generati su richiesta.
- Gli utenti hanno accesso alle app interne senza mai essere collocati sulla rete.
- Gli indirizzi IP possono sovrapporsi nei data center, ma dato che la rete è separata dagli utenti, l'eventuale sovrapposizione risulta irrilevante.
- Le policy per l'accesso alle applicazioni vengono valutate sul cloud Zscaler. La connessione in uscita all'applicazione tramite l'App Connector in esecuzione nell'ambiente dell'app viene stabilita solo dopo l'autenticazione dell'accesso di utente e dispositivo. L'ambiente dell'app è "invisibile" da Internet; questo significa che non vi sono connessioni in entrata al dispositivo o all'ambiente dell'app.
- Le policy granulari specifiche per applicazione e per utente/attributo possono essere scritte e gestite dal cliente o da un MSP.

Concedendo agli utenti solo l'accesso alle applicazioni di cui hanno bisogno in base al relativo ruolo, e non all'intera rete, ZPA offre una sicurezza maggiore rispetto a un approccio tradizionale basato su VPN. Ciò consente di disporre di un profilo di sicurezza intrinsecamente più efficace contro le forme più comuni di intrusione e i malware. Inoltre, Zscaler supporterà e accelererà l'adozione di un approccio zero trust ottimizzato per i clienti di AWS.

In relazione al framework di migrazione su AWS, ZPA consente l'accesso degli utenti ad applicazioni specifiche, fornendo un approccio uniforme per tutti i carichi di lavoro distribuiti su AWS. Limitare gli utenti solo alle applicazioni specifiche di cui hanno bisogno in base al loro ruolo migliora il profilo di sicurezza aziendale. Oltre al ruolo dell'utente, anche lo stato di gestione del dispositivo può essere utilizzato come contesto per rispondere a una richiesta di accesso a un'applicazione. Nell'ambito del modello di responsabilità condivisa di AW, ZPA aiuta i clienti di AWS a fare la propria parte, fornendo meccanismi e metodologie per ottenere il controllo granulare su quali utenti e dispositivi possono accedere alle applicazioni.

In che modo Zscaler Private Access accelera la migrazione su AWS

Preparazione e pianificazione

La soluzione Zscaler Private Access consente di accelerare l'adozione di AWS e di evitare molti dei passaggi tradizionalmente necessari per raggiungere questo obiettivo ponendo l'attenzione sull'aspetto più impegnativo e importante, anche se spesso trascurato, di ogni migrazione: gli utenti.

ZPA consentirà al cliente di:

- Sfruttare l' identità come nuovo perimetro, fornendo un livello di separazione netta tra gli utenti e le applicazioni che cercano di utilizzare.
- Assumere un profilo di sicurezza che non riconosca automaticamente l'attendibilità agli utenti semplicemente per il fatto che si trovano all'interno o all'esterno del perimetro di rete aziendale. Gli utenti vengono invece autenticati tramite la propria soluzione di gestione delle identità e degli accessi (IAM), e l'accesso alle app viene concesso loro in base a una serie di controlli delle policy. I controlli possono basarsi sugli attributi SAML restituiti dalla soluzione IAM.
- Abilitare un approccio basato sul rischio, utilizzando l'autenticazione a più fattori (MFA).
- Ridurre la necessità di un accesso a privilegi elevati e ridurre drasticamente la superficie di attacco per qualsiasi accesso in entrata. Questo risultato si ottiene intercettando le richieste degli utenti per le app interne e applicando la policy prima di connettere l'utente all'app, rendendo così le applicazioni "invisibili" sia da Internet che agli utenti interni non autorizzati.
- Offrire un'esperienza utente senza ostacoli, in quanto questa soluzione si integra in modo trasparente nel normale flusso di lavoro degli utenti, indipendentemente dal fatto che si trovino su una rete aziendale o pubblica. Se si dispone di Zscaler Client Connector (in precedenza Zscaler App), per effettuare la connessione alle applicazioni non è richiesta alcuna azione da parte dell'utente, indipendentemente dalla sua posizione o dal dispositivo che ha scelto di utilizzare.

