Symantec by Broadcom | Carbon Black. by Broadcom | ARROW

GUIDA

Guida alla distribuzione di Symantec ZTNA

Ambito di applicazione

Questa guida illustra l'adozione di ZTNA dal punto di vista di un professionista e intende illustrare le migliori pratiche in materia di pianificazione, integrazione e scalabilità dell'utilizzo di ZTNA all'interno di un'organizzazione. Ogni organizzazione è diversa e, a seconda dei profili degli utenti finali, degli inventari delle applicazioni e dell'infrastruttura IT, ognuna avrà un percorso unico. Una funzione fondamentale di questa guida è riconoscere i gruppi e i team interni che dovranno essere coinvolti per un'implementazione ZTNA riuscita.

Questa guida dovrà essere utilizzata insieme a Broadcom TechDocs per garantire che i passi di implementazione tecnica siano sempre allineati alle capacità attuali e alle configurazioni più aggiornate.

Tech Doc: Symantec Zero Trust Network Access

Pianificazione iniziale

Ci sono molti aspetti da considerare e molti stakeholder da coinvolgere quando si pianifica l'implementazione di uno ZTNA. Di seguito sono riportati gli elementi chiave che, se non considerati prima dell'implementazione tecnica, potrebbero causare ritardi significativi nel progetto.

Per i passi di pianificazione generale, fare riferimento a questo TechDoc

Denominazione e ubicazione del tenant ZTNA

Il tenant ZTNA richiede che vengano definiti 2 parametri prima della creazione del tenant nel CMP (Customer Management Portal, Portale di gestione clienti):

1. La geolocalizzazione del Management PoD (UE/USA) è un'impostazione fondamentale che determina la regione sia per l'instradamento del percorso dati che per la raccolta dei log. Questa selezione è fondamentale perché i Connectivity PoD, responsabili dell'elaborazione delle policy, sono collegati geograficamente ai rispettivi Management PoD. Assegnazione dei Management e dei Connectivity PoD
2. Il nome del tenant crea un dominio personalizzato univoco sia per l'accesso al Portale utente che alle applicazioni senza agenti. È fondamentale selezionare con attenzione il nome del tenant per rappresentare accuratamente la propria organizzazione e il proprio ambiente, poiché una volta impostato non sarà possibile modificarlo.

   L'URL completo del tenant è formato combinando il "Nome del tenant" scelto con il suffisso "luminatesec.com".

Provider di identità

L'integrazione di un Provider di identità (Identity Provider, IdP) è fondamentale per Symantec ZTNA, poiché costituisce la base del flusso di autenticazione. Sebbene gli utenti locali siano adeguati per le Proof of Concept (PoC), il coinvolgimento del team di gestione IdP dell'organizzazione come parte interessata è fondamentale per un'implementazione produttiva riuscita. Spesso, le persone che implementano ZTNA possono essere alla guida di iniziative di ingegneria Zero Trust, SSE, architettura proxy o VPN. La collaborazione con il team IdP è essenziale per comprendere in che modo gli utenti e i gruppi si rapportano alle applicazioni che ZTNA fornirà, il che, a sua volta, aiuta a definire la struttura delle policy necessaria.

Dal punto di vista tecnico, occorre considerare due aspetti fondamentali: l'integrazione con le piattaforme SSO dell'organizzazione, in genere provviste di SAML (e talvolta OIDC) e la Risoluzione dei gruppi, che può essere gestita analizzando gli attributi SAML o utilizzando il protocollo SCIM.

"SAML generico" è l'opzione di integrazione IdP consigliata. Questa scelta supporta sia l'integrazione SAML sia la risoluzione dei gruppi tramite le opzioni SCIM e Attributo SAML.

- TechDoc: Integrare IdP

Se SCIM non è supportato dall'IDP del cliente, per la risoluzione del gruppo deve essere utilizzata l'opzione "Attributo SAML". Ciò consente al cliente di analizzare la risoluzione del gruppo direttamente dalla risposta SAML.

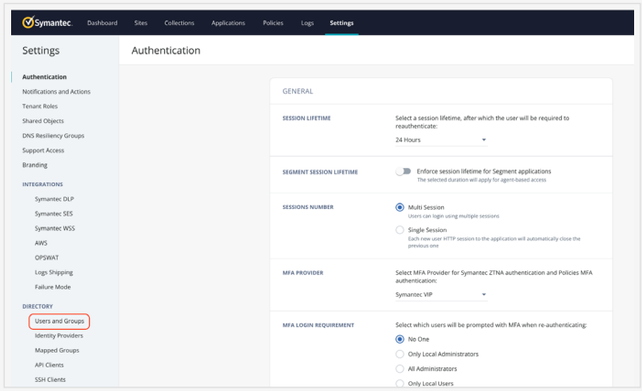
Guida alla distribuzione de Symantec ZTNA

Pianificazione iniziale

Provider di identità

Solo accesso senza agenti

Gli “Utenti locali” possono essere utilizzati per applicazioni senza agente (applicazioni Web, RDP, SSH, TCP) all’interno dello ZTNA Entity Store. Questa soluzione è adatta per la valutazione del servizio, la Proof of Concept (PoC) o l’accesso limitato di terze parti.



Solo accesso basato su agenti

Per l’accesso basato su agenti mediante agenti WSSA, SES ed ESA con Segment Applications, è richiesta l’integrazione SAML. Ciò significa che gli utenti locali non sono supportati. Inoltre, l’Identity Provider (IDP) deve essere integrato con Symantec Cloud SWG, il che rende necessaria l’autenticazione SAML per Cloud SWG all’interno dell’organizzazione.

- TechDoc: Autenticazione SAML Cloud SWG

Inventario delle applicazioni e metodo di accesso ZTNA

La migrazione a ZTNA è un processo dall’alto verso il basso che necessita di intelligence dal basso verso l’alto: in genere le VPN e altri protocolli di accesso remoto non hanno bisogno di sapere a quale applicazione un utente intende accedere, poiché questa viene in quel momento gestita dai proprietari delle applicazioni.

La prima considerazione importante da fare è se l’organizzazione desidera iniziare con ZTNA basato su agenti o senza agenti. Sebbene entrambe le soluzioni coesistano nella maggior parte delle implementazioni ZTNA, iniziare con una delle due è ideale in ottica di progetto pilota

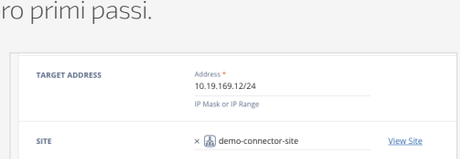
Accesso basato su agenti

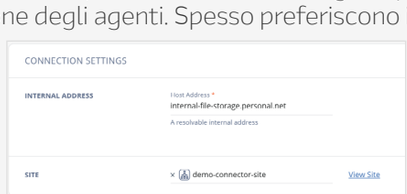
Il metodo di accesso basato su agenti offre tre vantaggi chiave::

- **Esperienza utente fluida:** gli utenti finali non subiscono alcun impatto, poiché non sono necessarie modifiche al dominio o alla rete.
- **Sfrutta l’infrastruttura esistente:** il metodo si basa sul DNS privato dell’organizzazione, eliminando la necessità di modificare il flusso di lavoro.
- **Onboarding rapido:** è possibile proteggere rapidamente interi cluster di rete con un’unica applicazione e policy. Le regole granulari sui privilegi minimi possono quindi essere applicate in una fase successiva, evitando vincoli temporali.

Per i clienti Symantec esistenti che utilizzano già agenti WSSA, SEC o ESA come parte delle loro distribuzioni SWG, CASB o EPP, ZTNA è spesso più facile da implementare. Ciò avviene perché gli amministratori delle policy ZTNA possono inizialmente definire ampie sezioni della rete dell’organizzazione in cui risiedono le applicazioni, senza dover conoscere le applicazioni specifiche a cui si accede. Nel tempo, questi amministratori possono perfezionare le policy per renderle più mirate, consentendo l’accesso solo ai domini o agli IP di cui gli utenti hanno specificatamente bisogno.

Al contrario, per i clienti che non hanno familiarità con Symantec, il metodo basato su agenti può complicare la distribuzione iniziale in base alle esigenze di distribuzione degli agenti. Spesso preferiscono il metodo senza agenti per i loro primi passi.