In questa sezione vengono forniti ulteriori dettagli e i vantaggi di ciascuno dei seguenti passaggi, a cui si fa riferimento nei suggerimenti sulle pratiche da adottare per la migrazione sul cloud AWS, che vengono spesso seguiti dai clienti e indicati nelle procedure di consulenza:

- **Preparazione e pianificazione**
- **Portfolio e rilevamento**
- **Pianificazione operativa e distribuzione**
- **Migrazione e convalida**
- **Operazioni in corso e investimenti futuri**

Portfolio e rilevamento

Molti clienti hanno già intrapreso il proprio percorso verso un modello cloud-first, e Zscaler conoscono i problemi che le aziende vogliono evitare durante i processi di migrazione verso il cloud, ovvero:

- Esperienza utente scadente con lo spostamento delle app dai data center privati al cloud pubblico. Questo problema può essere causato dalla necessità di formare continuamente gli utenti su come utilizzare le app e dalla complessità delle loro prestazioni.
- Complessità di rete causata dalla connessione dei data center privati al cloud pubblico.
- Costo e complessità del dimensionamento, della gestione e della previsione della capacità desiderata e necessaria per supportare il business globale.
- Significative minacce alla sicurezza e incertezza derivanti dalla concessione dell'accesso alla rete aziendale a utenti attendibili e non.

Zscaler Private Access consente di superare queste problematiche offrendo visibilità sulle app interne nelle tre fasi principali della progettazione della sicurezza riportate di seguito.

- Rilevamento: il rilevamento delle applicazioni basato sull'accesso degli utenti indica quali applicazioni interne vengono utilizzate all'interno di un'organizzazione e, conseguentemente, quali vengono usate su AWS.
- Ottimizzazione: una volta rilevata l'applicazione, si può procedere all'ottimizzazione delle policy per stabilire una baseline prima della migrazione. Ciò consente di evitare l'esposizione una volta che l'app viene spostata su AWS e riduce inoltre le tempistiche per la distribuzione finale.
- Produzione: la segmentazione delle applicazioni consente di applicare in modo rapido e granulare le policy in base al profilo di sicurezza e distribuzione richiesto per la realizzazione completa.

Esperienze dei clienti:

Per un grande produttore di bevande a livello mondiale, la procedura di rilevamento aveva individuato oltre 500 applicazioni on-premise. Zscaler ha reso attivo il reparto IT in 95 minuti, ottimizzando l'autenticazione a più fattori e altri attributi. La distribuzione definitiva è cambiata poco dalla distribuzione iniziale.

Zscaler Private Access aiuta ad accelerare la fase di rilevamento integrandosi in modo trasparente nel flusso di lavoro degli utenti. Questi ultimi possono accedere in tutta semplicità all'app che desiderano utilizzare senza dover interagire prima con un software di sicurezza, come ad esempio un client endpoint. Gli utenti non devono più comprendere come deve essere effettuato l'accesso a un'applicazione, sia essa nuova o legacy, e gli amministratori dispongono di una visibilità completa end-to-end sui flussi delle app.

Pianificazione operativa e distribuzione

Quando i clienti identificano le applicazioni da spostare su AWS, decidono anche come distribuire l'applicazione agli utenti. Questo può avvenire essenzialmente attraverso una di queste tre modalità:

Virtualizzazione – L'app rimane privata

- Viene studiata l'architettura esistente dell'applicazione. In un ambiente a tre livelli (server web, server app, server di database) ogni componente verrà virtualizzato e spostato a sua volta su AWS.
- Il front-end potrebbe essere spostato per primo, mentre il server app e il server di database potrebbero rimanere disponibili tramite VPN o attraverso una connessione dedicata, come Direct Connect.
- L'applicazione rimane "privata" e accessibile solo tramite VPN o connessione dedicata.

Grazie a Zscaler, siamo riusciti a essere molto agili [...]. Per questo risultato, riceviamo sempre un feedback molto positivo dagli altri reparti, che così possono continuare a lavorare da casa. Zscaler fa tramontare il concetto di VPN tradizionale".

Marc De Serio, CTO, Henry M. Jackson Foundation (HJF)

Virtualizzazione – L'app è resa pubblica

- È simile alla prima forma, ma il server web di front-end è reso disponibile direttamente su Internet.
- L'applicazione è utilizzabile pubblicamente.
- Vi è il requisito di implementare un firewall WAF (Web Application Firewall) per controllare i contenuti in entrata/in uscita dall'applicazione, le protezioni DDoS e la gestione delle identità e degli accessi per limitare l'accesso degli utenti.