Guida alla distribuzione de Symantec ZTNA

Pianificazione iniziale

Inventario de aplicaciones y método de acceso ZTNA

Accesso senza agenti:

ZTNA senza agenti offre un approccio più sicuro in quanto richiede la definizione esplicita dei privilegi minimi per le risorse fin dall'inizio. Questo metodo richiede la configurazione di tutte le applicazioni sulla console Symantec ZTNA e la specificazione di policy di accesso per utenti e gruppi. Sebbene modifichi il flusso di lavoro di un utente, richiedendo l'uso del DNS globale per l'accesso all'applicazione (pubblicando l'URL dell'applicazione nel DNS pubblico tramite aggiornamento CNAME o modificandolo), gli utenti in genere preferiscono l'accesso senza agenti rispetto alla VPN una volta che vi si sono abituati.

Oltre alle applicazioni Web, il metodo senza agenti si rivela vantaggioso per l'accesso SSH e RDP, inclusi i client SSH e RDP nativi, senza interrompere i flussi di lavoro DevOps

Pubblico di destinazione (Agent Traffic Manager)

Quando si implementa il metodo di accesso basato su agenti, è fondamentale selezionare attentamente il pubblico di destinazione per evitare interruzioni organizzative diffuse dovute a potenziali configurazioni errate. Inizialmente, limitare il pubblico di destinazione a un insieme ristretto di utenti o gruppi per il lancio di ZTNA utilizzando Agent Traffic Manager

Cumplimiento del dispositivo

La conformità del dispositivo può essere applicata con Symantec ZTNA tramite l'agente Symantec Endpoint Protection, che richiede che l'organizzazione disponga di una licenza per Symantec Enterprise Security. Questa capacità viene fornita tramite Host Integrity Checks: TechDoc

Durante il processo di pianificazione di ZTNA è fondamentale definire "cosa" l'organizzazione desidera convalidare sui dispositivi degli utenti finali. Certificati del dispositivo? Livello di patch del sistema operativo? Processi in esecuzione? Collaborare con il team di gestione degli endpoint dell'organizzazione può aiutare a trovare queste risposte e a garantire che la configurazione del profilo di conformità avvenga rapidamente.

Gestione amministrativa

A seconda del modo in cui l'organizzazione gestisce e distribuisce le applicazioni aziendali, potrebbe essere necessario che più team utilizzino la console di amministrazione ZTNA. In tal caso, stabilire in anticipo i ruoli e le responsabilità di ciascuno permetterà la creazione di policy RBAC che consentano a tutti di lavorare all'interno del proprio dominio senza interferire con quello di un altro gruppo.

Considerare in anticipo i vari gruppi che saranno necessari per la distribuzione di ZTNA in modo da poter definire rapidamente l'RBAC. Tre ruoli chiave da considerare:

- **Amministratore della piattaforma ZTNA:** l'amministratore globale responsabile dell'integrazione degli IdP, della gestione dei log, dell'assegnazione degli amministratori delle policy, della creazione dei siti di distribuzione e dell'autorizzazione dell'accesso alle API.
- **Amministratore del sito:** incaricato di gestire i connettori ZTNA e di distribuirli nei rispettivi siti.
- **Amministratori delle applicazioni (raccolta):** responsabili del caricamento delle applicazioni in ZTNA e della definizione della policy di chi può accedervi.
- **Amministratore delle policy di accesso (raccolta):** limitato alla sola gestione delle policy di accesso alle applicazioni

Maggiori informazioni sull'amministrazione RBAC sono disponibili sui TechDocs.

Guida alla distribuzione de Symantec ZTNA

Distribuzione iniziale

Integrazione del provider di identità

Come discusso in precedenza, è necessario pianificare una sessione di lavoro con il team di ingegneria IdP per consentire l'SSO e la risoluzione del gruppo in ZTNA. Per ZTNA basato su agenti, il Cloud SWG dell'organizzazione dovrebbe già avere un piano per l'integrazione con lo stesso IdP, ovvero sfruttare il SAML Captive Portal. Nella sezione di automazione riportata di seguito sono riportate le istruzioni per adottare l'autenticazione SAML per Symantec Agent.

Accesso amministratore

Se durante la pianificazione sono stati definiti i ruoli, la prima cosa da fare dopo aver integrato l'IdP è aggiungere altri amministratori. La migliore pratica è definire un gruppo all'interno dell'IdP e mapparlo come amministratore globale ZTNA.

Inoltre, può essere molto utile definire "raccolte" con amministratori responsabili dell'integrazione delle applicazioni e della creazione di policy di accesso.

Rispecchiare gli approcci interni basati su "livelli" applicativi o "gruppi di servizi" può contribuire ad allineare l'architettura ZTNA ai processi interni dell'organizzazione. In questo caso, lavorare con il gruppo IdP può essere di grande aiuto, poiché spesso tali gruppi di lavoro sono già stati definiti.

- TechDoc: Raccolte ZTNA

Distribuzione del connettore

Spesso denominato "Sito" in Symantec ZTNA, il connettore è il modo in cui il servizio cloud ZTNA si connette alle applicazioni gestite dai clienti nei data center o nei provider Cloud IaaS.

I connettori dovrebbero essere distribuiti il più vicino possibile alle applicazioni; parte del processo di inventario delle applicazioni dovrebbe includere la registrazione della posizione di ciascun gruppo di applicazioni; in tal caso, si consiglia di distribuire almeno due connettori su tali segmenti di rete.

I connettori sono disponibili nei formati Docker, Docker Compose, Kubernetes e VM ESXi.

Cloud Orchestrator

Per un ciclo di vita del connettore senza interruzioni all'interno di orchestratori cloud come K8S e OpenShift, Fargate (e altri), si consiglia di utilizzare la modalità di autenticazione "Sito". In questo modo si evita la necessità di una preregistrazione con una password monouso univoca (OTP) per ciascun connettore.

- Connettori: TechDoc

Continuità aziendale e Disaster Recovery

Quando si distribuiscono connettori per un sito, è necessario specificare la regione a cui si desidera che i connettori si colleghino: ciò si riferisce alla regione GCP. Nel caso in cui GCP subisca un'interruzione o l'organizzazione subisca un'interruzione di rete, un sito di backup mappato su una regione diversa può fungere da fase di ripristino.

Per fare ciò, è necessario creare un nuovo sito mappato su una regione diversa; tali connettori devono essere distribuiti in un'altra parte della rete dell'organizzazione che abbia ancora accesso alle applicazioni nel sito principale. In caso di interruzione, le applicazioni possono essere spostate da una sede all'altra all'interno di ZTNA.

Questo processo può essere automatizzato con uno script sfruttando l'API

- ZTNA. API: Associare l'applicazione al sito

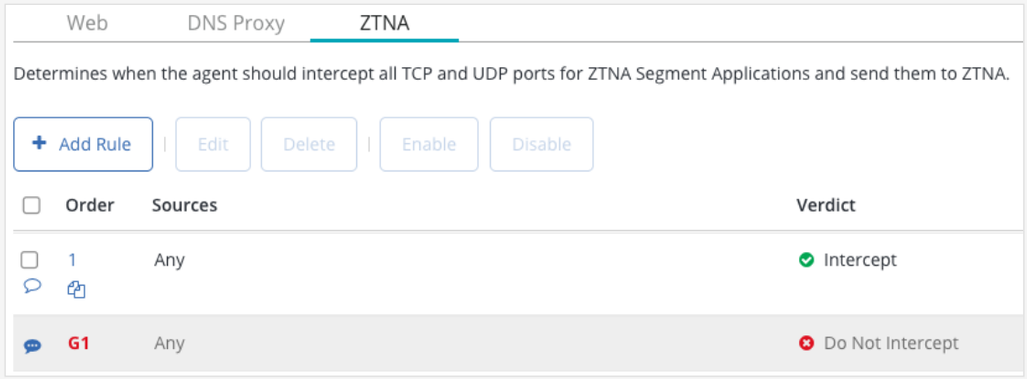
Guida alla distribuzione de Symantec ZTNA

Distribuzione iniziale

Agent Traffic Manager

Assicurarsi che siano definite le entità a cui verrà applicato ZTNA. Per impostazione predefinita, a ZTNA non sono assegnate entità, a meno che non siano configurate in modo esplicito.