Riprogettazione dell'architettura per il cloud

- Si tratta di applicazioni che non possono o non verranno spostate nella loro forma esistente.
- Il front-end si sposterà su EC2 o su Serverless con CloudFront: ridefinizione dello scopo e riprogrammazione del server web.
- Il livello intermedio viene spostato su EC2 o Serverless: ridefinizione dello scopo del middleware.
- Il back-end viene spostato su RDS/Aurora/ecc.: aggiornamento di schema, DB, ecc.
- L'IAM controlla gli accessi, mentre il WAF controlla i contenuti.
- Esperienza utente e modifica dell'accesso in linea con la migrazione su una nuova architettura.

Rendere pubblica un'applicazione comporta un rischio quantificabile per la sicurezza. Per alcune applicazioni, sia con la riprogettazione dell'architettura che con la virtualizzazione, questo rischio può rivelarsi accettabile per l'azienda. ZPA può consentire ai clienti di promuovere le applicazioni pubblicamente con la stessa architettura di sicurezza sfruttando l'accesso basato su browser: questo modello utilizza la stessa autenticazione SAML su ZPA e la stessa architettura di ZPA per non consentire accessi in entrata e fornisce lo stesso framework di policy e la stessa visibilità.

Tuttavia, per alcune applicazioni, come SAP, il rischio di esporre un'applicazione direttamente a Internet è troppo elevato. Nell'ambito della migrazione su AWS, è dunque fondamentale che la sicurezza venga migliorata. ZPA consente ai clienti di pianificare la migrazione, migliorare la sicurezza e mantenere le applicazioni private.

Migrazione e convalida

Nell'ambito della migrazione, è importante capire dove vengono compiuti dei progressi. Zscaler Private Access offre visibilità su dove vengono utilizzate le applicazioni e sulle policy di sicurezza correlate.

Questa soluzione rappresenta una separazione netta tra l'utente e l'app. La posizione dell'app può essere modificata, passando dal datacenter al cloud pubblico o da un VPC all'altro, senza che vi sia alcun impatto negativo sull'esperienza utente. Gli utenti non si connettono mai direttamente alle applicazioni, e il traffico deve passare attraverso il servizio cloud di ZPA. Inoltre, gli utenti non vengono mai collocati sulla rete, con il conseguente rafforzamento del profilo di sicurezza. Tutte le comunicazioni di ZPA sono connessioni in uscita dal data center o dal cloud pubblico verso il servizio cloud di ZPA. Di conseguenza, i firewall o le ACL del data center possono essere configurati per negare tutte le connessioni in entrata, e il data center/VPC può essere completamente invisibile al resto del mondo.

Zscaler Private Access si integra con il SOC (Security Operations Center) del cliente per il feed SIEM e le attività di reportistica e analisi. La rappresentazione grafica delle applicazioni e degli utenti è fornita mediante la console di gestione di ZPA, e possono essere effettuate delle modifiche alle policy per controllare l'accesso degli utenti alle applicazioni.

Zscaler non fornisce dei servizi di migrazione, ma supporta il processo di convalida della migrazione e garantisce che l'esperienza utente fornita sia in linea con i requisiti aziendali. La visibilità sull'andamento delle migrazioni delle applicazioni per clienti e consulenti è un elemento chiave supportato da ZPA.

Esperienze dei clienti:

Per il governo britannico, ZPA è ormai uno strumento fondamentale, ed è utilizzato per fornire le applicazioni e accedere su AWS. Questo cliente ha adottato un modello zero trust: TUTTE le app vengono utilizzate solo tramite ZPA.

Operazioni in corso e investimenti futuri

Zscaler Private Access consente agli amministratori di AWS e dei nostri clienti di creare delle policy personalizzate su scala globale, specifiche per app e per utente. In questo modo, è possibile ridurre la complessità della segmentazione basata sulla rete.

- Policy semplici per segmentare l'accesso in base all'identità e all'applicazione.
- Non è più necessario creare e implementare policy basate su indirizzi IP difficili da gestire. In altre parole, le operazioni possono essere agili internamente, e chi fa uso dell'applicazione non ne risente. Viene inoltre sfruttato l'ambito DevSecOps per spostare le applicazioni dal cloud privato a quello pubblico, mantenendo però quest'ultimo privato.
- I clienti hanno maggiore controllo e visibilità su quali applicazioni possono essere accessibili a terzi e collaboratori.
- Zscaler investe continuamente nel suo cloud e offre funzionalità sempre più avanzate. Questi progressi si basano sulle necessità e sulle esperienze dei nostri clienti, il cui traffico attraversa numerose organizzazioni globali e ci offre una portata e una visibilità che nessun'altra organizzazione è in grado di replicare da sola. Tutto questo rappresenta un continuo valore aggiunto che si accompagna all'investimento per la soluzione ZPA.