Per prevenire potenziali impatti, assegnare entità per ZTNA in ATM prima della creazione dell'applicazione Segment.



Catalogo delle applicazioni

Come discusso in precedenza, è fondamentale comprendere l'inventario delle applicazioni che ZTNA supporterà, sia senza agenti che basato su agenti. Dopo l'implementazione del connettore, gli amministratori dovranno definire le applicazioni singolarmente o come subnet se utilizzano Symantec Agent.

Assicurare che ogni applicazione sia mappata a una raccolta appropriata può semplificare la successiva creazione di policy di accesso.

Per garantire che non si verifichi alcun accesso indesiderato prima del lancio di ZTNA, è presente un interruttore di "abilitazione" per ogni applicazione.

Configurazione delle policy

L'accesso alle applicazioni per gli utenti è concesso solo quando esisterà una policy che definirà le entità pertinenti e l'applicazione di destinazione. Seguendo il principio del "privilegio minimo", le applicazioni saranno inaccessibili per impostazione predefinita.

Per consentire l'accesso all'applicazione, è necessario che sia in atto una policy specifica per tale applicazione.

È importante notare che più policy possono concedere l'accesso a diverse entità a diverse applicazioni. In tali casi, la regola della "risoluzione dei conflitti" (definita in Valutazionedelle policy di accesso) determinerà quale policy verrà applicata.

Guida alla distribuzione de Symantec ZTNA

Distribuzione iniziale

Onboarding dell'utente finale

L'estensione dell'accesso agli utenti finali dopo una proof-of-concept è una delle sfide più grandi per ZTNA, poiché i professionisti della sicurezza hanno spesso il compito di incidere il meno possibile sull'esperienza dell'utente finale. Le sezioni seguenti descrivono in dettaglio le migliori pratiche per far accedere gli utenti finali a ZTNA.

Implementazione graduale di ZTNA (SAML):

Utilizzare innanzitutto Symantec Agent per Zero Trust Network Access è il modo migliore per garantire che gli utenti finali abbiano accesso a tutte le applicazioni a cui normalmente accederebbero tramite VPN, poiché utilizza DNS interno e opera a livello 3, consentendo di supportare le applicazioni legacy.

L'abilitazione del SAML Captive Portal per Cloud SWG può rappresentare uno dei maggiori ostacoli per ZTNA, poiché molte organizzazioni sono riluttanti a compromettere l'esperienza dell'utente finale. In definitiva, è fondamentale applicare realmente il modello Zero Trust dal punto di vista dell'architettura, oltre che implementare Zero Trust Network Access.

Il SAML Captive Portal di Cloud SWG può ora essere distribuito gradualmente a gruppi specifici, in modo che le organizzazioni possano testarlo con utenti mirati, riducendo il rischio che il supporto IT venga sommerso dai ticket e garantendo una transizione senza intoppi.

- TechDoc: Implementazione graduale di SAML

Da lì, ZTNA può essere implementato gradualmente sfruttando Cloud SWG Agent Traffic Manager. Alcuni utenti o gruppi, che hanno abilitato SAML, possono iniziare ad accedere alle applicazioni interne tramite Symantec Agent, senza dover toccare l'endpoint.

- TechDoc: Agent Traffic Manager

In alternativa, per le organizzazioni che utilizzano l'agente Symantec Endpoint Security per il reindirizzamento del traffico, è possibile creare facilmente gruppi di dispositivi nella console ICDm, dove le policy di gruppo potranno specificare se il dispositivo dovrà eseguire il reindirizzamento del traffico e, in tal caso, come dovrà essere autenticato il traffico.

- TechDoc: Symantec Endpoint Security - Reindirizzamento Web e traffico

Onboarding rapido:

Per le organizzazioni che già utilizzano l'autenticazione SAML con il proprio agente Symantec, ZTNA può essere eseguito a livello aziendale senza apportare modifiche agli endpoint dell'utente: una volta che il tenant Cloud SWG e il tenant ZTNA sono integrati con un token e un DNS interno definito, le richieste interne degli utenti verranno immediatamente risolte e instradate all'applicazione corretta, se la policy lo consentirà.

Si consiglia di definire DNS, segmenti di rete e policy di accesso prima dell'integrazione con il tenant Cloud SWG, ma Agent Traffic Manager può essere utilizzato anche per garantire che nessun agente Cloud SWG sfrutti ZTNA finché l'organizzazione non sarà pronta.

Implementazione graduale dell'applicazione:

Per implementare gradualmente una nuova applicazione su un gruppo di test quando la tua organizzazione è già integrata a ZTNA, segui questi passi:

1. In ATM, configurare l'applicazione per il bypass per tutti gli utenti;
2. Creare l'applicazione all'interno della console ZTNA
3. Per il gruppo di test designato, escludere l'applicazione dal bypass in ATM

Questi passi garantiscono che il traffico dell'applicazione venga intercettato esclusivamente dal pubblico del gruppo di test

Accesso senza agenti

Alcune organizzazioni optano inizialmente per una distribuzione senza agenti, soprattutto se prevedono di supportare numerose applicazioni tramite il metodo senza agenti.

Questo approccio è ottimo perché può coesistere con le VPN e consentire alle organizzazioni di controllare completamente la velocità di implementazione. Si consiglia di iniziare con un numero limitato di applicazioni con basi di utenti ben definite e di spostarle su ZTNA.

Una buona pratica è quella di utilizzare un nome di dominio personalizzato per il tenant ZTNA, in modo che gli utenti capiscano che stanno accedendo ad applicazioni gestite dall'azienda.

- TechDoc: Dominio personalizzato

Guida alla distribuzione de Symantec ZTNA

Distribuzione iniziale

Conformità del dispositivo

Symantec Endpoint Security è necessario per la conformità dei dispositivi per l'accesso basato su agenti: sfruttando i controlli di integrità dell'host, gli amministratori possono garantire che solo gli endpoint aziendali autorizzati accedano alle applicazioni private.

Si consiglia di collaborare con i team interni di Endpoint Management per comprendere il profilo di base dei dispositivi aziendali e redigere criteri di conformità il più possibile semplici da allineare. È possibile sfruttare anche criteri aggiuntivi, come la geolocalizzazione dell'utente e l'IP di origine, per garantire la conformità agli standard sui dati come il GDPR, ecc.

- TechDoc: Conformità del dispositivo ZTNA

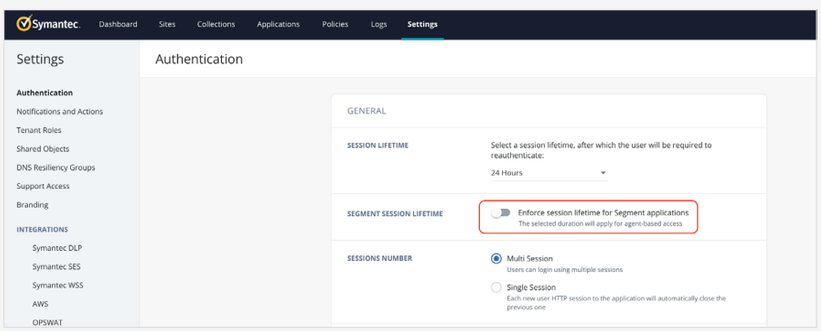
ZTNA "Sempre attivo/On-demand":

Alcuni clienti scelgono di utilizzare la modalità "ZTNA sempre attivo". Ciò consente agli utenti di rimanere connessi tramite l'agente Symantec finché la loro sessione Identity Provider (IDP) sarà attiva, offrendo un vantaggio significativo rispetto alle VPN tradizionali.

Tuttavia, alcuni scenari richiedono un approccio più mirato. Sebbene i clienti possano preferire sessioni IDP estese per l'accesso a Symantec Web Gateway (SWG) (per evitare frequenti richieste di autenticazione durante la navigazione in Internet), potrebbero al contempo dover applicare sessioni più brevi (ad esempio, 12 ore) per ZTNA, richiedendo una nuova autenticazione specifica per l'accesso alle applicazioni interne.

Per supportare questo approccio "On-demand", è necessario abilitare la funzionalità "Durata della sessione del segmento". Ciò garantisce che le sessioni ZTNA rispettino le impostazioni configurate di durata della sessione, senza forzare una nuova autenticazione per l'accesso generale a Internet.