L'infrastruttura delle VPN tradizionali di accesso remoto rappresenta un rischio indipendentemente dalla strategia di migrazione adottata, perché amplia la superficie di attacco delle minacce e colloca sempre gli utenti sulla rete. Zscaler Private Access consente di superare questo rischio implementando i quattro principi di sicurezza seguenti:

- Connettere gli utenti alle applicazioni private (su VPC o DC fisico) senza collocarli sulle reti interne.
- Non esporre mai le applicazioni agli utenti non autorizzati.
- Consentire la segmentazione delle applicazioni senza ricorrere alla complessa e costosa segmentazione della rete, ma in modo strettamente allineato rispetto a VPC, gruppi di sicurezza e/o altre funzioni di servizio.
- Utilizzare Internet come mezzo di trasporto sicuro sulla rete senza affidarsi alle VPN, che possono incrementare la superficie di attacco e complicare l'esperienza utente.

Il risultato di questo approccio è l'azzeramento del movimento laterale verso le applicazioni non autorizzate. Inoltre, le applicazioni alle quali l'utente non ha accesso rimangono completamente invisibili. Esse non possono essere rilevate tramite scansioni delle porte o altri meccanismi, sia al livello locale che con l'indirizzamento verso l'ambiente in cui sono ospitate da Internet. Le applicazioni non ricevono mai connessioni in entrata direttamente dagli utenti.

Esperienze dei clienti:

Attualmente, MAN Energy Solutions fornisce agli sviluppatori partner l'accesso solo agli ambienti e alle applicazioni DevOps di cui hanno bisogno. L'accesso dei partner, in passato, rappresentava una potenziale superficie di attacco, che ora risulta contenuta, in quanto i controlli di accesso basati sull'identità non collocano mai questi utenti e i loro dispositivi sulla rete.

Conclusione

La funzione principale di Zscaler Private Access consiste nel gestire attivamente l'accesso e l'interazione degli utenti autorizzati con i carichi di lavoro, prima, durante e dopo la migrazione sul cloud, migliorando al contempo l'esperienza complessiva dell'utente finale.

I principali vantaggi della trasformazione includono:

- Riduzione delle tempistiche dei progetti di trasformazione e migrazione
- Miglioramento del profilo di sicurezza dopo lo spostamento delle app
- Esperienza utente migliorata, sia durante che dopo la migrazione delle applicazioni

I casi d'uso per l'adozione di ZPA includono

- Adozione del cloud e migrazione delle applicazioni
- Fusioni e acquisizioni
- Accesso di terze parti

La soluzione Zscaler Private Access può essere distribuita in modalità limitata o completa. ZPA si basa su AWS, e il service edge pubblico di ZPA viene distribuito su AWS e in altre sedi in tutto il mondo. Gli App Connector di Zscaler sono collocati su VPC. Zscaler Client Connector è un'applicazione leggera che supporta tutti i principali sistemi operativi per PC e dispositivi mobili. Contattataci per una prova gratuita, una prova di concetto formale o un rollout incrementale di produzione in sostituzione di una prova di concetto. ZPA è disponibile su AWS Marketplace come soluzione con contratto SaaS e supporta la funzione Offerte.

Referenze

Risorse aggiuntive per ricevere informazioni:

Home page di Zscaler: www.zscaler.it

Home page di ZPA: www.zscaler.it/products/zscaler-private-access

Home page di ZPA per AWS: www.zscaler.it/products/zpa-for-aws

Documenti tecnici e di supporto: help.zscaler.com/zia?filter=documentation

MAN Energy Solutions: www.zscaler.it/resources/case-studies/man-energy-solutions.pdf

Framework di adozione del cloud AWS: https://aws.amazon.com/it/professional-services/CAF/

Modello di responsabilità condivisa di AWS: https://aws.amazon.com/it/compliance/shared-responsibility-model/

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.it