- Tech Doc: Durata della sessione del segmento



Guida alla distribuzione de Symantec ZTNA

Automazione e operazionalizzazione

Cumplimiento del dispositivo

Onboarding dell'applicazione:

Ogni applicazione che verrà distribuita da ZTNA dovrà essere definita all'interno del motore delle policy: ciò può comportare un notevole sforzo di lavoro, poiché è necessario che tutte le applicazioni o le posizioni di rete siano predefinite. I team di ingegneria ZTNA dovrebbero collaborare con i gruppi IdP e ITSM all'interno dell'organizzazione per comprendere l'inventario delle applicazioni: l'ideale è predisporre una pipeline per l'onboarding automatico e mantenere aggiornate le applicazioni in ZTNA. Questa operazione potrà essere automatizzata con l'API ZTNA.

- API: Gestire le applicazioni

Per la configurazione iniziale con accesso basato su agenti, le organizzazioni possono valutare di iniziare definendo ampie subnet a cui consentire l'accesso agli utenti, per assicurarsi che non perdano nessuna applicazione. Ciò consentirà agli utenti anche l'accesso ad applicazioni a cui altrimenti non avrebbero bisogno di accedere: la policy ZTNA segue la corrispondenza del prefisso più lungo, quindi gli amministratori potranno creare definizioni di segmenti di rete sovrapposti e quella più precisa avrà la precedenza. Pertanto, man mano che vengono definite applicazioni ad alto impatto, è possibile che vengano applicate policy di accesso più rigorose.

- Corrispondenza del prefisso più lungo: Wikipedia

Monitoraggio:

Sebbene il monitoraggio generale del servizio sia importante, la maggior parte può essere automatizzato effettuando impostazioni di notifica nella console ZTNA per lo stato del connettore e quello dell'applicazione. Un ulteriore livello di monitoraggio che le organizzazioni dovrebbero prendere in considerazione è l'accesso degli utenti: è possibile interrogare l'API ZTNA per fornire solo i log dei tentativi di connessione non riusciti. Ciò può aiutare a chiarire se utenti e gruppi hanno bisogno di accedere alle applicazioni e alla policy ZTNA.

Sebbene al momento questa funzionalità non sia supportata, può essere inclusa nelle revisioni IAM per semplificare e ottimizzare in futuro le policy ZTNA.

- API: Log forensi

Prevenire la perdita dei dati:

DLP Cloud Detection è disponibile per ZTNA senza agenti, colmando una lacuna nell'offerta di accesso ad applicazioni private da dispositivi non gestiti. Prima dell'implementazione, il team ZTNA dovrà collaborare con il team di amministrazione DLP per definire un framework di governance che consenta di comprendere al meglio quali policy DLP assegnare alle diverse applicazioni. Gli amministratori DLP utilizzeranno la console DLP Enforce per creare policy DLP; l'unica azione che il team ZTNA dovrà intraprendere è definire a quale applicazione senza agenti dovranno essere assegnate le policy DLP. Le policy DLP verranno assegnate a un gruppo di "Rilevamento applicazioni" e l'ID di tale gruppo verrà assegnato alla policy ZTNA. L'assegnazione delle policy DLP per i gruppi di rilevamento applicazioni è di tipo

molti-a-molti, ma a ciascuna applicazione in ZTNA potrà essere assegnato solo un gruppo di rilevamento applicazioni. La creazione di "livelli" dell'applicazione o "ambiti di dati" può aiutare a configurare una sola volta la policy ZTNA, consentendo poi al team DLP di aggiornare e riassegnare le policy secondo necessità senza l'intervento del team di ingegneria ZTNA.

DevSecOps:

ZTNA offre una grande opportunità di eliminare la dipendenza dello sviluppo software dalla VPN, consentendo di adottare una vera e propria architettura di microservizi per la pipeline CI/CD. I team di pianificazione di ZTNA dovranno collaborare con i propri team di sviluppo interni per verificare la possibilità di integrazione in ZTNA in modo che gli sviluppatori non debbano accedere alle risorse cloud da reti note, il che rappresenta la tipica policy di sicurezza della maggior parte delle organizzazioni.

Symantec ZTNA dispone di un provider Terraform predefinito che potrà essere integrato nella pipeline CI/CD, ma l'API ZTNA è in grado di supportare qualsiasi provider.

- Terraform: Github
- Symantec ZTNA: Puertas de enlace SSH

Escalamiento automático:

I connettori delle applicazioni Symantec ZTNA bilanciano automaticamente il carico delle sessioni su un "sito", ma nel caso in cui fosse necessaria una maggiore larghezza di banda, l'implementazione di connettori aggiuntivi potrà distribuire attivamente il carico senza la necessità di tempi di inattività.

Un fattore che un'organizzazione dovrebbe considerare è l'automazione dell'implementazione di nuovi connettori da una piattaforma ITSM: i siti sono preconfigurati, e in caso di necessità di un nuovo connettore, è possibile interrogare l'API ZTNA per ottenere una password monouso e avviare immediatamente un nuovo contenitore.

- API ZTNA: Creare un connettore

Guida alla distribuzione de Symantec ZTNA

Automazione e operazionalizzazione

Accesso Just In Time

Molte organizzazioni hanno difficoltà a sentirsi a proprio agio nell'assegnare l'accesso alle applicazioni al di sopra delle applicazioni stesse: con ZTNA, gli amministratori dovranno decidere a quali applicazioni gli utenti potranno accedere prima ancora di autenticarsi nell'applicazione stessa.

Per questo motivo, le organizzazioni dovrebbero prendere in considerazione l'integrazione con la piattaforma ITSM, in modo che gli utenti possano inviare richieste per ottenere automaticamente l'accesso. L'accesso just-in-time implica che gli utenti possono ottenere l'accesso per un breve periodo di tempo, per completare il loro processo aziendale, e tale accesso potrà essere revocato automaticamente; a quel punto il team IAM dovrebbe valutare la richiesta di accesso permanente.

- API ZTNA: Aggiornare la policy di accesso

Resilienza aziendale

Symantec ZTNA è implementato come una vera e propria piattaforma SaaS di microservizi su Google Cloud Platform, il che significa che è presente ridondanza integrata a tutti i livelli del servizio. Il punto principale di potenziale errore è la connessione del connettore dell'applicazione a Symantec Enterprise Cloud. I connettori sono collegati a specifiche regioni GCP, principalmente per motivi di sicurezza e riservatezza dei dati.

Ogni regione GCP ha tre zone di disponibilità, di cui il connettore ZTNA sarà attivo-attivo in due zone. Nel caso in cui una zona di disponibilità GCP subisca un'interruzione, il connettore passerà automaticamente tutte le connessioni lungo la zona di disponibilità attiva e stabilirà una nuova connessione con la terza zona di disponibilità. Mantenere tutti i collegamenti all'interno della regione.

Se una regione GCP non fosse disponibile in nessuna zona, gli amministratori ZTNA verrebbero avvisati dell'interruzione. Inoltre, per determinare questo stato, è possibile interrogare anche l'API ZTNA.

Il servizio può essere ripristinato rapidamente sfruttando una diversa regione GCP. Il modo per configurare questa soluzione sarebbe quello di avere due "siti" ZTNA distribuiti nella stessa posizione di distribuzione dell'applicazione (data center, IaaS, ecc.). Il "Sito A" sarebbe il sito primario per l'utilizzo normale, configurato in modo tale da connettersi alla regione GCP più vicina per motivi di prestazioni o a una regione specifica per motivi di conformità dei dati. Quindi, il "Sito B" verrebbe configurato per utilizzare una diversa regione GCP, perciò questi due connettori si troverebbero uno accanto all'altro sulla rete dell'organizzazione, ma ognuno si connetterebbe a regioni GCP diverse.

Le applicazioni ZTNA per quella posizione sarebbero configurate per connettersi tramite il connettore ZTNA "Sito A" e nessuna applicazione sarebbe connessa al "Sito B". In caso di interruzione, tramite l'interfaccia utente ZTNA e tramite l'API, tutte le applicazioni potranno essere aggiornate per iniziare a connettersi tramite il "Sito B", che andrebbe alla regione GCP online.

Poiché tutto ciò avviene dietro il servizio ZTNA, non sono necessarie modifiche al DNS né modifiche al flusso di lavoro dell'utente finale.

- API ZTNA: Aggiornare l'applicazione